



使用者指南

AWS Security Hub



AWS Security Hub: 使用者指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 Security Hub 和 Security Hub CSPM ?	1
AWS Security Hub	2
功能	2
整合	3
Accessibility	3
定價	4
概念	4
成本估算器	8
依帳戶類型存取	9
先決條件	9
設定跨帳戶存取權	10
使用成本估算器	13
重要說明	20
相關資訊	21
啟用 Security Hub	21
為 AWS 組織啟用 Security Hub	21
在獨立帳戶中啟用 Security Hub	23
指定委派管理員	24
建立委派管理員政策	25
管理成員帳戶的組態	26
移除委派管理員	30
重新啟用 Security Hub	30
建議	31
帳戶涵蓋範圍	32
帳戶涵蓋範圍頁面	32
安全涵蓋範圍小工具	34
延伸計畫	34
延伸計畫的許可	34
註冊擴展計劃合作夥伴	35
取消訂閱合作夥伴	35
跨區域彙總	36
彙總的資料類型	36
管理員和成員帳戶的彙總	37
自動化規則和跨區域彙總	38

啟用彙總	38
檢閱彙總設定	39
更新彙總設定	39
刪除彙總	40
「摘要」儀表板	41
考量事項	41
可用的小工具	41
可用的篩選條件	53
檢視 Security Hub 中資源的詳細資訊	54
調查結果格式：OCSF	55
OCSF 概觀	55
相關資源	55
AWS OCSF 擴充功能	56
涵蓋範圍問題清單	78
AWS Security Hub CSPM 的涵蓋範圍調查結果	78
Amazon GuardDuty 的涵蓋範圍調查結果	79
Amazon Inspector 的涵蓋範圍調查結果	79
Amazon Macie 的涵蓋範圍調查結果	79
隱藏涵蓋範圍調查結果	80
公開調查結果	80
公開調查結果的運作方式	80
公開調查結果的元件	81
嚴重性分類	82
公開調查結果的優點	83
公開問題清單的來源	83
最佳實務	83
支援的資源	84
支援的特徵	84
產生暴露問題清單	86
判斷暴露問題清單的嚴重性等級	90
檢閱暴露問題清單	90
潛在攻擊路徑圖	92
修復暴露問題清單	93
未使用的存取權調查結果	138
未使用的存取分析如何運作	138
未使用的存取問題清單類型	138

服務連結分析器	139
檢視未使用的存取調查結果	139
公開調查結果中未使用的存取權	139
未使用許可的政策建議	140
定價	140
政策建議	140
政策建議的運作方式	140
誰可以產生建議	141
建議生命週期	141
錯誤案例	141
使用主控台	141
API 參考	142
自動化	142
自動化規則	142
EventBridge 自動化規則	157
第三方整合	3
Jira Cloud	165
ServiceNow	170
票證整合的 KMS 金鑰政策	176
測試票證整合	179
監控用量和成本	181
誰可以存取用量頁面	181
組織和帳戶成本摘要	181
功能檢視	182
帳戶檢視	183
成本最佳化策略	184
相關資源	184
停用 Security Hub	184
停用單一帳戶的 Security Hub	184
停用整個組織的 Security Hub	184
安全	186
資料保護	187
身分與存取管理	189
法規遵循驗證	214
恢復能力	214
基礎設施安全性	214

VPC 端點 (AWS PrivateLink)	215
記錄 API 呼叫	216
CloudTrail 中的 Security Hub 資訊	217
範例：Security Hub 日誌檔案項目	217
AWS Security Hub CSPM	221
Security Hub CSPM 的優點	222
存取 Security Hub CSPM	223
相關服務	224
Security Hub CSPM 免費試用、用量和定價	224
檢視用量詳細資訊	224
定價詳情	225
概念	225
啟用 Security Hub CSPM	230
驗證必要的許可	230
啟用 Security Hub CSPM 與 Organizations 整合	230
手動啟用 Security Hub CSPM	232
後續步驟：姿勢管理和整合	234
設定 AWS Config	234
本機組態	238
中央組態	239
管理多個 帳戶	275
使用 管理帳戶 AWS Organizations	275
透過邀請手動管理帳戶	276
多帳戶環境的建議	277
使用 管理帳戶 AWS Organizations	278
應邀管理帳戶	291
管理員和成員帳戶允許的動作	303
帳戶動作對資料的影響	308
跨區域彙總資料	310
彙總的資料類型	311
管理員和成員帳戶的彙總	312
中央組態和彙總	313
啟用彙總	314
檢閱彙總設定	316
更新彙總設定	317
停止彙總	319

標準	320
標準參考	321
啟用標準	394
檢閱標準的詳細資訊	399
關閉自動啟用的標準	402
停用標準	403
控制項	406
合併控制項檢視	406
控制項的摘要安全分數	407
控制項參考	407
設定控制項的許可	1124
啟用控制項	1125
停用控制項	1132
安全檢查和分數	1141
控制類別	1212
檢閱控制項的詳細資訊	1215
篩選和排序控制項	1217
控制參數	1218
檢閱和管理控制問題清單	1230
整合	1258
檢閱整合清單	1258
啟用來自 整合的問題清單流程	1260
從整合停用問題清單的流程	1261
從整合檢視問題清單	1262
AWS 服務 整合	1262
第三方整合	1281
自訂產品整合	1314
調查結果	1316
用於尋找供應商的 BatchImportFindings	1318
客戶的 BatchUpdateFindings	1321
檢閱問題清單詳細資訊和歷史記錄	1324
篩選問題清單	1328
分組問題清單	1330
設定問題清單的工作流程狀態	1331
將問題清單傳送至自訂動作	1334
問題清單格式：ASFF	1334

洞見	1617
檢閱洞見並採取行動	1617
受管的洞見	1620
自訂洞見	1630
自動化	1637
自動化規則	1638
自動化回應和修復	1662
「摘要」儀表板	1676
摘要儀表板的可用小工具	1677
篩選儀表板	1680
自訂儀表板	1681
區域限制	1682
跨區域彙總限制	1682
依區域的整合可用性	1683
區域標準可用性	1685
依區域的控制項可用性	1685
控制的區域限制	1685
使用 CloudFormation 建立資源	1917
Security Hub CSPM 和 CloudFormation 範本	1917
進一步了解 CloudFormation	1918
訂閱公告	1918
Amazon SNS 訊息格式	1923
停用 Security Hub CSPM	1925
安全	1927
資料保護	1927
身分與存取管理	1928
法規遵循驗證	1956
恢復能力	1956
基礎設施安全性	1957
VPC 端點 (AWS PrivateLink)	1957
記錄 API 呼叫	1959
CloudTrail 中的 Security Hub CSPM 資訊	217
範例：Security Hub CSPM 日誌檔案項目	217
標記資源	1962
標記基本概念	1962
在 IAM 政策中使用標籤	1963

將標籤新增至資源	1964
編輯 資源的標籤	1966
檢閱 資源的標籤	1968
移除資源的標籤	1970
配額	1972
最大配額	1972
費率配額	1972
文件歷史紀錄	1973
.....	mmlvii

什麼是 Security Hub 和 Security Hub CSPM ？

AWS Security Hub 和 AWS Security Hub CSPM AWS 服務 可保護您的雲端環境。服務互相補充。搭配使用時，它們可提供您 AWS 環境安全狀態的寶貴洞見。

[Security Hub CSPM](#) 提供安全狀態的完整檢視，並協助您根據安全產業標準和最佳實務評估雲端環境。[Security Hub](#) 提供統一的體驗，協助您排定優先順序並回應重大安全問題。Security Hub CSPM 調查結果會自動路由到 Security Hub，它們與其他安全服務的問題清單相關聯，例如 Amazon Inspector，以產生公開。這可協助您識別環境中最關鍵的風險。Security Hub 也提供自動化工作流程功能，可協助您將 Security Hub CSPM 調查結果納入您的操作工作流程。

最佳實務是，建議您啟用這兩個服務。如果您的主要重點是識別錯誤設定和評估您的安全狀態，則可以啟用 Security Hub CSPM，而無需啟用 Security Hub。不過，如果您在未啟用 Security Hub CSPM 的情況下啟用 Security Hub，Security Hub 就無法使用 Security Hub CSPM 調查結果來提供環境中 AWS 風險與暴露的相關資訊。為了獲得最佳體驗，我們建議您不僅啟用 Security Hub 和 Security Hub CSPM，也啟用這些其他安全服務：[Amazon GuardDuty](#)、[Amazon Inspector](#) 和 [Amazon Macie](#)。

AWS Security Hub 簡介

AWS Security Hub 是統一的雲端安全解決方案，可排定關鍵安全問題的優先順序，並協助您大規模回應。Security Hub 透過自動關聯和豐富來自多個來源的安全訊號來偵測安全問題，例如狀態管理、漏洞管理 (Amazon Inspector)、敏感資料 (Amazon Macie) 和威脅偵測 (Amazon GuardDuty)。這可讓安全團隊透過自動化分析和情境洞察，優先考慮其雲端環境中的主動風險。透過直覺式視覺化，Security Hub 會將複雜的安全訊號轉換為可行的洞見，讓您能夠快速做出有關安全性的明智決策。Security Hub 也包含自動化回應工作流程，協助您修復風險、提高團隊生產力，並將營運中斷降至最低。

功能

統一安全解決方案

在統一的雲端安全解決方案中，透過集中式管理，在整個雲端環境中獲得更廣泛的可見性。

可行的安全洞見

透過進階分析取得可行的安全洞見，以了解與您環境相關的安全風險。

減少回應時間

使用自動化工作流程和整合的票證系統來簡化回應時間。

公開調查結果

Security Hub 會關聯來自 Security Hub CSPM 控制檢查、Amazon Inspector 和其他的調查結果，AWS 服務以偵測與 AWS 資源相關的暴露。

未使用的存取分析

Security Hub 會自動識別 90 天內未使用的 IAM 角色、使用者、存取金鑰和許可。當您啟用 Security Hub 時，服務會在您的帳戶中建立服務連結的 IAM Access Analyzer。未使用的存取調查結果會反白顯示過度佈建的 IAM 主體，協助您實作最低權限的存取。對於未使用的許可調查結果，Security Hub 可以產生最低權限政策建議，以顯示縮小範圍的取代政策。

調查結果在開放式網路安全結構描述架構 (OCSF) 中格式化

Security Hub 在 OCSF 中產生調查結果，並從 Security Hub CSPM 和其他收到 OCSF 中的調查結果 AWS 服務：

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

儀表板

Security Hub 主控台可全面檢視您的暴露、威脅、安全涵蓋範圍和資源，以及稱為攻擊路徑圖的互動式視覺化，其中顯示潛在攻擊者如何存取和控制與暴露調查結果相關的資源。

與第三方產品的整合

您可以使用 Security Hub 整合來增強您的安全狀態。例如，如果您使用 Jira Cloud 或 ServiceNow ITSM，您可以使用此功能從問題清單建立票證。

整合

Security Hub 會收到下列問題清單 AWS 服務。

- AWS Security Hub CSPM
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- IAM Access Analyzer

Accessibility

Security Hub 適用於大多數 AWS 區域。如需目前可使用 Security Hub 的區域清單，請參閱 [《》中的 Security Hub 端點和配額](#) AWS 一般參考。如需有關 AWS 區域 管理的資訊 AWS 帳戶，請參閱《AWS 帳戶管理 參考指南》中的 [指定 AWS 區域 您的帳戶可以使用哪些](#)。

您可以為組織中的個別帳戶或帳戶啟用 Security Hub。在每個區域中，您可以透過下列任何方式存取和使用 Security Hub：

Security Hub 主控台

Security Hub 主控台是瀏覽器型界面，可用來建立和管理 AWS 資源。在此主控台中，您可以存取您的帳戶、資料和資源。

Security Hub API

Security Hub API 可讓您以程式設計方式存取您的帳戶、資料和資源。您可以直接將 HTTPS 請求傳送至 Security Hub。

AWS CLI

使用 [AWS CLI](#)，您可以在系統命令列中執行命令，以執行任務並建置執行任務的指令碼。在某些情況下，AWS CLI 可能比 Security Hub 主控台更實用。

AWS SDKs

[AWS SDKs](#) 包含適用於各種程式設計語言和平台 (C++、Go、Java、.NET 和 Python) 的程式庫和範本程式碼。它們以您偏好的語言提供 Security Hub 和其他 AWS 服務的程式設計存取權，並可協助您管理任務，例如管理錯誤、簽署請求和重試請求。

定價

Security Hub 概念

在 Security Hub 中，我們以常見的 AWS 概念和術語為基礎，並使用這些額外的術語。

帳戶

包含資源的標準 AWS 帳戶 AWS。AWS 使用您的 AWS 帳戶登入以啟用 Security Hub。

如果您的帳戶已註冊 AWS Organizations，您的組織會指定 Security Hub 管理員帳戶。此帳戶可以啟用其他組織帳戶做為成員帳戶。

組織只能有一個管理員帳戶。帳戶不能同時是管理員帳戶和成員帳戶。

Security Hub 支援下列帳戶：

- 組織管理帳戶 — 管理 AWS 組織的 AWS 帳戶。
- 委派管理員帳戶 — 管理 AWS 服務 AWS 組織使用 AWS 的帳戶。
- 成員帳戶 — AWS 為 AWS 組織成員的帳戶。
- 獨立帳戶 — 未 AWS Organizations 啟用 AWS 的帳戶

管理員帳戶

這種類型的 AWS 帳戶可以檢視相關聯成員帳戶的調查結果。

當組織管理帳戶將帳戶指定為 Security Hub 管理員帳戶時，此類型的帳戶 AWS 會成為管理員帳戶。Security Hub 管理員帳戶可以將任何組織帳戶啟用為成員帳戶，也可以邀請其他帳戶成為成員帳戶。

組織只能有一個管理員帳戶。帳戶不能同時是管理員帳戶和成員帳戶。

彙總區域

彙總區域可讓您在 AWS 區域 單一玻璃窗格中檢視來自多個 的安全調查結果。

彙總區域是您檢視和管理問題清單 AWS 區域 的。調查結果會從連結的區域彙總到彙總區域中。更新的問題清單會跨區域複寫。

在彙總區域中，儀表板和庫存頁面包含來自所有連結區域的資料。自動化頁面只能用來定義彙總區域中的自動化規則。第三方票證整合只能在彙總區域中設定。

已封存的問題清單

狀態為 的調查結果ARCHIVED。這些調查結果指出調查結果提供者或調查調查結果的客戶認為調查結果不再相關。

問題清單提供者可以封存他們建立的問題清單。客戶可以使用 Security Hub API 的 [BatchUpdateFindingsV2](#) 操作或在 Security Hub 主控台中更新狀態，來封存他們認為不再相關的任何問題清單。

在 Security Hub 主控台中，預設篩選條件設定會從問題清單和資料表中排除封存的問題清單。您可以更新篩選條件，以包含封存的問題清單。如果您使用 [GetFindingsV2](#) 操作擷取問題清單，該操作會同時擷取封存和作用中的問題清單。下列範例顯示如何在結果中排除封存的問題清單。

```
{
  "StringFilters":
  [
    {
      "FieldName": "status",
      "Filter":
      {
        "Value": "Archived",
        "Comparison": "EQUALS"
      }
    }
  ]
}
```

跨區域彙總

從連結區域將問題清單和資源彙總到彙總區域。您可以從彙總區域檢視所有資料，並從彙總區域更新問題清單。

委派管理員帳戶

在 **中** AWS Organizations，服務的委派管理員帳戶可以管理組織的服務使用。

在 Security Hub 中，Security Hub 管理員帳戶也是 Security Hub 的委派管理員帳戶。當組織管理帳戶首次指定 Security Hub 管理員帳戶時，Security Hub 會呼叫 Organizations 將該帳戶設為委派管理員帳戶。

然後，組織管理帳戶必須選擇委派管理員帳戶作為所有區域中的 Security Hub 管理員帳戶。

曝光

暴露是安全控制、設定錯誤或其他可能被作用中威脅利用之區域的更廣泛弱點。

公開的範例包括：

- 資源的控制平面設定錯誤。
- 存在具有高可利用性可能性的軟體漏洞。
- 可公開存取的資源（網路或 API）。

暴露問題清單

一種問題清單類型，描述存在於您環境中的公開。曝光問題清單包含特徵和訊號。訊號可以包含一或多個類型的曝光特徵。AWS 當來自 Security Hub CSPM、Amazon Inspector、Amazon GuardDuty、Amazon Macie 或其他 AWS 服務的訊號指出存在暴露時，AWS Security Hub 會產生暴露調查結果。資源可以參與一或多個暴露問題清單。如果資源沒有任何暴露特徵或特徵不足，Security Hub 不會為該資源產生暴露調查結果。

公開調查結果的範例為：可從網際網路連線的 EC2 執行個體，且具有高度攻擊的軟體漏洞。

問題清單

安全檢查或安全性相關偵測的可觀察記錄。Security Hub 透過其他安全調查結果的相互關聯產生和更新調查結果。這些稱為暴露問題清單。問題清單也可以來自與其他 AWS 服務 和第三方產品的整合。

尋找擷取

將問題清單匯入 Security Hub。調查結果擷取事件包括新調查結果和現有調查結果的更新。

連結的區域

當您啟用跨區域彙總時，連結的區域是將問題清單和資源庫存彙總至彙總區域的區域。

在連結的區域中，儀表板和庫存頁面僅包含該區域的調查結果 AWS 區域。

開放式網路安全結構描述架構 (OCSF)

[Open Cybersecurity 結構描述架構 \(OCSF\)](#) 是網路安全產業中 AWS 和 領導合作夥伴的協作、開放原始碼工作。OCSF 為常見安全事件提供標準結構描述、定義版本控制條件以促進結構描述演變，並包含安全日誌生產者和消費者的自我監管程序。如需詳細資訊，請參閱 [Security Hub 中的 OCSF 問題清單](#)。

成員帳戶

AWS 帳戶 授予管理員帳戶檢視其問題清單並對其採取動作的許可。當 Security Hub 管理員帳戶將其啟用為成員帳戶時，這種類型的 AWS 帳戶 會成為成員帳戶。

訊號

有助於公開調查結果的問題清單。訊號可以稱為貢獻調查結果。訊號可以源自 Security Hub CSPM AWS Config或其他 AWS 服務，例如 Amazon Inspector。

服務連結組態記錄器

一種 AWS Config 記錄器類型，用於記錄服務特定資源上的組態資料。Security Hub 以事件驅動的方式使用這些記錄器，以取得暴露分析涵蓋範圍、資源庫存報告和狀態管理控制評估的資源組態項目。此功能會作為基本計劃定價的一部分提供給所有 Security Hub 客戶。啟用 Security Hub 後，會在您的帳戶中建立下列服務連結組態記錄器：

- 在每個 AWS 帳戶 和 中 AWS 區域，AWSConfigurationRecorderForSecurityHubAssets都會建立名為 的服務連結組態記錄器。
- 對於全域資源類型，名為 的額外服務連結組態記錄器AWSConfigurationRecorderForSecurityHubAssetsGlobal會在 us-east-1 中建立 AWS 區域。

服務連結分析器

Security Hub 代表您建立和管理的 IAM Access Analyzer。當您啟用 Security Hub 時，會自動建立服務連結未使用的存取分析器，以識別 90 天回顧期間內未使用的 IAM 角色、使用者、存取金鑰和許可。分析器會在美國東部（維吉尼亞北部）執行，因為 IAM 是全球服務。Security Hub 會將未使用的存取調查結果複寫到您已啟用 Security Hub 的所有區域。您不需要單獨啟用 IAM Access Analyzer 或採取任何其他動作。此功能會作為基本計劃定價的一部分提供給所有 Security Hub 客

戶。您可以在 IAM Access Analyzer 主控台中檢視服務連結分析器，但您無法在 Security Hub 啟用時修改或刪除它。當您在的所有區域中停用服務時，Security Hub 會刪除分析器 AWS 帳戶。如需詳細資訊，請參閱[the section called “未使用的存取權調查結果”](#)。

特徵

導致暴露問題清單的安全偏差。特性類型包括假設性、設定錯誤、可達性、敏感資料和漏洞。特徵與一個訊號相關聯，且訊號可以包含多個特徵。例如，Security Hub CSPM 控制項表示客戶受管政策允許管理存取控制。此訊號包含組態錯誤特性。

未使用的存取問題清單

識別在 90 天回顧期間內未使用的 IAM 角色、使用者、存取金鑰或一組許可的問題清單。Security Hub 會使用服務連結的 IAM Access Analyzer 產生未使用的存取調查結果。未使用的存取調查結果有四種類型：未使用的 IAM 角色、未使用的 IAM 使用者存取金鑰、未使用的 IAM 使用者密碼，以及未使用的許可。

AWS Security Hub 成本估算器

Security Hub 成本估算器是一種主控台功能，可提供整個 AWS 環境功能的預估值。成本估算器會顯示您在 AWS Security Hub CSPM、Amazon Inspector 和 Amazon GuardDuty 中的個別服務成本，以及您透過 Security Hub 的簡化定價計劃在 Security Hub 中的預估成本。您可以調整預估用量和資源計數，以符合您的 AWS 用量，以提高預估的準確性。成本估算器可在 Security Hub 可用的所有區域使用。

成本估算器會使用兩種定價模型來估計安全功能的每月成本：

- 個別服務定價 – 分別支付每個安全功能的費用 (GuardDuty、Amazon Inspector、Security Hub CSPM)。
- Security Hub 簡化定價 – 跨 3 個定價計劃的統一定價、具有每個資源定價的基本計劃、具有每個事件和每個 GB 日誌定價的威脅分析，以及具有每個資源定價的 Lambda 程式碼掃描。

估算器會在可用時使用 AWS Cost Explorer 資料。當 Cost Explorer 資料無法使用時，您可以手動輸入用量資料。成本估算是根據觀察和使用者提供的用量，以及公有定價資訊。估算可能不會反映企業折扣。

成本估算器的主要優點包括：

- 了解啟用 Security Hub 時，如何在不啟用 Security Hub 的情況下，將成本與個別服務進行比較

- 在啟用 功能之前估計成本
- 調整用量參數以建立不同案例的模型
- 將預估匯出為 PDF 以供利益相關者檢閱

依帳戶類型存取

Note

對於委派管理員和成員帳戶，成本估算器預設會在編輯模式下開啟，讓您可以立即輸入用量資料。當 Cost Explorer 資料可用時，管理帳戶和獨立帳戶會在檢視模式中開啟。

此功能會自動擷取實際過去用量的相關資訊，以估計特定帳戶類型的成本。如需每個帳戶類型的詳細資訊，以及每個帳戶類型可用的資料，請參閱下文。

依帳戶類型存取許可

帳戶類型	Cost Explorer 資料	資料輸入	Scope (範圍)
管理帳戶 (MA)	自動填入	可用的手動覆寫	整個組織
委派管理員 (DA)	透過跨帳戶角色自動填入*	可用的手動覆寫	整個組織
成員帳戶	透過跨帳戶角色自動填入*	可用的手動覆寫	整個組織
獨立帳戶 (SA)	自動填入	可用的手動覆寫	單一帳戶

* 管理帳戶中需要跨帳戶 IAM 角色組態。請參閱以下[設定跨帳戶存取權](#)章節。

先決條件

所需的 IAM 許可

若要使用所有成本估算器的容量，您的 IAM 主體必須具有下列許可：

成本估算器所需的 IAM 許可

API 作業	服務	用途
<code>ce:GetCostAndUsage</code>	AWS Cost Explorer	擷取歷史用量和成本資料
<code>pricing:GetProducts</code>	AWS 定價	取得目前的定價費率
<code>organizations:ListAccounts</code>	AWS 組織	計算組織中的帳戶
<code>organizations:DescribeOrganization</code>	AWS 組織	判斷帳戶類型
<code>securityhub:ListOrganizationAdminAccounts</code>	Security Hub	列出組織管理員帳戶
<code>iam:GetRole</code>	IAM	檢查跨帳戶角色是否存在（僅限管理帳戶）*
<code>sts:AssumeRole</code>	IAM	擔任跨帳戶角色（僅限委派管理員/成員帳戶）**

* 只有在 Management Account 使用者驗證跨帳戶角色狀態時才需要。

** 僅適用於使用跨帳戶存取的委派管理員和組織成員帳戶。

其他需求

Cost Explorer

必須為自動資料入口啟用（啟用後 24 小時處理延遲）。

設定跨帳戶存取權

委派管理員和成員帳戶可以透過設定跨帳戶 IAM 角色，從管理帳戶存取整個組織 AWS Cost Explorer 的資料。此組態可讓這些帳戶檢視實際用量資料，而無需切換到管理帳戶。

先決條件

在設定成本估算器的跨帳戶存取之前，需要下列項目和資訊：

- 管理帳戶必須 AWS Cost Explorer 已啟用。
- 在管理帳戶中建立角色的 IAM 許可。
- 知道將授予跨帳戶存取權的委派管理員或成員帳戶 ID。

設定步驟

成本估算器直接在主控台中提供引導式設定指示。若要存取指示，請前往您組織管理帳戶中位於 <https://console.aws.amazon.com/securityhub/v2/home#/costEstimator> 的成本估算器頁面。找到跨帳戶存取區段，並依照概述的步驟設定跨帳戶角色。

角色組態

成本估算器的跨帳戶存取需要設定具有信任政策和許可政策的 IAM 角色。必須在具有下列組態的管理帳戶中建立跨帳戶角色：

角色名稱（需要確切名稱） – `AwsSecurityHubCostEstimatorCrossAccountRole`

建議的信任政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{ACCOUNT_ID}:role/{ROLE_NAME}"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

透過取代政策範例中的下列值來編輯政策：

- 將 `{ACCOUNT_ID}` 取代為您授予跨帳戶存取權的委派管理員或成員帳戶 ID。
- 在您授予存取權的委派管理員或成員帳戶中，以 IAM 角色名稱取代 `{ROLE_NAME}`。

建議的許可政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ce:GetCostAndUsage",
      "Resource": "*"
    }
  ]
}
```

Note

信任政策限制對特定帳戶和角色的存取。只有指定的 IAM 主體可以擔任此角色，防止未經授權的存取。

驗證

在管理帳戶中建立角色之後，請使用下列步驟來確認設定是否正常運作。

1. 登入委派管理員或成員帳戶。
2. 前往位於 <https://console.aws.amazon.com/securityhub/v2/home#/costEstimator> 的 Security Hub 成本估算器
3. 頁面應該會自動：
 - a. 偵測組織中的管理帳戶。
 - b. 擔任跨帳戶角色。
 - c. 使用整個組織的用量載入 Cost Explorer 資料。

如果成功，您會看到實際用量資料，而不是手動輸入欄位。

疑難排解

本節涵蓋設定跨帳戶存取時可能發生的常見問題和解決方案。

此帳戶無法使用組織用量資料

此提醒表示無法存取跨帳戶角色。此提醒的可能原因包括：

1. 角色不存在：管理帳戶尚未建立角色。
 - 解決方案：請聯絡您的管理帳戶管理員，以使用設定指引建立角色。
2. 角色名稱不相符：角色名稱不完全相符。
 - 解決方案：驗證角色名稱為 `AwsSecurityHubCostEstimatorCrossAccountRole`。
3. 信任政策不正確：信任政策不允許您的帳戶擔任該角色。
 - 解決方案：驗證信任政策包含您的帳戶 ID 和角色名稱。
4. 缺少 AssumeRole 許可：您的 IAM 主體缺少 `sts:AssumeRole`。
 - 解決方案：請聯絡您的管理員以新增 `sts:AssumeRole` 許可。

若要檢視詳細設定指示：請按一下提醒中的「檢視指示」連結，以 step-by-step 指引和政策範本的狀態。

解決方法：您仍然可以在編輯模式中手動輸入用量值，以使用成本估算器。

使用成本估算器

存取成本估算器

從 Security Hub 登陸頁面存取成本估算器

1. 使用您的 AWS 組織管理或委派管理員 AWS 帳戶登入資料登入您的帳戶。在 us-east-1 區域中開啟 Security Hub 主控台，網址為 <https://console.aws.amazon.com/securityhub/v2/home>。
2. 在登陸頁面上，找到 定價卡。
3. 選擇預估成本。

在 Security Hub 啟用和組態步驟期間存取成本估算器

1. 在加入界面的新 Security Hub 卡中尋找定價。
2. 選擇檢視預估值。

從 GuardDuty、Amazon Inspector 或 Security Hub CSPM 主控台存取成本估算器

1. 導覽至服務儀表板或摘要頁面。
2. 選擇定價資訊卡中的比較定價。

了解成本估算器界面

頁面配置

成本估算器頁面包含三個主要區段：

- 概觀區段 – 說明統一的安全管理和成本最佳化優勢。
- 定價資訊 – 具有功能類別和定價方案的可擴展面板。
- 定價比較表 – Side-by-side 成本比較。

定價比較表

資料表標頭包含檢視/編輯模式控制項和重設選項。資料表會以兩欄顯示成本：

- 個別服務 – 個別安全服務的目前或預估成本。
- Security Hub – 使用簡化定價模型預估成本。

定價區域

第一欄會顯示定價內容資訊，包括預估使用 us-east-1 定價進行計算的備註。徽章表示預估中不包含企業折扣。

檢視成本估算

使用成本估算器時，您可以檢視、編輯、重設和匯出預估值。

根據預設，成本估算器會在檢視模式中開啟。

檢視成本估算

1. 使用中所說的其中一種方法存取成本估算器 [存取成本估算器](#)。
2. 檢閱摘要列中的每月總成本。
3. 檢閱功能群組及其詳細成本明細。
4. 選擇功能名稱以檢視快顯視窗中的描述。

檢視模式中的資料來源

估算器會顯示來自多個來源的資料，以標籤表示：

- 預設 – 來自 AWS Cost Explorer（過去 30 天）的資料。
- \$-/mo – 無法使用成本資料（當 Cost Explorer 無法存取時顯示）。
- 自訂用量 – 使用者輸入的值。
- 未啟用 – 當 Cost Explorer 許可不存在時顯示。

帳戶特定的行為

以下說明成本估算器如何跨不同類型的帳戶和組態運作。

委派管理員和成員帳戶

設定跨帳戶存取時：

- Cost Explorer 資料可供整個組織使用。
- 預設在檢視模式中開啟（與管理帳戶相同）。可以切換到編輯模式來修改預估值。

未設定跨帳戶存取：

- 警示顯示：「組織用量資料不適用於此帳戶」。
- 根據預設，手動項目會以編輯模式開啟。
- 按一下提醒中的「檢視指示」以取得設定指引。

管理帳戶

建立跨帳戶角色時：

- 「跨帳戶存取」區段顯示設定的狀態。
- 顯示建議用於驗證的政策。
- 提供在 IAM 主控台中檢視角色的連結。

未建立跨帳戶角色：

- 「跨帳戶存取」區段會顯示設定指南。

- 提供預先填入政策的step-by-step說明。
- 直接連結至 IAM 主控台以建立角色。

無法驗證角色狀態：

- 如果沒有呼叫 的許可iam:GetRole，主控台無法判斷您是否已建立必要的角色。
- 顯示「無法驗證」與對應的錯誤訊息。

獨立帳戶

未建立跨帳戶角色：

- 現有行為沒有變更。
- 啟用時，可以使用 Cost Explorer 資料。
- 預設在檢視模式中開啟。

編輯用量值

編輯模式可讓您修改維度值，並查看即時成本更新。

編輯用量值

1. 在資料表標頭中選擇編輯。
2. 在維度輸入欄位中輸入值。
3. 自動檢視更新後的成本。
4. 選擇檢視以返回檢視模式。

Important

- 當您離開成本估算器頁面時，不會儲存編輯
- 修改後的預估使用 us-east-1（維吉尼亞北部）定價，不包含企業折扣
- 在「僅顯示目前成本」模式中編輯 會自動切換回預估模式

重設估算器

此動作會清除所有自訂值，並從 Cost Explorer 重新載入預設資料。

將所有值重設為預設值

1. 在資料表標頭中選擇重設。
2. 在確認對話方塊中，選擇重設。

匯出預估值

在成本估算器中，您預估的資料可以匯出至 PDF 檔案。

匯出成本估算

1. 確保您處於檢視模式。
2. 在頁面標頭中選擇下載 PDF。

PDF 會自動下載，檔案名稱為：SecurityHub-Cost-Estimate-YYYY-MM-DD.pdf。

疑難排解

本節涵蓋使用成本估算器時可能發生的常見問題和解決方案

沒有可用的 Cost Explorer 資料

問題

提醒會顯示「您的帳戶沒有可用的成本資料」。

依帳戶類型列出的解決方案

解決方案取決於您的帳戶類型：

遺失 Cost Explorer 資料的解決方案

帳戶類型	解決方案
管理帳戶	啟用 Cost Explorer 並等待 24 小時以進行資料處理

帳戶類型	解決方案
委派的管理員	聯絡 Management Account 管理員以請求存取
成員帳戶	聯絡 管理帳戶或委派管理員進行存取
獨立帳戶	啟用 Cost Explorer 並等待 24 小時以進行資料處理

解決方法

在編輯模式中輸入自訂值。

跨帳戶存取無法運作

問題

「委派的管理員或成員帳戶會顯示「組織用量資料不適用於此帳戶」提醒。

可能的原因和解決方案

1. 管理帳戶中不存在跨帳戶角色。
 - a. 解決方案：聯絡 管理帳戶管理員以建立角色。
 - b. 成本估算器提供管理帳戶使用者的引導式設定指示。
2. 角色名稱不完全相符。
 - a. 必要角色名稱：AwsSecurityHubCostEstimatorCrossAccountRole。
 - b. 解決方案：確認 IAM 主控台的角色名稱完全相符（區分大小寫）。
3. 信任政策不允許您的帳戶。
 - a. 解決方案：驗證信任政策主體包含您的帳戶 ID 和角色名稱。
 - b. 格式：arn:aws:iam::{YOUR_ACCOUNT_ID}:role/{YOUR_ROLE_NAME}。
4. 缺少 AssumeRole 許可。
 - a. 解決方案：確認您的 IAM 主體具有 sts:AssumeRole 許可。
 - b. 授權您的 AWS 管理員以新增此許可。

解決方法：

在編輯模式中輸入自訂值，以手動估算沒有 Cost Explorer 資料的成本。

取得詳細說明

- 按一下提醒中的「檢視指示」連結，以開啟具有下列項目的模態：
 - Step-by-step設定指引
 - 預先填入的政策範本
 - 針對錯誤的特定秘訣進行故障診斷

許可錯誤

問題

特定 API 操作的「拒絕存取」錯誤。

解決許可錯誤

1. 請注意錯誤訊息中的拒絕操作（例如 `ce:GetCostAndUsage`）。
2. 選擇複製以複製錯誤詳細資訊。
3. 將錯誤詳細資訊傳送給您的 AWS 管理員。
4. 請求 中列出的必要 IAM 許可[所需的 IAM 許可](#)。

Note

您仍然可以使用編輯模式在缺少許可時輸入手動值，除非定價 API 存取遭拒（防止所有成本估算）。

功能顯示「未啟用」

問題

功能會顯示「未啟用」狀態。

說明

當您擁有 Cost Explorer 存取權但功能目前未處於作用中狀態時，就會顯示此狀態。如果您改為看到 \$-/mo，這表示您的帳戶類型無法使用 Cost Explorer 資料。

檢視成本估算

1. 選擇編輯以進入編輯模式。
2. 輸入 功能的維度值。
3. 檢視更新後的成本預估。

功能顯示「不適用」

問題

功能會在個別服務欄中顯示「不適用」。

說明

此功能只能透過 Security Hub 簡化定價使用，不能作為獨立服務。

修改後的成本與 Cost Explorer 不符

問題

編輯後的成本與原始 Cost Explorer 值不同。

說明

修改後的預估使用 us-east-1（維吉尼亞北部）定價費率，不包含企業折扣。Cost Explorer 資料會反映實際成本和適用的折扣。

重要說明

- 估算是根據觀察和使用者提供的用量，以及公有定價資訊 – 實際成本可能會根據用量模式和企業協議而有所不同
- 30 天回顧 – Cost Explorer 資料反映過去 30 天的用量
- 定價區域 – 所有預估都使用 us-east-1（維吉尼亞北部）費率
- 不會影響設定 – 估算器的變更不會影響您目前的 Security Hub 或服務組態
- 企業折扣 – 修改後的預估不包含企業折扣；只有 Cost Explorer 資料反映實際的折扣成本
- 資料重新整理 – Cost Explorer 資料每日更新；重新整理頁面以查看最新資料

相關資訊

- [AWS Security Hub 定價](#)
- [AWS Cost Explorer 使用者指南](#)
- [AWS 定價 API 參考](#)
- [啟用 Security Hub](#)

啟用 Security Hub

您可以為任何 啟用 Security Hub AWS 帳戶。文件的本節說明為 AWS 組織或獨立帳戶啟用 Security Hub 所需的所有步驟。

如需如何啟用 Security Hub 的簡短示範，請觀看以下影片：[Security Hub 入門演練和示範](#)。

為 AWS 組織啟用 Security Hub

本節包含三個步驟：

- 在步驟 1 中，AWS 組織管理帳戶會為其 AWS 組織指定委派管理員、建立委派管理員政策，並選擇性地為其自己的帳戶啟用 Security Hub。
- 在步驟 2 中，組織的委派管理員會為其自己的帳戶啟用 Security Hub。

- 在步驟 3 中，組織的委派管理員會為 Security Hub 和其他支援的安全服務設定組織中的所有成員帳戶。

步驟 1. 委派管理員帳戶，並選擇性地在 AWS 組織管理帳戶中啟用 Security Hub

Note

此步驟只需要在組織管理帳戶的一個區域中完成。

為 Security Hub 指派委派管理員帳戶時，您可以為委派管理員選擇的帳戶將取決於您如何為 Security Hub CSPM 設定委派管理員。如果您已為 Security Hub CSPM 設定委派管理員，且該帳戶不是組織管理帳戶，則該帳戶將自動設定為 Security Hub 委派管理員，且無法選擇不同的帳戶。如果 Security Hub CSPM 的委派管理員帳戶設定為組織管理帳戶，或完全未設定，您可以選擇哪個帳戶將成為您的 Security Hub 委派管理員帳戶，組織管理帳戶除外。

如需在 Security Hub 中指定委派管理員的資訊，請參閱[在 Security Hub 中指定委派管理員帳戶](#)。如需有關在 Security Hub 中建立委派管理員政策的資訊，請參閱[在 Security Hub 中建立委派管理員政策](#)。

指定 Security Hub 的 administrator

1. 使用您的 AWS 組織管理 AWS 帳戶登入資料登入您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 在 Security Hub 首頁中，選取 Security Hub，然後選擇開始使用。
3. 在委派管理員區段中，根據提供的選項選擇管理員帳戶。最佳實務是，我們建議在安全服務之間使用相同的委派管理員，以實現一致的控管。
4. 選擇信任存取核取方塊。選擇此選項可授予您的委派管理員帳戶在成員帳戶中設定特定功能的能力，例如 GuardDuty 惡意軟體防護。如果您取消勾選此選項，Security Hub 將無法代表您啟用這些功能，而且您將需要直接透過與功能相關聯的服務啟用這些功能。
5. （選用）針對帳戶啟用，選取方塊以啟用您 AWS 帳戶的 Security Hub。
6. 針對委派管理員政策，選擇下列其中一個選項來新增政策陳述式。
 - a. （選項 1）選擇為我更新此項目。選取政策陳述式下的方塊，確認 Security Hub 會自動建立委派政策，將所有必要的許可授予委派管理員。
 - b. （選項 2）選擇我想要手動連接此項目。選擇複製並連接。在 AWS Organizations 主控台的委派管理員 AWS Organizations 下，選擇委派，然後在委派政策編輯器中貼上資源政策。選擇建立政策。開啟您在 Security Hub 主控台標籤。

7. 選擇設定。

步驟 2. 在委派管理員帳戶中啟用 Security Hub

委派的管理員帳戶會完成此步驟。在 AWS 組織管理帳戶為其組織指定委派管理員之後，委派管理員必須先為其自己的帳戶啟用 Security Hub，才能為整個 AWS 組織啟用。

在委派管理員帳戶中啟用 Security Hub

1. 使用您的委派管理員登入 AWS 資料登入您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從 Security Hub 首頁中選擇開始使用。
3. 安全功能區段概述自動啟用的功能，並包含在 Security Hub 的每個資源基本價格中
4. （選用）對於標籤，判斷是否要將鍵/值對新增至帳戶設定。
5. 選擇啟用 Security Hub 以完成啟用 Security Hub。
6. （建議）從彈出視窗中選擇設定我的組織並繼續步驟 3。

步驟 3. 建立在所有成員帳戶中啟用 Security Hub 的政策

在組織的委派管理員帳戶中使用 Security Hub 後，您需要建立政策，以定義在組織成員帳戶中啟用哪些服務和功能。如需詳細資訊，請參閱[啟用具有政策類型的組態](#)。

啟用 Security Hub 後，會在您的帳戶中建立下列資源：

- 稱為 [AWSServiceRoleForSecurityHubV2](#) 的服務連結角色。
- 服務連結組態記錄器。如需詳細資訊，請參閱 Security Hub 概念文件中[的服務連結記錄器](#)。
- 服務連結分析器。如需詳細資訊，請參閱 Security Hub 概念文件中[的服務連結分析器](#)。

在獨立帳戶中啟用 Security Hub

此程序說明如何在獨立帳戶中啟用 Security Hub。獨立帳戶是 AWS 帳戶 尚未啟用 AWS 組織的。

在獨立帳戶中啟用 Security Hub

1. 使用 AWS 您的帳戶登入資料登入您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。

2. 在 Security Hub 首頁中，選取開始使用。
3. 在安全功能區段中，執行下列其中一項：
 - a. (選項 1) 選擇啟用所有功能。這將開啟所有 Security Hub 基本功能、威脅分析和其他功能。
 - b. (選項 2) 選擇自訂功能。選取威脅分析和其他應開啟的功能。您無法取消選取屬於 Security Hub 基本計劃功能的任何功能。
4. 在區域區段中，選擇啟用所有區域或啟用特定區域。如果您選擇啟用所有區域，您可以決定是否自動啟用新區域。如果您選擇啟用特定區域，您必須選擇要啟用的區域。
5. (選用) 針對資源標籤，將標籤新增為鍵/值對，以協助您輕鬆識別組態。
6. 選擇 Enable Security Hub (啟用 Security Hub)。

啟用 Security Hub 後，會在您啟用服務的每個帳戶中建立下列資源：

- 稱為 [AWSServiceRoleForSecurityHubV2](#) 的服務連結角色。
- 服務連結組態記錄器。如需詳細資訊，請參閱 Security Hub 概念文件中[的服務連結記錄器](#)。
- 服務連結分析器。如需詳細資訊，請參閱 Security Hub 概念文件中[的服務連結分析器](#)。

在 Security Hub 中指定委派管理員

在 AWS 組織管理帳戶中，您可以為組織指定委派管理員。最佳實務是，我們建議在安全服務之間使用相同的委派管理員，以實現一致的控管。

本主題中的程序說明如何在 Security Hub 中指定委派管理員。它假設您之前已啟用 Security Hub，但未在啟用工作流程期間指定委派管理員。

考量事項

在 Security Hub 中指定委派管理員時，請考慮下列事項：

- AWS 組織管理帳戶可以在 Security Hub CSPM 中將自己指定為委派管理員。AWS 組織管理帳戶無法將自己指定為 Security Hub 中的委派管理員。在此案例中，AWS 組織管理帳戶必須指定另一個 AWS 帳戶做為 Security Hub 中的委派管理員。最佳實務是，我們建議在安全服務之間使用相同的委派管理員，以實現一致的控管。
- 如果 AWS 組織管理帳戶在 Security Hub CSPM 中指定委派管理員，則該委派管理員會自動成為 Security Hub 中的委派管理員。在此案例中，Security Hub 只允許此特定 AWS 帳戶做為委派管理員。

Note

如果 AWS 組織管理帳戶在 Security Hub 中使用與 Security Hub CSPM 相同的委派管理員，則透過 Security Hub CSPM 主控台或使用 AWS Organizations API 移除它也會在 Security Hub 中移除它。同樣地，透過 Security Hub 主控台或使用 AWS Organizations API 將其移除也會在 Security Hub CSPM 中移除。從 Security Hub CSPM 移除委派管理員時，中央組態會自動選擇退出。

啟用 Security Hub 後指定委派管理員

此程序供 AWS 組織管理帳戶完成。它假設 AWS 組織管理帳戶先前已啟用 Security Hub，但未在啟用工作流程期間指定委派管理員。

Note

完成此程序後，您必須建立政策，允許組織的委派管理員設定 Security Hub 並在其中執行特定動作 AWS Organizations。如需詳細資訊，請參閱[在 Security Hub 中建立委派管理員政策](#)。

在 Security Hub 中指定委派管理員

1. 使用您的組織管理 AWS 帳戶登入資料登入您的帳戶，然後開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從導覽窗格中，選擇一般。
3. 在委派管理員中，選擇設定。選取其中一個提供的 AWS 帳戶，或輸入 AWS 帳戶您要指定為組織委派管理員之的 12 位數 AWS 帳戶號碼。選擇儲存。

在 Security Hub 中建立委派管理員政策

AWS 組織管理帳戶可以建立政策，允許委派管理員設定 Security Hub 並在其中執行特定動作 AWS Organizations。本主題中的程序說明如何建立政策。完成程序時，您可以允許 Security Hub 為您建立政策或手動建立政策。建議您允許 Security Hub 為您建立政策，除非您想要針對特定使用案例自訂政策。AWS 組織管理帳戶只有在啟用 Security Hub 並指定委派管理員，但在完成[啟用](#)工作流程時略過建立政策時，才必須完成此程序。如需如何更新此政策的資訊，請參閱AWS Organizations 《使用者指南》中的[使用 更新資源型委派政策 AWS Organizations](#)。

Note

完成此程序後，委派管理員可以建立政策，允許其管理組織中的成員帳戶。如需詳細資訊，請參閱[建立政策做為委派管理員來管理成員帳戶](#)。

建立委派管理員政策

1. 使用您的組織管理 AWS 帳戶登入資料登入您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從導覽窗格中，選擇一般。
3. 對於委派的管理員政策，請執行下列其中一項操作：
 - a. (選項 1) 選擇建立政策。選取政策陳述式下的方塊，確認 Security Hub 會自動建立委派政策，將所有必要的許可授予委派管理員。
 - b. (選項 2) 開啟政策。選擇複製並連接。在 AWS Organizations 主控台的委派管理員 AWS Organizations 下，選擇委派，然後在委派政策編輯器中貼上資源政策。選擇建立政策。開啟您在 Security Hub 主控台標籤，然後選擇設定。

管理 AWS 組織中成員帳戶的組態

AWS 組織的委派管理員可以跨成員帳戶和區域設定安全功能。有兩種可用的組態類型：政策和部署。政策會為 AWS Security Hub 和 Amazon Inspector 的帳戶和區域產生 AWS Organizations 政策。部署是一種一次性動作，可在 Amazon GuardDuty 和 AWS Security Hub CSPM 的所選帳戶和區域中啟用安全功能。與政策不同，您無法檢視或編輯部署，且部署不適用於新啟用的帳戶。Amazon GuardDuty 和 AWS Security Hub CSPM 提供適用於新成員帳戶的自動啟用功能。

Security Hub 組態目錄

Security Hub 的組態目錄提供多種選項，以協助為提供的安全功能設定您的 AWS Organization 帳戶。

以下是 Security Hub 組態目錄中可用的選項。

Security Hub (基本和其他功能)

這是針對 Security Hub 部署的建議組態。

類型：政策和部署

描述：此組態在 Security Hub 的基本安全管理、狀態管理、威脅分析和漏洞管理功能上產生錯誤。它可選擇性地啟用其他功能。

來自 GuardDuty 的威脅分析

類型：部署

描述：開啟選取的 Amazon GuardDuty 功能，以持續監控、分析和處理 AWS 環境中的 AWS 資料來源和日誌。

Security AWS Hub CSPM 中的狀態管理)

類型：部署

描述：此組態會開啟 Security Hub CSPM 的標準和控制項，以偵測 AWS 您的帳戶和資源何時偏離安全最佳實務。

Amazon Inspector 的漏洞管理

類型：政策

描述：此組態會開啟選取的 Amazon Inspector 功能，以自動探索工作負載、執行個體、容器映像等，並掃描它們是否有漏洞和網路暴露。

啟用具有 政策類型的組態

下列程序說明如何為 AWS Organization 帳戶建立具有 政策類型的組態。若要建立組態政策，必須在 AWS 組織管理帳戶中建立委派的管理員政策。如需有關在 Security Hub 中建立委派管理員政策的資訊，請參閱[在 Security Hub 中建立委派管理員政策](#)。

建立啟用和停用成員帳戶的政策

1. 使用您的 AWS 帳戶搭配委派管理員登入資料來登入。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從導覽窗格中，選擇管理，然後選擇組態。
3. 從組態目錄中選擇具有政策或政策類型和部署的項目。若要完整設定 Security Hub，建議您選擇 Security Hub（基本和其他功能）。
4. 在詳細資訊區段的設定 Security Hub 頁面上，輸入政策的名稱和描述。
5. 在安全功能區段中，執行下列其中一項操作：

- a. (選項 1) 選擇啟用所有功能。這將開啟所有 Security Hub 基本功能、威脅分析和其他功能。
 - b. (選項 2) 選擇自訂功能。選取威脅分析和其他應開啟的功能。您無法取消選取屬於 Security Hub 基本計劃功能的任何功能。
6. 在帳戶選取區段中，選取下列其中一個選項。如果您想要將組態套用至所有組織單位和帳戶，請選擇所有組織單位和帳戶。如果您想要將組態套用至特定組織單位和帳戶，請選擇特定組織單位和帳戶。如果您選擇此選項，請使用搜尋列或組織結構樹來指定要套用政策的組織單位和帳戶。如果您不想將組態套用至任何組織單位或帳戶，請選擇無組織單位或帳戶。
 7. 在區域區段中，選擇啟用所有區域、停用所有區域或指定區域。如果您選擇啟用所有區域，您可以決定是否自動啟用新區域。如果您選擇停用所有區域，您可以決定是否自動停用新區域。如果您選擇指定區域，則必須選擇要啟用和停用的區域。
 8. (選用) 如需進階設定，請參閱 [指引](#) AWS Organizations。
 9. (選用) 針對資源標籤，將標籤新增為鍵/值對，以協助您輕鬆識別組態。
 10. 選擇下一步。
 11. 檢閱您的變更，然後選擇套用。您的目標帳戶是根據政策設定。政策的組態狀態會顯示在政策頁面頂端。如果已設定或發生部署失敗，每個功能都會提供 狀態。對於任何失敗，請按一下失敗訊息的連結以查看更多詳細資訊。若要在帳戶層級檢視有效政策，您可以檢閱組態頁面上的組織索引標籤，您可以在其中選擇帳戶。

啟用具有部署類型的組態

下列程序說明如何為 AWS Organization 帳戶建立部署類型的組態。

建立啟用和停用成員帳戶的部署

1. 使用您的 AWS 帳戶搭配委派管理員登入資料來登入。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從導覽窗格中，選擇管理，然後選擇組態。
3. 從組態目錄中選擇具有部署類型的項目。若要完整設定 Security Hub，建議您選擇 Security Hub (基本和其他功能)。
4. 在安全功能區段中，選取應該開啟的安全功能。
5. 在帳戶選取區段中，選取下列其中一個選項。如果您想要將組態套用至所有組織單位和帳戶，請選擇所有組織單位和帳戶。如果您想要將組態套用至特定組織單位和帳戶，請選擇特定組織單位和帳戶。如果您選擇此選項，請使用搜尋列或組織結構樹來指定要套用政策的組織單位和帳戶。如果您不想將組態套用至任何組織單位或帳戶，請選擇無組織單位或帳戶。

6. 在區域區段中，選擇啟用所有區域、停用所有區域或指定區域。如果您選擇啟用所有區域，您可以決定是否自動啟用新區域。如果您選擇停用所有區域，您可以決定是否自動停用新區域。如果您選擇指定區域，則必須選擇要啟用和停用的區域。
7. 選擇設定。

編輯組態政策

您可以編輯與具有 政策類型的組態相關聯的功能、區域和帳戶。

以下說明如何在 Security Hub 中編輯組態政策

建立編輯組態政策

1. 使用您的 AWS 帳戶搭配委派管理員登入資料來登入。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從導覽窗格中，選擇管理，然後選擇組態。
3. 在已設定政策索引標籤中，選取要編輯的政策選項按鈕。選擇編輯。
4. 若要在帳戶選擇區段中進行變更，請選取下列其中一個選項。如果您想要將組態套用至所有組織單位和帳戶，請選擇所有組織單位和帳戶。如果您想要將組態套用至特定組織單位和帳戶，請選擇特定組織單位和帳戶。如果您選擇此選項，請使用搜尋列或組織結構樹來指定要套用政策的組織單位和帳戶。如果您不想將組態套用至任何組織單位或帳戶，請選擇無組織單位或帳戶。
5. 若要在區域區段中進行變更，請選擇啟用所有區域、停用所有區域或指定區域。如果您選擇啟用所有區域，您可以決定是否自動啟用新區域。如果您選擇停用所有區域，您可以決定是否自動停用新區域。如果您選擇指定區域，則必須選擇要啟用和停用的區域。
6. 選擇下一步。
7. 檢閱您的變更，然後選擇 Update (更新)。您的目標帳戶是根據政策設定。

刪除組態政策

您可以刪除您具有一種政策類型的組態。當您刪除政策時，所有連接的帳戶和組織單位都會從政策中移除。

以下說明如何刪除 Security Hub 中的組態政策。

建立刪除組態政策

1. 使用您的 AWS 帳戶搭配委派管理員登入資料來登入。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從導覽窗格中，選擇管理，然後選擇組態。
3. 在已設定政策索引標籤中，選取要編輯的政策選項按鈕。選擇 Delete (刪除) 按鈕。
4. 在確認方塊中輸入刪除。選擇刪除。

在 Security Hub 中移除委派管理員帳戶

您可以隨時在 Security Hub 主控台中移除委派管理員帳戶。不過，此動作不僅會從 Security Hub 移除委派管理員，還會從 Security Hub CSPM 移除委派管理員。我們建議您只在使用安全帳戶確認此操作時，才執行此動作。

Note

如果您使用組織管理帳戶以外的帳戶做為 Security Hub CSPM 委派管理員，則透過 CSPM 主控台或 AWS Organizations API 將其移除也會從 Security Hub 中移除。同樣地，如果您透過 Security Hub 主控台或 AWS Organizations API 移除 Security Hub 委派管理員，它也會從 Security Hub CSPM 中移除。從 CSPM 移除委派管理員時，中央組態會自動選擇退出。

移除委派管理員帳戶

1. 使用您的組織管理 AWS 帳戶登入資料登入您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從導覽窗格中，選擇一般。
3. 在委派管理員中，選擇移除委派管理員。在快顯視窗中，輸入移除，然後選擇移除。

重新啟用 Security Hub

在先前使用 Security Hub 政策停用的帳戶上重新啟用 Security Hub 之前，您必須先分離停用政策。如果您在停用政策仍連接至帳戶或組織單位時嘗試重新啟用 Security Hub，則停用政策會覆寫啟用，且 Security Hub 會保持停用狀態。

移除組織或帳戶的 Security Hub 停用政策。

1. 使用您的 AWS 帳戶搭配您的組織管理帳戶登入資料來登入。開啟位於 <https://console.aws.amazon.com/organizations/v2/home> 的 Security Hub 主控台。
2. 從導覽面板選擇AWS 帳戶。
3. 如果目前的 Security Hub 停用政策適用於整個組織，請在組織結構下選擇根。如果目前的 Security Hub 停用政策適用於特定帳戶，請在組織結構下選擇特定帳戶，然後遵循每個帳戶的剩餘步驟。
4. 在政策索引標籤中，尋找標題為 Security Hub 政策的區段
5. 選擇停用 Security Hub 的政策旁的選項按鈕。選擇 Detatch。

從組織或帳戶連接政策後，您就可以重新啟用 Security Hub。如需重新啟用 Security Hub 的詳細資訊，請參閱[管理 AWS 組織中成員帳戶的組態](#)。

Security Hub 建議

中的下列安全服務會以 OCSF 格式將問題清單 AWS 傳送至 Security Hub。啟用 Security Hub 之後，我們建議您啟用這些功能 AWS 服務，以提高安全性。

Security Hub CSPM

當您[啟用 Security Hub CSPM](#)時，您可以全面檢視其中的安全狀態 AWS。這可協助您根據安全產業標準和最佳實務來評估您的環境。雖然您可以在不啟用 Security Hub CSPM 的情況下開始使用 Security Hub，但我們建議您啟用 Security Hub CSPM，因為 Security Hub 會關聯來自 Security Hub CSPM 的安全訊號，以改善您的狀態管理。

如果您[啟用 Security Hub CSPM](#)，我們也建議您為帳戶[啟用 AWS 基礎安全最佳實務標準](#)。此標準包含一組控制項，可偵測您的 AWS 帳戶和資源何時偏離安全最佳實務。當您為帳戶啟用 AWS 基礎安全最佳實務標準時，AWS Security Hub CSPM 會自動啟用其所有控制項，包括下列資源類型的控制項：

- 帳戶控制
- Amazon DynamoDB 控制項
- Amazon Elastic Compute Cloud 控制項
- AWS Identity and Access Management (IAM) 控制項
- AWS Lambda 控制項

- Amazon Relational Database Service (Amazon RDS) 控制項
- Amazon Simple Storage Service 控制項

您可以停用此清單中的任何控制項。不過，如果您停用任何這些控制項，您就無法接收支援資源的公開調查結果。如需適用於 AWS 基礎安全最佳實務標準之控制的相關資訊，請參閱[AWS 基礎安全最佳實務 1.0.0 版 \(FSBP\) 標準](#)。

GuardDuty

當您[啟用 GuardDuty](#) 時，您可以在 Security Hub 主控台的儀表板中檢視所有威脅和安全涵蓋範圍調查結果。如果您啟用 GuardDuty，GuardDuty 會自動開始以 OCSF 格式將資料傳送至 Security Hub。

Amazon Inspector

當您[啟用 Amazon Inspector](#) 時，您可以在 Security Hub 主控台的儀表板中檢視所有公開和安全性涵蓋範圍調查結果。如果您啟用 Amazon Inspector，Amazon Inspector 會自動開始以 OCSF 格式將資料傳送至 Security Hub。

我們建議您啟用 Amazon EC2 掃描和 Lambda 標準掃描。當您啟用 Amazon EC2 掃描時，Amazon Inspector 會掃描您帳戶中的 Amazon EC2 執行個體是否有套件漏洞和網路連線能力問題。當您啟用 Lambda 標準掃描時，Amazon Inspector 會掃描 Lambda 函數是否有套件相依性中的軟體漏洞。如需詳細資訊，請參閱《Amazon Inspector 使用者指南》中的[啟用掃描類型](#)。

Macie

[啟用 Macie](#) 時，您可以偵測 Amazon S3 儲存貯體的其他暴露。我們建議設定[自動敏感資料探索](#)，讓 Macie 可以每天評估您的 Amazon S3 儲存貯體庫存。

Security Hub 中的帳戶涵蓋範圍

Security Hub 可讓您透過政策和組態，跨區域和組織帳戶啟用多項功能。其中一些功能來自 Security Hub 以外的服務，包括 Amazon Inspector、Amazon GuardDuty、AWS Security Hub CSPM 和 Amazon Macie。您可以使用帳戶涵蓋範圍頁面來追蹤這些功能涵蓋哪些帳戶和區域。

帳戶涵蓋範圍頁面

帳戶涵蓋範圍頁面可讓您查看跨 AWS 帳戶啟用的安全功能。此檢視可協助您識別安全涵蓋範圍中的差距，並追蹤整個組織採用的功能。

存取 Security Hub 帳戶涵蓋範圍頁面

1. 開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 在導覽窗格中的設定下，選擇帳戶涵蓋範圍。

概觀區段

概觀區段會顯示所有受監控帳戶的彙總安全性涵蓋範圍指標。此高階視覺化會顯示啟用的每個安全功能的帳戶百分比，其中提供了安全狀態的完整檢視表。您可以選取涵蓋功能的每個百分比來篩選涵蓋範圍調查結果，以顯示與該功能涵蓋範圍相關的調查結果。

概觀區段中的百分比是使用以下計算來決定：

$$\text{(Count of number of accounts and regions the capability is enabled in)} / \text{((Total number of accounts Security Hub is enabled in) * (Number of regions the capability is available in))}$$

帳戶索引標籤

帳戶索引標籤可透過依帳戶功能篩選來啟用帳戶特定的涵蓋範圍分析。每個安全功能都會顯示涵蓋範圍百分比，當選取時，該百分比會顯示該功能內個別功能的詳細明細及其涵蓋範圍百分比。當您選取這些百分比時，系統會篩選涵蓋範圍調查結果結果，以顯示指出該功能和該列中帳戶涵蓋範圍的結果。

帳戶索引標籤中的百分比是使用以下計算來決定：

$$\text{(Count of number of regions the capability is enabled in)} / \text{(Number of regions the capability is available in)}$$

在某些情況下，涵蓋範圍百分比可能顯示為 0%：

- Security Hub 未在帳戶中啟用，因此不會擷取任何涵蓋範圍調查結果。
- Security Hub 正在等待產生涵蓋範圍調查結果。

涵蓋範圍問題清單索引標籤

涵蓋範圍問題清單索引標籤會顯示安全性功能檢查偵測到帳戶中已停用的功能時所產生的資訊問題清單。這些調查結果有助於識別可以增強安全涵蓋範圍的領域。每個涵蓋範圍調查結果都會提供有關涵蓋範圍調查結果的標題、調查結果的帳戶和區域，以及調查結果目前狀態的資訊。每個調查結果也都有一

個設定連結，可讓您前往可以管理該功能的組態的個別服務，或前往 Security Hub 組態頁面，您可以在其中更新安全服務的目前組態。

如需涵蓋範圍調查結果的詳細資訊，請參閱 [Security Hub 中的涵蓋範圍調查結果](#)。

安全涵蓋範圍小工具

帳戶涵蓋範圍也可以透過 Security Hub 摘要儀表板中的安全涵蓋範圍小工具檢視。如需小工具的詳細資訊，請參閱[安全性涵蓋範圍小工具](#)文件。

Security Hub 延伸計劃

Security Hub 延伸計劃透過以 AWS Security Hub 為中心的整合安全操作體驗，協助保護跨雲端、端點、網路、身分、資料、電子郵件和瀏覽器的整個企業資產。使用 Security Hub 延伸計劃，您可以選擇可滿足您的安全需求的合作夥伴解決方案，並註冊彈性pay-as-you-go定價，無需預付投資或長期承諾。您可以隨著業務需求的演進而新增或移除合作夥伴解決方案。

Security Hub 延伸計劃適用於所有已啟用 Security Hub Essentials 計劃的客戶。Security Hub Extended 計劃的費用會顯示在您的每月 AWS 帳單中，並以 AWS 做為記錄賣方。

Security Hub 所有解決方案的延伸計劃定價可在 [Security Hub 定價詳細資訊頁面](#)的延伸計劃索引標籤上取得。

Security Hub Extended 計劃的許可

若要從 Security Hub Extended 計劃訂閱合作夥伴產品，除了 Security Hub 許可之外，您還需要下列許可：

- `aws-marketplace:ViewSubscriptions`
- `aws-marketplace:Subscribe`

若要從 Security Hub Extended 計劃取消訂閱合作夥伴產品，除了 Security Hub 許可之外，您還需要下列許可：

- `license-manager:ListReceivedLicenses`
- `aws-marketplace:ListAgreementCharges`
- `aws-marketplace:Unsubscribe`

如需 AWS Marketplace 許可的詳細資訊，請參閱 Marketplace AWS 買方指南中的[控制 AWS 對 Marketplace 訂閱的存取](#)。

檢閱和註冊延伸計劃合作夥伴

Security Hub Extended 計劃可透過 Security Hub 委派管理員帳戶或獨立帳戶存取。在 Security Hub 延伸計劃頁面上，您可以檢視每個合作夥伴的詳細資訊、啟動合作夥伴解決方案的訂閱，並透過合作夥伴的加入頁面開始每個合作夥伴解決方案的加入程序。

存取 Security Hub Extended 計劃並註冊合作夥伴的產品

1. 使用您的委派管理員或獨立帳戶登入資料登入 AWS 管理主控台。
2. 開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
3. 在導覽窗格中，選擇管理，然後選擇延伸計劃。
4. 針對您要註冊的每個合作夥伴解決方案，選擇檢視產品。
5. 檢閱產品定價詳細資訊，然後在您準備好開始加入合作夥伴產品的程序時選擇訂閱。
6. 訂閱程序完成後，請選擇設定您的帳戶以重新導向至合作夥伴的註冊頁面。
7. 提供合作夥伴註冊頁面的必要資訊，並遵循合作夥伴提供的後續步驟來完成加入步驟。

Important

在完成合作夥伴產品的加入程序之前，您不需要支付合作夥伴解決方案的費用。

從延伸計劃合作夥伴取消訂閱

如果您不想再使用擴展計劃合作夥伴解決方案，您可以取消訂閱合作夥伴清單。

若要取消訂閱合作夥伴解決方案，請遵循 AWS Marketplace 買方指南中[取消 SaaS 訂閱](#)的指引。

Important

除了取消訂閱之外，根據您為公司設定解決方案的方式，請遵循合作夥伴解決方案所需的任何其他離職步驟。

了解 Security Hub 中的跨區域彙總

跨區域彙總可讓您將多個 AWS 區域的調查結果、資源和趨勢彙總到單一主區域。然後，您可以從主要區域管理所有這些資料。

假設您將美國東部（維吉尼亞北部）設定為主要區域，並將美國西部（奧勒岡）和美國西部（加利佛尼亞北部）設定為連結區域。當您檢視美國東部（維吉尼亞北部）的調查結果頁面時，您會看到所有三個區域的調查結果。這些調查結果的更新也會反映在所有三個區域中。

彙總的資料類型

使用一或多個連結區域啟用跨區域彙總時，Security Hub 會將下列資料從連結區域複寫至主要區域。每個已啟用跨區域彙總的帳戶都會發生這種情況。

- 調查結果
- Resources
- 趨勢

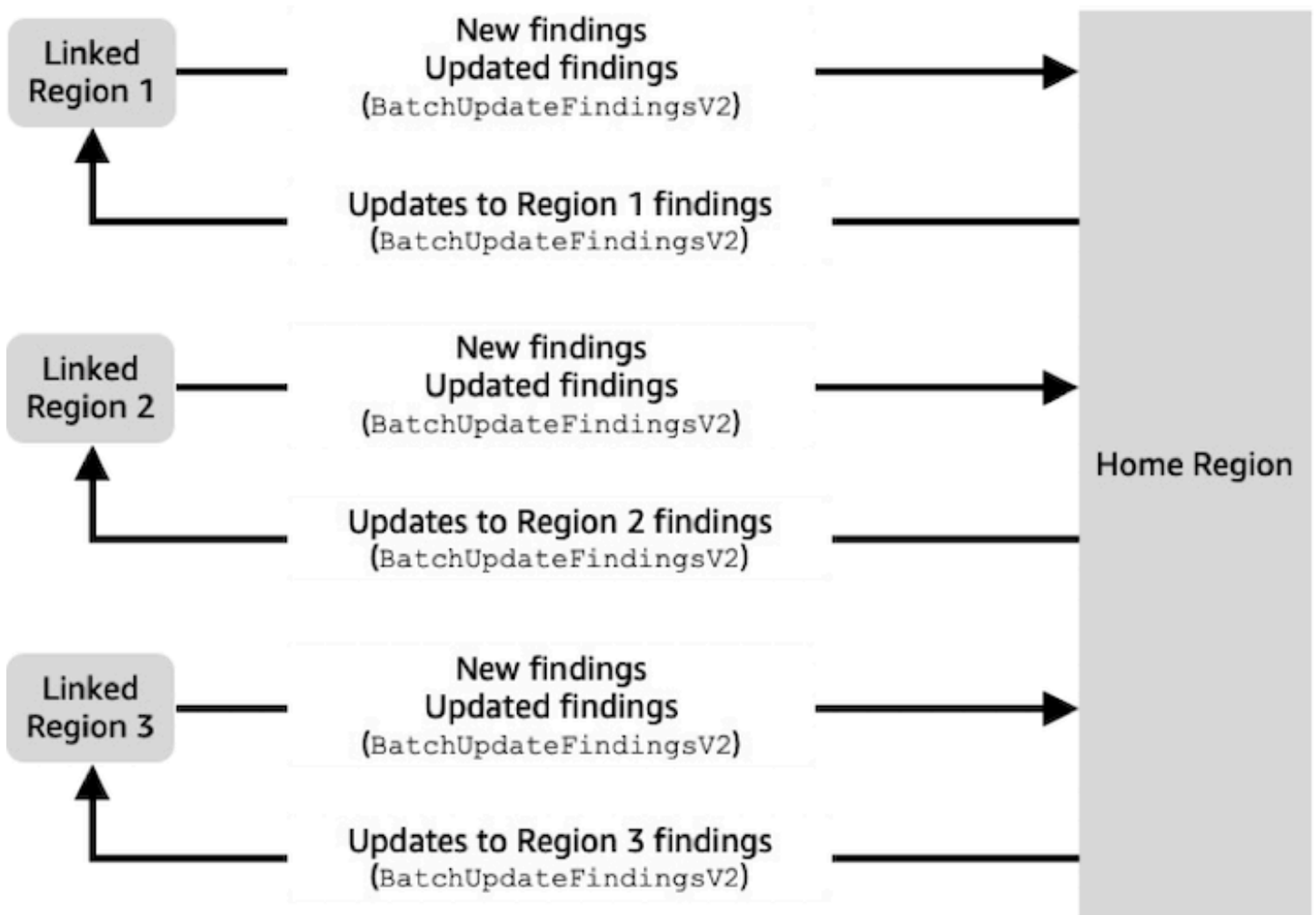
除了先前清單中的新資料之外，Security Hub 也會在連結的區域和主要區域之間複寫此資料的更新。在連結區域中發生的更新會複寫至主要區域。主要區域中發生的更新會複寫回連結的區域。如果主要區域和連結區域有衝突的更新，則會使用最新的更新。

除非問題清單有更新，否則在區域成為連結區域時已存在的任何問題清單都不會複寫至主要區域。區域連結至主要區域後，主要區域和連結區域之間的問題清單會有所不同，直到連結區域中的問題清單更新或過時為止。

在區域成為連結區域時已存在的任何資源都會複寫至主要區域，通常在區域連結至主要區域後 24-48 小時內。

移除連結的區域時，該區域的任何問題清單或資源都會保留在主要區域中，直到問題清單或資源過時為止。

趨勢資料是根據趨勢所在區域中存在的問題清單和資源。主區域中的趨勢資料將反映已同步至主區域的調查結果和資源的目前狀態。



跨區域彙總不會增加 Security Hub 的成本。當 Security Hub 複寫新資料或更新時，您不需要付費。

在主區域中，摘要頁面提供跨連結區域的作用中問題清單和資源的檢視。

Security Hub 只會從帳戶已啟用 Security Hub 的區域彙總資料。帳戶不會根據跨區域彙總組態自動啟用 Security Hub。

可以在未選取任何連結區域的情況下啟用跨區域彙總。在此情況下，不會發生資料複寫。

管理員和成員帳戶的彙總

獨立帳戶和管理員帳戶可以設定跨區域彙總。如果由管理員設定，則管理員帳戶的存在對於跨區域彙總在受管帳戶中運作至關重要。如果管理員帳戶已從成員帳戶移除或取消關聯，成員帳戶的跨區域彙總將會停止，或者如果成員帳戶在與管理員建立關聯之前具有跨區域彙總組態，則該彙總組態會再次對該帳戶生效。

當管理員帳戶啟用跨區域彙總時，Security Hub 會將管理員帳戶在所有連結區域中產生的資料複寫至主要區域。此外，Security Hub 會識別與該管理員相關聯的成員帳戶，而且每個成員帳戶都會繼承管理員的跨區域彙總設定。Security Hub 會將成員帳戶在所有連結區域中產生的資料複寫至主要區域。

管理員可以存取和管理受管區域內所有成員帳戶的安全調查結果。此外，管理員可以檢視受管區域內所有成員帳戶的資源庫存。

作為 Security Hub 成員帳戶，您必須登入主區域，才能檢視來自所有連結區域的帳戶彙總資料。成員帳戶沒有檢視其他成員帳戶資料的權限 `DeleteAggregatorV2`，也不允許呼叫 `CreateAggregatorV2`、和 `GetAggregatorV2` APIs。

自動化規則和跨區域彙總

啟用跨區域彙總時，只能在定義的主區域中建立自動化規則。您定義的任何規則都會套用至所有連結的區域，除非您的規則條件適用於特定區域。您必須為任何非連結區域的區域建立個別的自動化規則。

在啟用跨區域彙總之前，在主區域中建立的任何規則都會自動套用至連結的區域。建立彙總工具後，先前在連結區域中建立的規則將不再適用。刪除彙總工具或不再連結區域後，連結區域中定義的規則會繼續套用。

啟用跨區域彙總

您必須從要指定為主要 AWS 區域的區域啟用跨區域彙總。

若要啟用跨區域彙總，您可以建立稱為問題清單彙總工具的 Security Hub 資源。問題清單彙總工具資源會指定您的主要區域和連結的區域（如果有的話）。

您無法使用預設為停用的 AWS 區域做為您的主要區域。如需預設停用的區域清單，請參閱《AWS 一般參考》中的啟用區域。

當您啟用跨區域彙總時，您可以選擇視需要指定一或多個連結區域。啟用跨區域彙總不會在該區域中啟用 Security Hub。若要在區域中啟用 Security Hub，請參閱 Security Hub 使用者指南中的將政策建立為委派管理員以管理成員帳戶。

啟用跨區域彙總（主控台）

1. 從管理員帳戶或在獨立帳戶中開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 AWS Security Hub 主控台
2. 使用 AWS 區域選擇器，登入您要用作彙總區域的區域。
3. 在 Security Hub 導覽功能表中，選擇設定，然後選擇一般。
4. 在跨區域彙總區段中，選擇設定。

5. 根據預設，主區域設定為無彙總區域。
6. 在主要區域下，選取 選項，將目前區域指定為主要區域。
7. 或者，對於連結的區域，選取要從中彙總資料的 區域。
8. 選擇儲存。

檢閱跨區域彙總設定

您可以從管理員帳戶或獨立帳戶中的任何 AWS 區域檢視 AWS Security Hub 中目前的跨區域彙總組態。成員帳戶無法檢視跨區域彙總組態。組態包含主要區域和連結的區域（如果有的話）。

依照步驟檢視您目前的跨區域彙總設定

檢視跨區域彙總設定（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 AWS Security Hub 主控台。
2. 在導覽窗格中，選擇設定，然後選擇一般。
3. 如果未啟用跨區域彙總，則一般頁面會顯示啟用跨區域彙總的選項。只有管理員帳戶和獨立帳戶可以啟用跨區域彙總。
4. 如果啟用跨區域彙總，則區域索引標籤會顯示下列資訊：
 - 主要區域
 - 是否自動彙總 Security Hub 支援且您選擇加入之新區域的調查結果、資源和趨勢
 - 連結區域清單（如果有選取）

更新跨區域彙總設定

您可以透過變更連結的區域或目前的主區域，在 AWS Security Hub 中更新目前的跨區域彙總設定。

除非您在 AWS 帳戶中啟用區域，否則不會針對選擇加入區域實作跨區域彙總的變更。在 2019 年 3 月 20 日當天或之後 AWS 推出的區域為選擇加入區域。

當您停止從連結區域彙總資料時，AWS Security Hub 不會從主要區域中可存取的該區域移除任何現有的彙總資料。

您無法使用本節中的更新程序來變更主要區域。若要變更主要區域，您必須執行下列動作：

1. 刪除目前的跨區域彙總組態。如需說明，請參閱 [the section called “刪除彙總”](#)。

2. 變更為您希望成為新主區域的 區域。
3. 啟用跨區域彙總。如需說明，請參閱[the section called “刪除彙總”](#)。

您必須從目前的主區域更新跨區域彙總組態。

變更連結的區域（主控台）

1. 從管理員帳戶或在獨立帳戶中開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 AWS Security Hub 主控台。
2. 登入目前的彙總區域。
3. 在 Security Hub 導覽功能表中，選擇設定，然後選擇一般。
4. 針對跨區域彙總，選擇編輯。
5. 針對連結區域，更新選取的連結區域。
6. 選擇儲存。

刪除跨區域彙總

如果您不希望 AWS Security Hub 彙總資料，您可以刪除問題清單彙總工具。或者，您可以保留問題清單彙總工具，但無法透過將現有彙總工具更新為未選取連結區域 AWS，將任何區域連結至主要區域。

若要變更您的主要區域，您必須刪除目前的問題清單彙總工具，並建立新的問題清單彙總工具。

當您刪除問題清單彙總工具時，Security Hub 會停止彙總資料。它不會從主要區域移除任何現有的彙總資料。

刪除問題清單彙總工具（主控台）

您只能從目前的主區域刪除問題清單彙總工具。

在主要區域以外的區域中，Security Hub 主控台上的問題清單彙總面板會顯示訊息，您必須編輯主要區域中的組態。選擇此訊息以顯示切換至主要區域的連結。

停止跨區域彙總（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 AWS Security Hub 主控台。
2. 確保您已登入目前的主區域。
3. 在 Security Hub 導覽功能表中，選擇設定，然後選擇一般。

4. 在跨區域彙總下，選擇編輯。
5. 在彙總區域下，選擇無彙總區域。
6. 選擇儲存。
7. 在確認對話方塊的確認欄位中，輸入 **Confirm**。
8. 選擇確認。

在 Security Hub 的摘要儀表板中工作

Security Hub 主控台內的摘要儀表板會顯示安全性小工具的暴露、威脅、資源和安全涵蓋範圍概觀。您可以透過新增和移除小工具，以及建立和套用篩選條件集來擷取每個小工具中的資料，來自訂儀表板。

考量事項

在與儀表板互動之前，請考慮下列事項：

- 儲存的篩選條件集或小工具配置變更等自訂項目會自動儲存。
- 每次開啟儀表板時，資料會自動重新整理。
- 如果您設定跨區域彙總，儀表板會包含所有連結區域的調查結果（檢視您主要區域的儀表板時）。

如果您的帳戶是組織的委派管理員帳戶、組織中的成員帳戶或獨立帳戶，請考慮下列事項。

- 委派管理員帳戶所做的自訂，將與成員帳戶所做的自訂分開儲存。自訂可能包含已儲存的篩選條件集或小工具配置的變更。
- 如果您的帳戶是組織的委派管理員帳戶，則資料會包含您帳戶和成員帳戶的調查結果。
- 如果您的帳戶是組織中的成員帳戶或獨立帳戶，資料只會包含您帳戶的調查結果。

根據最佳實務，我們建議不要在儲存的篩選條件集、自訂小工具或其他相關的自由格式文字欄位中包含機密、敏感或個人身分識別資訊 (PII)。

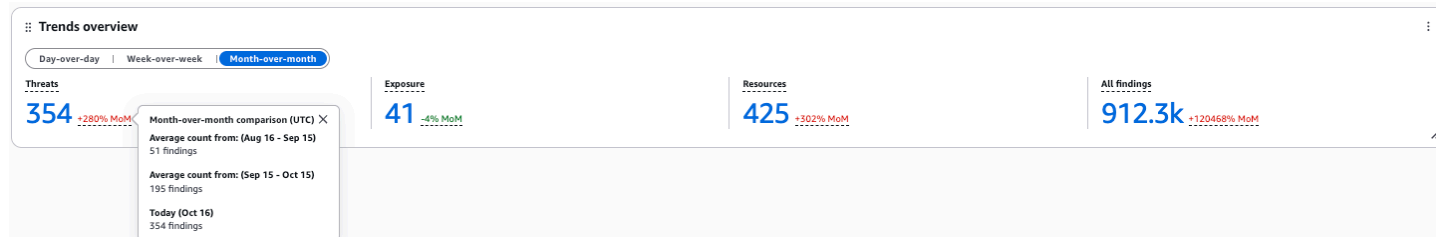
可用的小工具

您可以在摘要儀表板的執行和分類索引標籤中與不同的小工具互動。執行標籤包含小工具，可顯示您暴露、威脅和資源的趨勢資料，以及安全涵蓋範圍小工具，以協助跨不同的安全功能追蹤您的帳戶涵蓋範圍。分類索引標籤包含小工具，可顯示您的暴露、威脅和資源摘要。不過，您可以在兩個索引標籤中新增小工具、移除小工具和管理每個小工具的位置，以自訂您的體驗。

趨勢小工具

下列小工具會顯示您暴露、威脅和資源的趨勢資料，以便您可以隨著時間進行分析。

趨勢概觀小工具



此小工具會顯示您在下列期間內的暴露、威脅、資源和調查結果的概觀：

- Month-over-month反映過去兩個月的period-over-period計數。
- Week-over-week反映過去兩週的period-over-period數。
- Day-over-day反映過去 2 天的period-over-period計數。

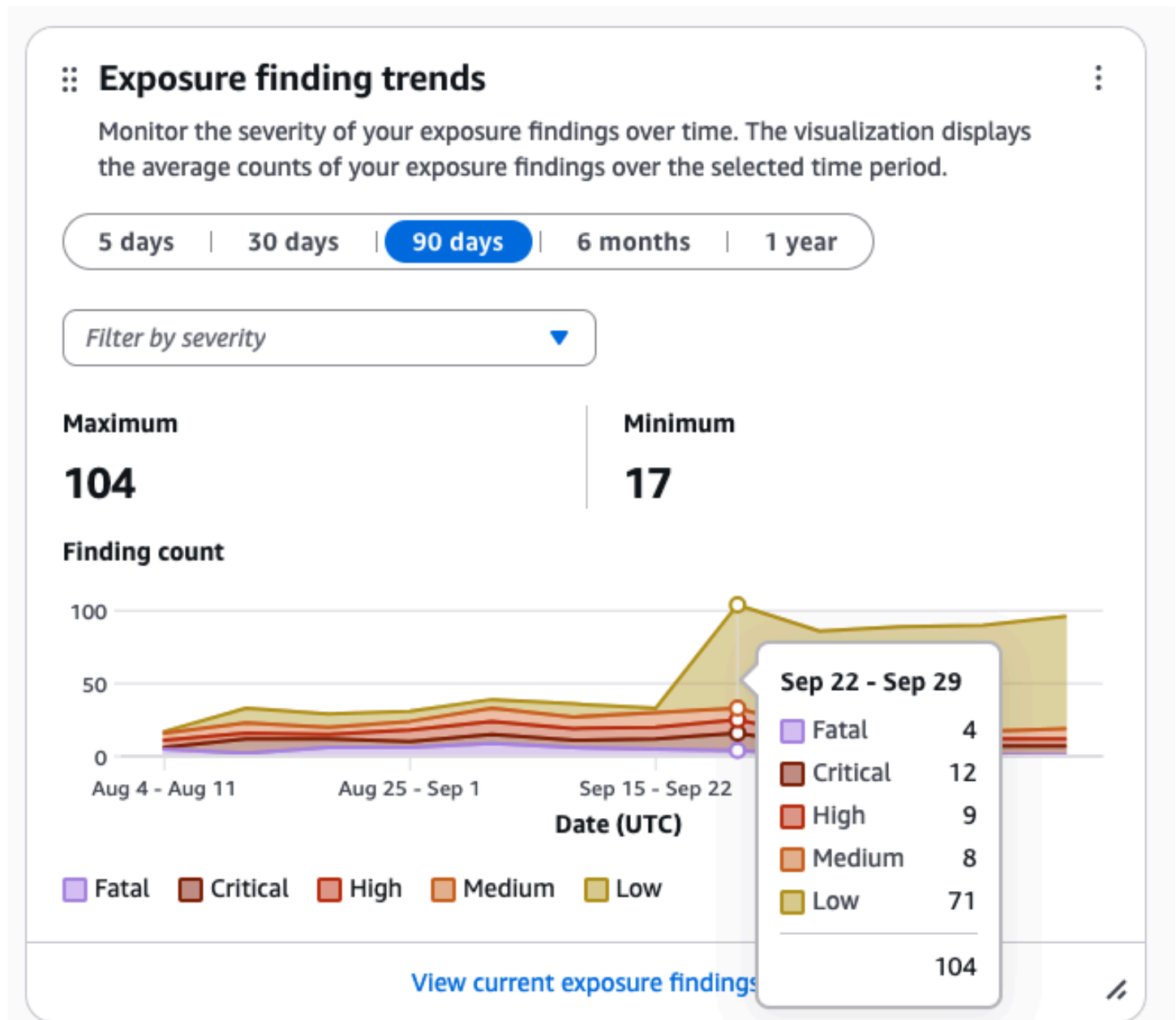
百分比旁邊的數字反映截至目前period-over-period計數。選擇此數字會引導您前往 主控台中對應的儀表板。如果您導覽至顯示趨勢資料的另一個儀表板，則儀表板只會顯示過去 90 天的趨勢資料，如果您的帳戶不包含超過 30 天的調查結果或資源，則只會顯示最適合的期間。

Note

若要在小工具中接收資料，您必須啟用下列安全服務：

- AWS Security Hub CSPM – 接收有關公開的資料
- Amazon Inspector – 接收有關曝光的資料
- GuardDuty – 接收威脅的資料

公開調查結果趨勢小工具



此小工具會顯示您在下列期間內的暴露問題清單嚴重性：

- 5 天
- 30 天
- 90 天
- 6 個月
- 1 年

視覺效果會顯示所選期間內問題清單的平均計數。

嚴重性篩選條件

您可以包含或排除下列嚴重性篩選條件來更新圖形：

- 嚴重
- 嚴重
- 高
- 中性
- 低
- 資訊性
- Other (其他)
- 不明

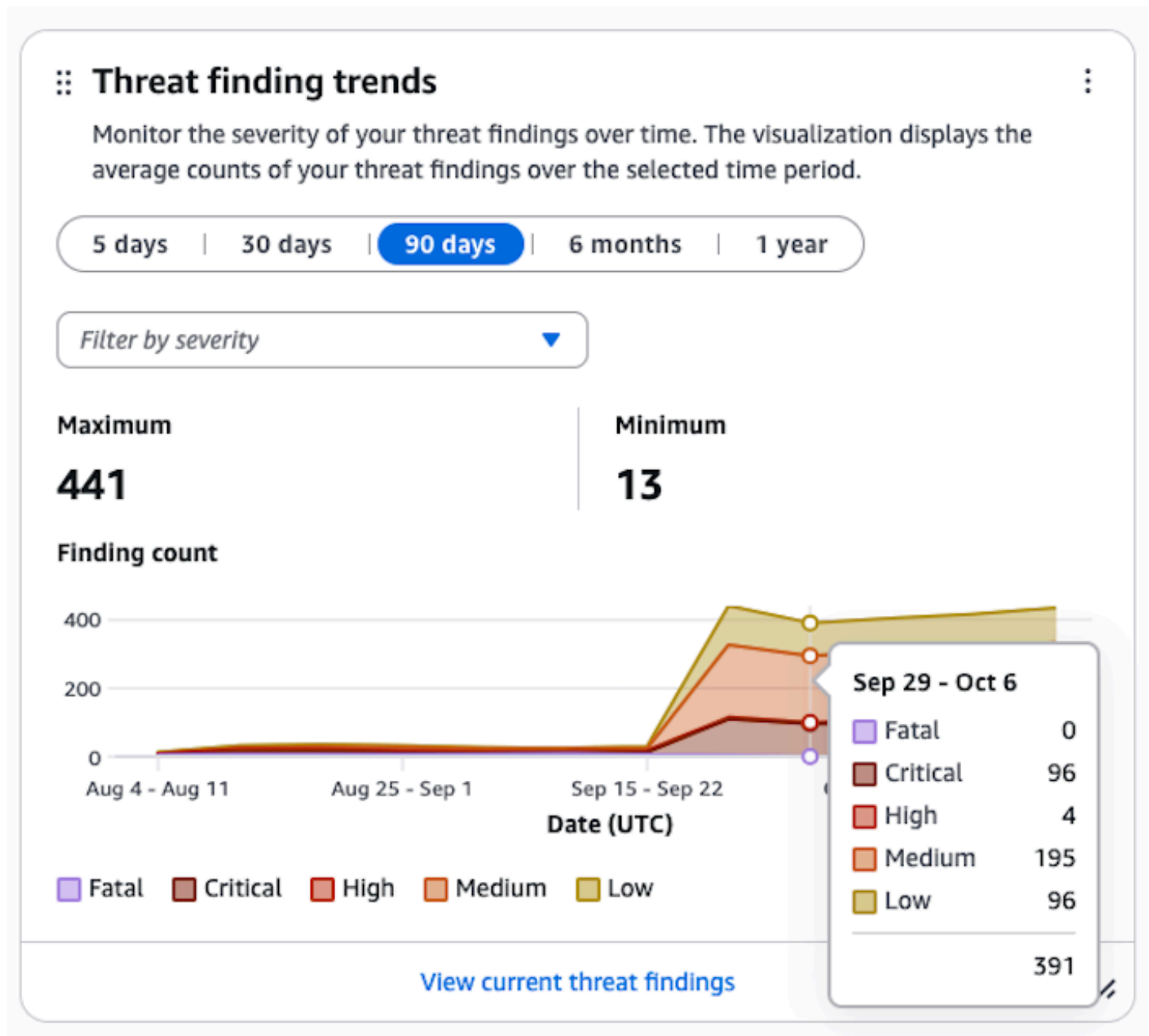
套用的嚴重性篩選條件會顯示在不同方塊中的視覺效果底部。您可以將滑鼠暫留在視覺化上，以檢閱特定時間點的問題清單平均計數。您也可以檢閱符合每個套用嚴重性篩選條件的調查結果平均計數。

您可以選擇檢視所有目前的公開調查結果，以導向至公開儀表板。根據預設，曝光儀表板只會顯示過去 90 天的趨勢資料。如果您的帳戶不包含超過 30 天的公開調查結果，儀表板會根據最適合的期間顯示趨勢資料。

Note

若要在此小工具中接收資料，您必須啟用 [Amazon Inspector](#) 和 [Security Hub CSPM](#)。

威脅清單趨勢小工具



此小工具會在下列期間內顯示威脅調查結果的嚴重性：

- 5 天
- 30 天
- 90 天
- 6 個月
- 1 年

視覺效果會顯示所選期間內問題清單的平均計數。

嚴重性篩選條件

您可以包含或排除下列嚴重性篩選條件來更新圖形：

- 嚴重
- 嚴重
- 高
- 中性
- 低
- 資訊性
- Other (其他)
- 不明

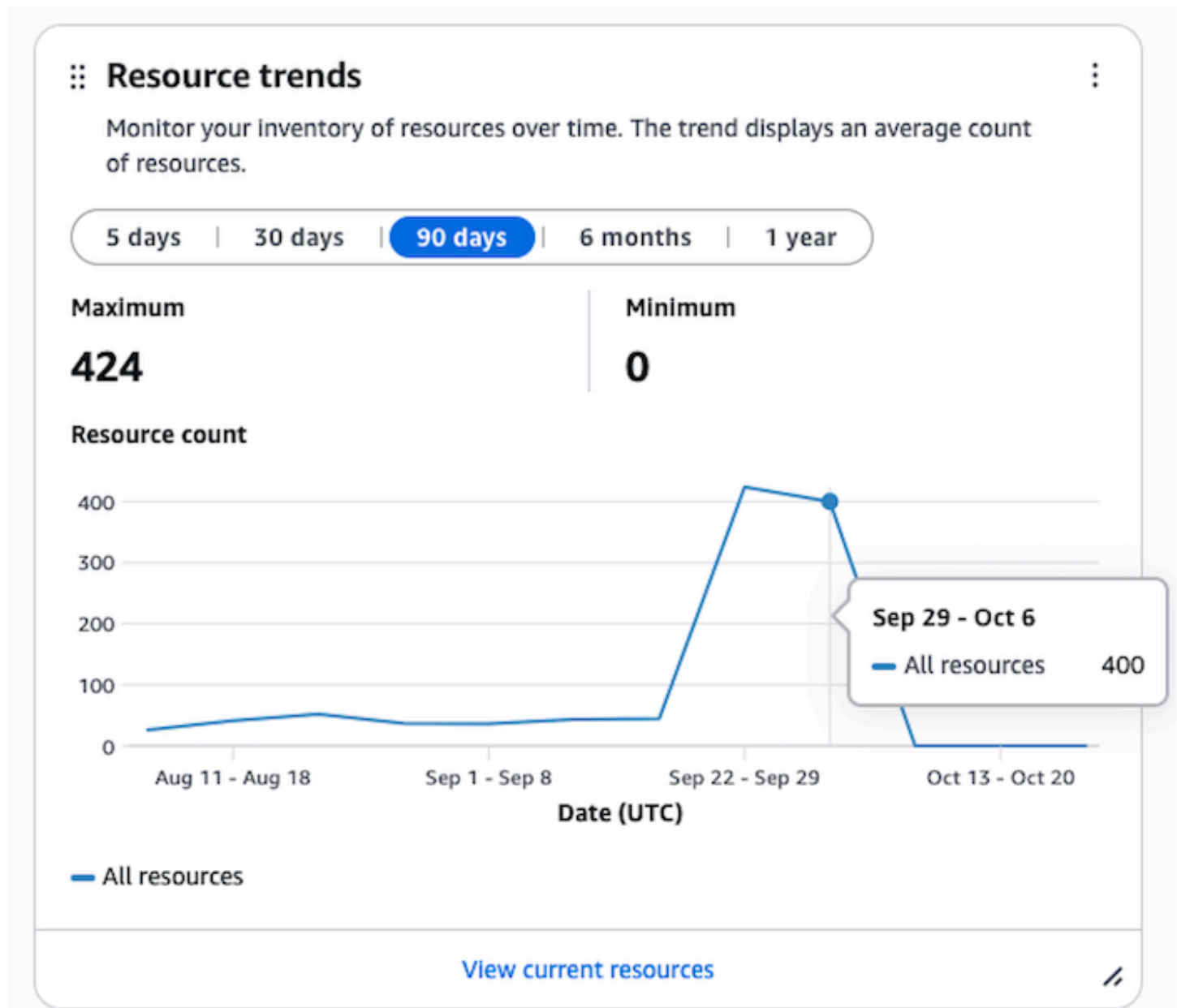
套用的嚴重性篩選條件會顯示在不同方塊中的視覺效果底部。您可以將滑鼠暫留在視覺化上，以檢閱特定時間點的問題清單平均計數。您也可以檢閱符合每個套用嚴重性篩選條件的調查結果平均計數。

您可以選擇檢視所有目前的威脅調查結果，以導向至暴露儀表板。根據預設，威脅儀表板只會顯示過去 90 天的趨勢資料。如果您的帳戶不包含超過 30 天的威脅調查結果，儀表板會根據最適合的期間顯示趨勢資料。

Note

若要在此小工具中接收資料，您必須啟用 [GuardDuty](#)。

資源趨勢小工具



此小工具會顯示您在下列期間內的資源庫存：

- 5 天
- 30 天
- 90 天
- 6 個月
- 1 年

視覺效果會顯示所選期間內資源的平均計數。您可以將滑鼠暫留在視覺化上，以檢閱特定時間點的資源平均計數。

您可以選擇檢視要導向資源儀表板的目前資源。根據預設，資源儀表板只會顯示過去 90 天的趨勢資料。如果您的帳戶不包含超過 30 天的資源，儀表板會根據最適合的時段顯示趨勢資料。

此小工具會顯示您在下列期間內的資源庫存：

- 5 天
- 30 天
- 90 天
- 6 個月
- 1 年

趨勢的資料保留

Security Hub 會為啟用 Security Hub 的所有 AWS 帳戶保留趨勢資料一年。趨勢資料保留一年後，會從 Security Hub 中刪除。

委派管理員和獨立帳戶的趨勢資料會在 Security Hub 停用後或帳戶終止時刪除。

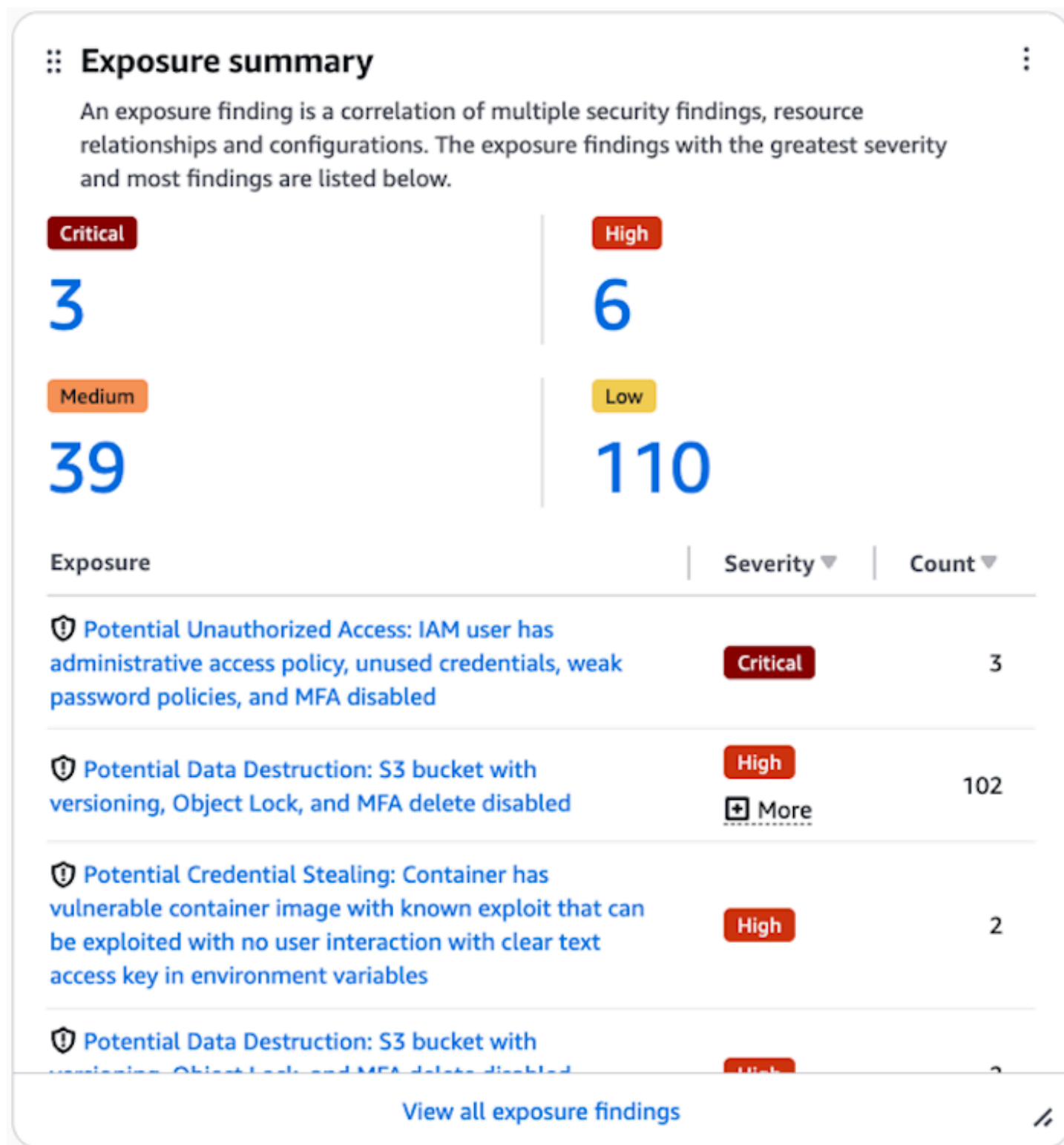
已啟用 Security Hub 之成員帳戶的趨勢資料保留秘密：

- 如果成員帳戶離開組織，Security Hub 仍會儲存趨勢資料，直到帳戶離開組織的時間為止。
- 如果成員帳戶停用 Security Hub，則直到帳戶停用時的趨勢資料將保留一年。
- 如果成員帳戶終止，趨勢資料將與終止的帳戶取消關聯（例如，將清除已終止的 accountID），其餘趨勢資料將保留一年。

摘要小工具

下列小工具會顯示您的暴露、威脅和資源摘要。

曝光摘要小工具



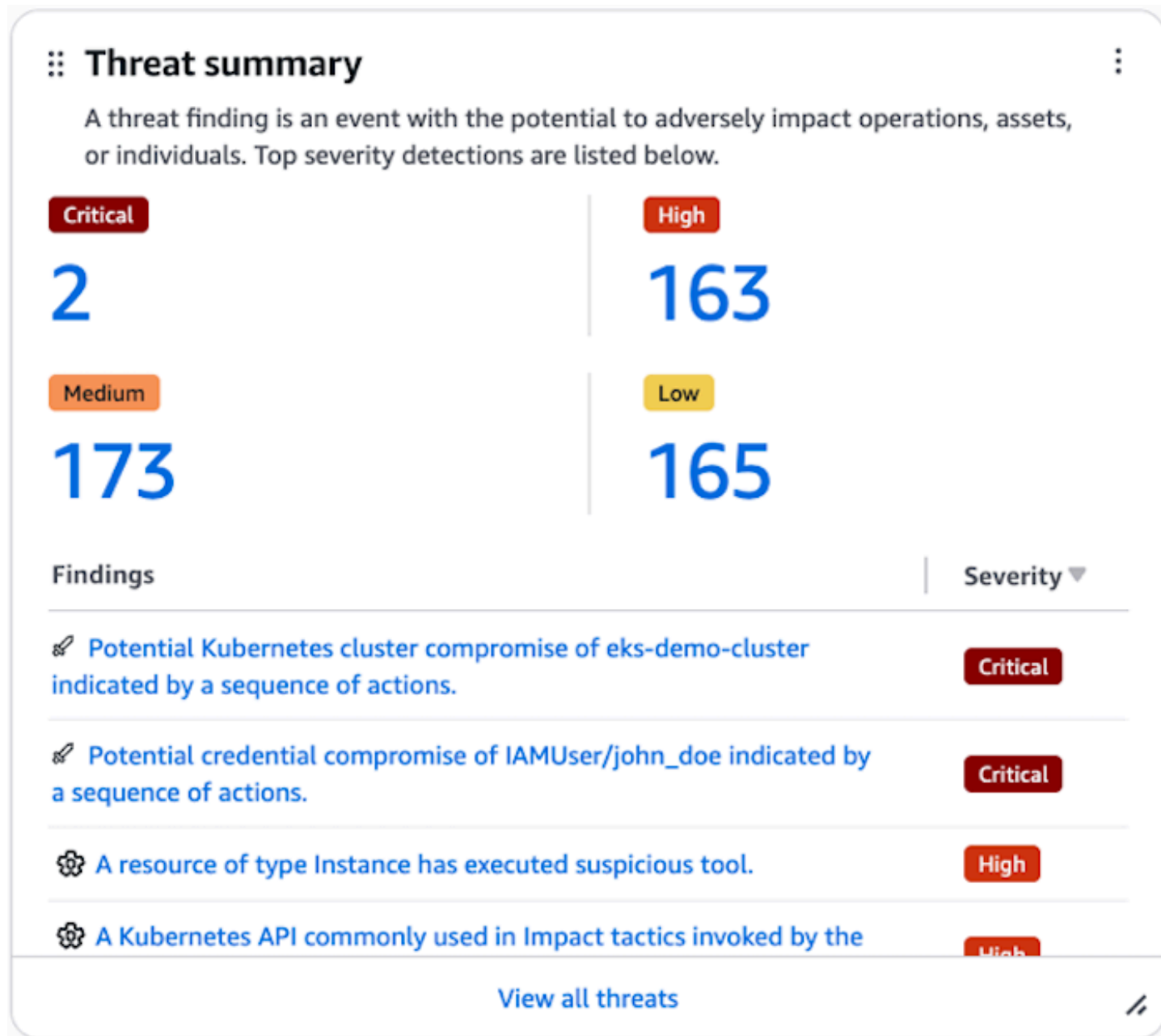
此小工具會依嚴重性顯示您的曝光。公開是根據 Security Hub 和其他 AWS 安全服務的問題清單和特徵分析，例如 Amazon Inspector。此小工具中的曝光清單僅限於具有最高嚴重性的八個曝光。嚴重性

較高的曝光會先出現在清單中。如果兩個或多個曝光的嚴重性相同，則清單會自動將這些曝光分組到較近期的曝光之後。選擇檢視所有曝光會引導您前往曝光儀表板。

Note

若要在此小工具中接收資料，您必須啟用 [Amazon Inspector](#) 和 [Security Hub CSPM](#)。

威脅摘要小工具



此小工具會依嚴重性顯示您的威脅。威脅是指可能危及您環境安全的惡意活動或可疑活動。此小工具中的威脅清單僅限於具有最高嚴重性的八個威脅。嚴重性較高的威脅會先出現在清單中。如果兩個或多個威脅的嚴重性相同，則清單會自動將這些威脅分組為較近期的威脅。選擇檢視所有威脅會引導您前往威脅儀表板。

 Note

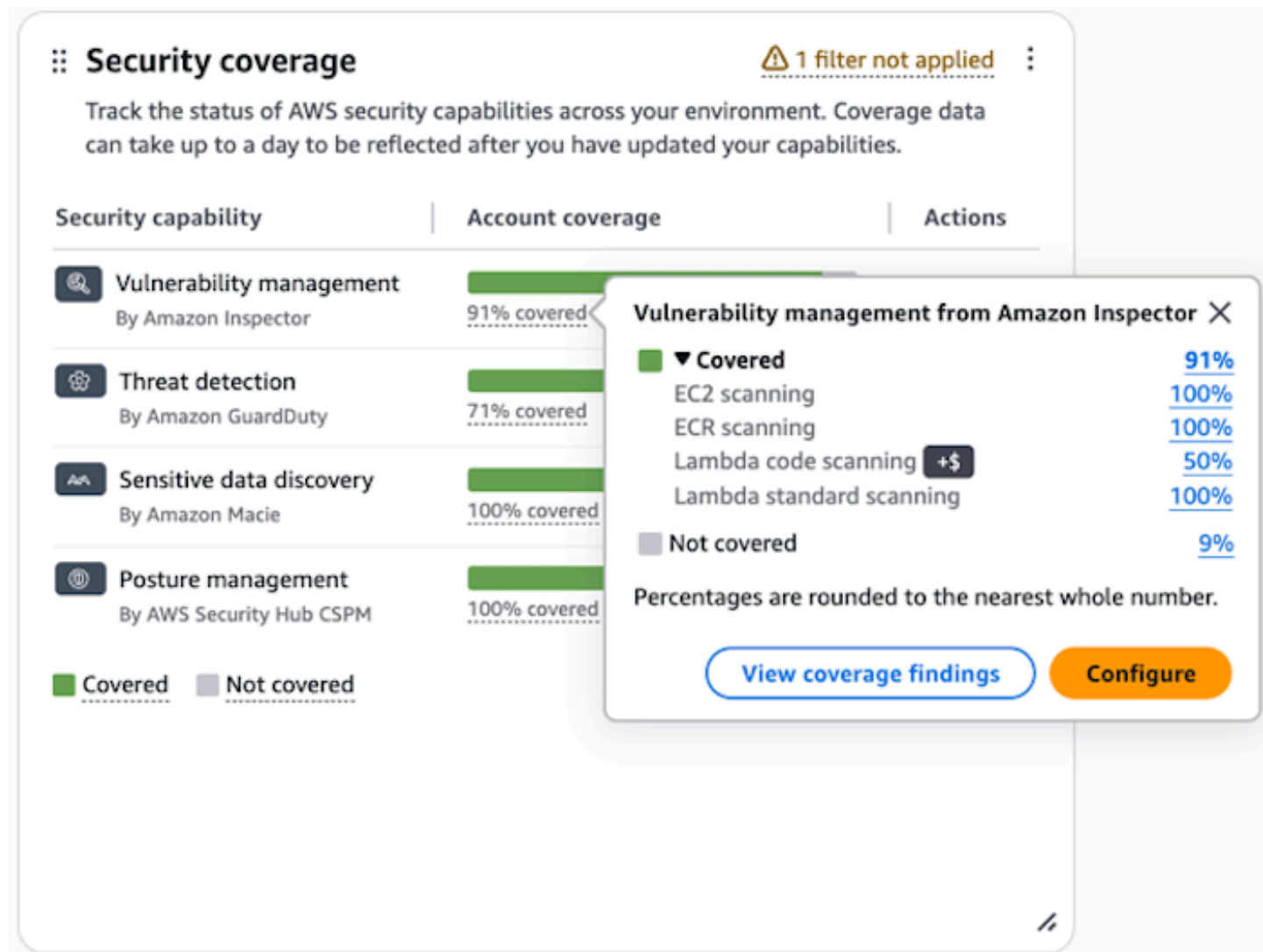
若要在此小工具中接收資料，您必須[啟用 GuardDuty](#)。

資源摘要小工具

Resource summary 		
View resources prioritized by exposures and attack sequences.		
Resource	Resource type	Findings
i-0a276277d0104f998	AWS::EC2::Instance	2 exposure findings 0 attack sequence findings 4724 other findings
i-0f3c1d0199cdd96f4	AWS::EC2::Instance	2 exposure findings 0 attack sequence findings 32 other findings
i-062f63d9a6f716002	AWS::EC2::Instance	2 exposure findings 0 attack sequence findings 14 other findings
i-0987f8e3a022a6bc1	AWS::EC2::Instance	2 exposure findings 0 attack sequence findings 14 other findings
View all resources		

此小工具會依與資源相關聯的類型和問題清單來顯示資源。資源的優先順序是公開和攻擊序列。選擇檢視所有資源會將您導向資源儀表板。

安全涵蓋範圍小工具



小工具會顯示下列安全功能的 帳戶涵蓋範圍摘要：

- Amazon Inspector 漏洞管理
- Amazon GuardDuty 的威脅偵測
- Amazon Macie 的敏感資料探索
- Security AWS Hub CSPM 的姿勢管理

帳戶涵蓋範圍欄中的百分比代表針對 Security Hub 啟用 AWS 區域 的每個安全功能，通過 AWS 帳戶和失敗的涵蓋範圍檢查數量。您可以透過選擇百分比來檢閱安全功能通過和失敗的涵蓋範圍檢查。已涵

蓋 表示已通過涵蓋範圍檢查。未涵蓋表示涵蓋範圍檢查失敗。檢閱通過和失敗的涵蓋範圍檢查數量百分比時，涵蓋範圍下的每個百分比代表安全功能涵蓋的涵蓋範圍調查結果百分比。在某些情況下，涵蓋範圍檢查的百分比會四捨五入至最接近的整數。

隱藏的涵蓋範圍調查結果

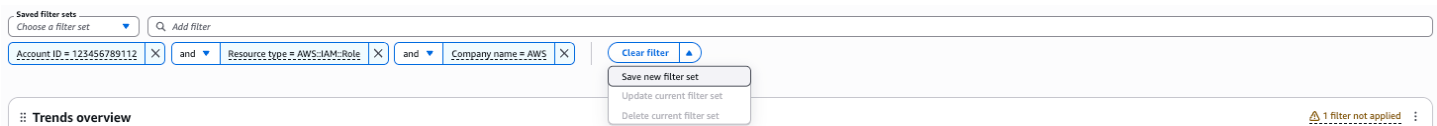
如果 Security Hub 中的任何涵蓋範圍問題清單遭到隱藏，小工具會顯示訊息，通知您涵蓋範圍已排除：

已透過隱藏的涵蓋範圍調查結果排除安全功能的涵蓋範圍。

如需涵蓋範圍調查結果的詳細資訊，請參閱 [Security Hub 中的涵蓋範圍調查結果](#)。

可用的篩選條件

您可以使用新增篩選條件列，將篩選條件套用至安全性小工具。



篩選條件依下列類別組織：

- 共用篩選條件 – 適用於所有安全性小工具
- 調查結果篩選條件 – 適用於顯示調查結果資料的安全性小工具
- 資源篩選條件 – 適用於顯示資源資料的安全小工具

您可以使用 和/或 運算子連接篩選條件，然後在下拉式清單中選擇儲存新的篩選條件集，以建立篩選條件集。

套用至公開調查結果趨勢小工具和威脅調查結果趨勢小工具的篩選條件

目前，這些小工具支援的篩選條件包括下列項目：

- 帳戶 ID
- 尋找類別名稱
- 調查結果類型
- 產品名稱
- 區域

- 狀態

套用至資源趨勢小工具的篩選條件

目前，此小工具支援的篩選條件包括下列項目：

- 帳戶 ID
- 區域
- 資源類別
- Resource Type (資源類型)

篩選條件未套用至小工具



如果小工具不支援篩選條件，則篩選條件不會套用至小工具。在此情況下，小工具會顯示警告訊息，讓您知道有多少篩選條件未套用，並列出它不支援哪些篩選條件的名稱。

檢視 Security Hub 中資源的詳細資訊

資源頁面會追蹤您帳戶和組織的常見資源。您可以在導覽窗格中選擇資源，以存取 Security Hub 主控台資源頁面。資源頁面的優點是可協助您監控安全狀態、組織資源，以及檢閱資源的詳細資訊。選擇資源類型時，您可以檢閱與資源類型相關聯的所有資源。您可以檢閱與資源相關聯的任何問題清單。資源頁面中可用的資源類型包括 AWS 安全服務涵蓋的任何帳戶中的資源，將調查結果提供給 Security Hub。

Note

委派管理員可以檢視與成員帳戶相關聯的所有資源。如果您已設定住家 AWS 區域，您可以從 AWS 區域連結檢視您住家中的所有資源 AWS 區域。

如果您選擇資源，您可以檢閱該資源的詳細資訊。這些詳細資訊包括資源名稱、ID、ARN、類型和類別。您可以檢閱與資源相關聯的帳戶 ID、建立資源的時間（時間戳記），以及建立資源的位置 (AWS

區域。您也可以檢閱資源的其他組態詳細資訊。您可以在可複製的 JSON 程式碼片段中找到這些詳細資訊。

如果您從概觀索引標籤切換到調查結果索引標籤，您可以檢閱與資源相關聯的任何調查結果。問題清單索引標籤會顯示每個問題清單的名稱、每個問題清單的類型，以及每個問題清單的嚴重性。您可以依不同的欄位分組問題清單，並使用篩選條件搜尋問題清單。如果您選擇問題清單，您可以檢閱問題清單的概觀，其中包括合規以及如何修復問題清單相關問題的相關資訊。特徵索引標籤會顯示已識別有關資源的每個特徵。您可以檢視用於為資源建立公開調查結果的貢獻性特徵。您也可以查看內容特徵，這些是為資源識別的其他安全項目，但不會直接導致任何暴露問題清單。如果您返回資源，您可以選擇開啟資源，以在主控台中檢閱資源的資源類型。例如，如果資源是 IAM 資源，您可以在 IAM 主控台中開啟資源。

資源頁面提供您組織和搜尋資源的不同方式。您可以依類型將資源分組。例如，您可以依帳戶 ID、問題清單類型 AWS 區域、資源類別、資源名稱和資源類型來分組資源。快速篩選條件可協助您依類別、帳戶和調查結果類型檢閱資源。

Security Hub 和開放式網路安全調查結果格式 (OCSF)

OCSF 概觀

Security Hub 調查結果使用 OCSF 進行格式化，OCSF 是開放原始碼專案，提供可擴展的架構來開發結構描述，以及與廠商無關的核心安全結構描述。廠商和其他資料生產者可以採用並擴展其特定網域的結構描述。資料生產者可以映射不同的結構描述，以協助安全團隊簡化資料擷取和標準化，以便資料科學家和分析師可以使用常見的語言進行威脅偵測和調查。目標是提供在任何環境、應用程式或解決方案中採用的開放標準，同時補充現有的安全標準和程序。

框架由一組資料類型、屬性字典和分類組成。它不限於網路安全網域和事件，但架構的初始重點是網路安全事件的結構描述。OCSF 與儲存格式、資料收集和 Extract-Transform-Load (ETL) 程序無關。網路安全事件的核心結構描述旨在與實作無關。結構描述架構定義檔案和產生的標準化結構描述會寫入為 JSON。

Security Hub 目前支援 OCSF 結構描述 1.6 版中的調查結果。

相關資源

如需 OCSF 及其實作的詳細資訊，請參閱下列資源：

- [公有 OCSF 文件](#)

- [OCSF 延伸用途文件](#)
- [OCSF 核心結構描述參考](#)
- [OCSF 延伸項目登錄檔](#)

AWS OCSF 擴充功能

OCSF [結構描述](#) 可以透過新增屬性、物件、類別、設定檔和事件類別來擴展。結構描述是核心結構描述實體和延伸項目的彙總。

OCSF 的延伸允許特定廠商或客戶透過新增屬性來增強現有的結構描述，以提供網域特定的自訂、改善資料互通性，以及新增更詳細的安全分析內容。

開放式網路安全結構描述架構 (OCSF) 的 AWS 延伸為 OCSF 事件內的雲端資源提供屬性定義。此延伸推出新的 `cloud_resources` 設定檔，以全面的雲端特定資源屬性擴展標準 OCSF `resource_details` 物件，讓安全團隊更深入地了解資源組態、潛在漏洞和關鍵中繼資料，這些中繼資料對於跨雲端環境的有效威脅偵測和調查至關重要。

延伸 `resource_details` 物件

AWS 延伸模組會使用下列屬性參考清單中提及的屬性來延伸 `resource_details` 物件。這些屬性可確保標準化事件架構中跨不同提供者正確識別和分類雲端資源。

AWS OCSF 屬性參考的延伸

[基本屬性](#) 和資源 [特定物件](#) 區段提供每個屬性的範例，這些屬性是 `resource_details` AWS OCSF 延伸的一部分。

每個屬性定義都包含 OCSF 狀態，概述其目前與公有 OCSF 結構描述的關係：

- 現有：此屬性已在標準 OCSF `resource_details` 中，現在是 AWS 延伸模組的一部分。
- 新功能：屬性不是 OCSF 的一部分，並作為 AWS 延伸模組的一部分引入。它不存在於核心 OCSF 結構描述中。
- 已新增至 `resource_details`：屬性是在 OCSF 中定義，但不是 `resource_details` 的一部分。

基本屬性

這些是用於資源識別、位置和基本中繼資料的基本屬性。它們由簡單的資料類型組成，例如字串、時間戳記和陣列。

雲端分割區

資源所在的雲端分割區。

需求

建議

Type

String

OCSF 狀態

現有

範例

```
{
  "resources": [
    {
      "cloud_partition": "aws"
    }
  ]
}
```

擁有者帳戶 ID

資源所屬的 12 位數帳戶識別符。

需求

建議

Type

String

OCSF 狀態

現有

範例

```
{
```

```
"resources": [  
  {  
    "owner": {  
      "account": {  
        "uid": "123456789012"  
      }  
    }  
  }  
]
```

資源類型

識別特定服務和資源的 AWS CloudFormation 資源類型。

需求

必要

Type

String

格式

必須遵循 AWS CloudFormation 資源類型命名慣例：AWS::::<ResourceType>

OCSF 狀態

現有

範例

```
{  
  "resources": [  
    {  
      "type": "AWS::EC2::Instance"  
    }  
  ]  
}
```

資源識別符

雲端資源的唯一識別符（例如 i-1234567890abcdef0）。

需求

建議

Type

String

格式

必須是有效的資源識別符。長度下限為 1。長度上限為 768。

OCSF 狀態

現有

範例

```
{
  "resources": [
    {
      "uid": "i-1234567890abcdef0"
    }
  ]
}
```

替代資源識別符

雲端資源的唯一識別符，通常是 Amazon Resource Name (ARN)。

需求

建議

Type

String

格式

應為有效的 AWS ARN。常見的模式包括：

- "arn:partition:service:region:account-id:resource-id"
- "arn:partition:service:region:account-id:resource-type/resource-id"

- "arn:partition:service:region:account-id:resource-type:resource-id"

注意：某些像 S3 的服務使用變化，例如 `arn:aws:s3:::bucket-name`（不含 region 或 account-id）。

OCSF 狀態

現有

範例

```
{
  "resources": [
    {
      "uid_alt": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
    }
  ]
}
```

```
"{
  "resources": [
    {
      "uid_alt": "arn:aws:s3:::my-bucket-name"
    }
  ]
}"
```

資源名稱

雲端資源的唯一名稱。

需求

建議

Type

String

格式

使用者建立的名稱，其值將取決於環境。

OCSF 狀態

現有

範例

```
{
  "resources": [
    {
      "name": "My-Server-1"
    }
  ]
}
```

雲端區域

資源所在的 AWS 區域。

需求

建議

Type

String

格式

有效的雲端區域識別符（例如 us-east-1、eu-west-1、ap-southeast-2）

OCSF 狀態

現有

範例

```
{
  "resources": [
    {
      "region": "us-west-2"
    }
  ]
}
```

```
}
```

資源建立時間

資源建立的時間。

需求

建議

Type

時間戳記

格式

Unix 時間戳記，自 epoch 起以毫秒為單位 (1970 年 1 月 1 日，00 : 00 : 00 UTC)

OCSF 狀態

現有

範例

```
{
  "resources": [
    {
      "created_time": 1762019193000
    }
  ]
}
```

Tags (標籤)

資源中繼資料和組織的鍵值對。

需求

建議

Type

索引鍵陣列：值物件

格式

允許 定義 key : value 對的一般物件。

OCSF 狀態

現有

範例

```
{
  "resources": [
    {
      "tags": [
        {
          "name": "Environment",
          "value": "Production"
        },
        {
          "name": "Owner",
          "value": "SecurityTeam"
        }
      ]
    }
  ]
}
```

IP Address (IP 地址)

與執行個體相關聯的 IP 地址，採用 IPv4 或 IPv6 格式。

需求

選用

Type

String

格式

有效的 IPv4 或 IPv6 地址

OCSF 狀態

現有

範例

```
{
  "resources": [
    {
      "ip": "10.0.1.25"
    }
  ]
}
```

IP 地址

與裝置相關聯的 IP 地址陣列 (IPv4 或 IPv6)。這些可能包括公有和私有 IP 地址。

需求

選用

Type

IP 地址陣列

OCSF 狀態

新增

範例

```
{
  "resources": [
    {
      "ip_addresses": ["10.0.1.25", "52.12.34.56"]
    }
  ]
}
```

VPC UID

資源所在的 VPC ID。

需求

選用

Type

String

格式

VPC 識別符 (例如 vpc-12345678900)

OCSF 狀態

已新增至 resource_details

範例

```
{
  "resources": [
    {
      "vpc_uid": "vpc-0a1b2c3d4e5f6g7h8"
    }
  ]
}
```

具有基本屬性的資源物件範例

```
{
  "resources": [
    {
      "cloud_partition": "aws",
      "owner": {
        "account": {
          "uid": "123456789012"
        }
      },
      "region": "us-east-1",
      "type": "AWS::EC2::NetworkInterface",
      "uid": "eni-03e6c892dd45e836c",
      "uid_alt": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-03e6c892dd45e836c",
      "zone": "us-east-1f",
      "vpc_uid": "vpc-0ef6045717b0362f6"
    }
  ]
}
```

資源特定物件

這些是複雜的巢狀物件，可提供特定資源類型和服務的詳細資訊。每個物件都包含具有服務特定組態和中繼資料的多個欄位和子物件。

裝置

運算資源的增強型雲端執行個體屬性，包括加密詳細資訊、映像資訊、執行個體描述檔和啟動時間。

需求

選用

Type

物件

OCSF 狀態

已新增至 `resource_details`。請參閱 OCSF [裝置](#) 物件定義。

AWS 延伸項目會將下列屬性新增至此物件：

- `encryption_details` - 資源的加密詳細資訊
- `image` - 影像資訊
- `instance_profile` - 要與執行個體建立關聯的 IAM 執行個體描述檔
- `launch_time` - 執行個體啟動的時間
- `uid_alt` - 資源的 Amazon Resource Name (ARN)

範例

```
{
  "device": {
    "image": {
      "uid": "ami-99999999",
      "name": "LoadTestAMI-Current"
    },
    "instance_profile": {
      "uid": "LoadTestingInstanceId",
      "uid_alt": "arn:aws:iam::012345678999:instance-profile/generated"
    },
  },
}
```

```
{
  "launch_time": 1762019193000,
  "launch_time_dt": "2025-08-02T02:05:06Z",
  "model": "m3.xlarge",
  "network_interfaces": [
    {
      "ip": "198.51.100.0",
      "security_groups": [
        {
          "name": "LoadTestingSecurityGroupName",
          "uid": "LoadTestingSecurityId"
        }
      ],
      "uid": "eni-abcdef12"
    }
  ],
  "type": "Virtual",
  "type_id": 6,
  "uid": "i-99999999"
}
```

網路介面

網路介面詳細資訊和組態，包括附件和安全群組。

需求

選用

Type

物件

OCSF 狀態

已新增至 resource_details。請參閱 OCSF [網路介面](#) 物件定義。

AWS 延伸項目會將下列屬性新增至此物件：

- attachments - 網路介面附件的相關資訊
- security_groups - 安全群組唯一識別符陣列
- uid_alt - 資源的 Amazon Resource Name (ARN)

範例

```
{
  "network_interface": {
    "uid": "eni-0a1b2c3d4e5f6g7h8",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-0a1b2c3d4e5f6g7h8",
    "name": "prod-web-server-eni",
    "attachments": [
      {
        "uid": "eni-attach-0abcd1234efgh5678",
        "instance_uid": "i-0123456789abcdef0",
        "name": "/dev/eth0",
        "state": "attached",
        "attach_time": 1762019193000
      }
    ],
    "security_groups": [
      {
        "uid": "sg-0a1b2c3d4e5f6g7h8",
        "name": "web-server-sg"
      },
      {
        "uid": "sg-9i8h7g6f5e4d3c2b1",
        "name": "ssh-access-sg"
      }
    ]
  }
}
```

儲存裝置

儲存裝置詳細資訊，包括附件、加密和快照資訊。

需求

選用

Type

物件

OCSF 狀態

新增

儲存裝置物件包含下列屬性：

- name - 儲存裝置的名稱
- uid - 儲存裝置的唯一識別符
- attachments - 儲存裝置附件
- encryption_details - 儲存裝置加密金鑰
- is_encrypted - 儲存裝置是否已加密（必要）
- snapshot_id - 儲存裝置快照識別符
- uid_alt - 資源的 Amazon Resource Name (ARN)

範例

```
{
  "storage_device": {
    "is_encrypted": false,
    "name": "LocalVolumeDeviceName1",
    "snapshot_id": "snap-12345678901234567",
    "uid": "vol-09d5050dea915943d",
    "uid_alt": "arn:aws:ec2:us-west-2:123456789000:volume/vol-09d5050dea915943d"
  }
}
```

資料庫

資料庫執行個體屬性，包括引擎類型、端點和使用者資訊。

需求

選用

Type

物件

OCSF 狀態

已新增至 resource_details。請參閱 OCSF [資料庫](#) 物件定義。

AWS 延伸項目會將下列屬性新增至此物件：

- cluster_uid - 資料庫叢集識別符
- db_endpoint - 資料庫端點
- encryption_details - 資料庫加密詳細資訊
- engine - 資料庫引擎名稱（例如 mysql）
- is_encrypted - 資料庫是否已加密
- is_iam_authentication - 是否啟用 IAM 身分驗證
- is_public - 資料庫是否可公開存取
- port - 資料庫連接埠號碼
- security_groups - 與資料庫執行個體相關聯的 VPC 安全群組陣列
- snapshot_details - 資料庫快照詳細資訊
- status - 資料庫狀態（例如可用）
- subnet_group - 資料庫子網路群組是 VPC 中的子網路集合
- uid_alt - 資源的 Amazon Resource Name (ARN)
- user - 資料庫使用者
- version - 資料庫版本

範例

```
{
  "database": {
    "cluster_uid": "SampleDBClusterId",
    "engine": "mysql",
    "is_iam_authentication": true,
    "is_public": false,
    "type": "Relational",
    "type_id": 1,
    "uid": "SampleDBId",
    "version": "13.6"
  }
}
```

資料庫叢集

資料庫執行個體屬性，包括引擎類型、端點和使用者資訊。

需求

選用

Type

物件

OCSF 狀態

新增

資料庫物件包含下列屬性：

- uid - 資料庫叢集的唯一識別符
- uid_alt - 資源的 Amazon Resource Name (ARN)
- name - 資料庫叢集的名稱
- status - 資料庫叢集狀態
- engine - 與叢集相關聯的引擎
- version - 資料庫叢集版本
- cluster_members - 屬於叢集的資料庫執行個體清單
- security_groups - 與叢集相關聯的安全群組陣列
- is_encrypted - 資料庫叢集是否已加密
- is_iam_authentication - 是否啟用 IAM 身分驗證
- encryption_details - 資料庫叢集加密詳細資訊
- subnet_group - 與叢集相關聯的子網路群組
- port - 資料庫叢集連接埠號碼
- zones - 可用區域的清單
- db_endpoint - 資料庫叢集端點
- snapshot_details - 資料庫快照的詳細資訊

範例

```
{
  "db_cluster": {
    "uid": "production-aurora-cluster",
    "uid_alt": "arn:aws:rds:us-east-1:123456789012:cluster:production-aurora-cluster",
    "name": "production-aurora-cluster",
    "status": "available",
    "engine": "aurora-mysql",
    "version": "8.0.mysql_aurora.3.04.0",
    "cluster_members": [
      "instance-1",
      "instance-2"
    ],
    "security_groups": [
      {
        "uid": "sg-0a1b2c3d4e5f6g7h8",
        "name": "db-security-group"
      }
    ],
    "is_encrypted": true,
    "is_iam_authentication": true,
    "encryption_details": {
      "key_uid": "arn:aws:kms:us-east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    },
    "subnet_group": {
      "uid": "production-db-subnet-group"
    },
    "port": 3306,
    "zones": [
      "us-east-1a",
      "us-east-1b",
      "us-east-1c"
    ],
    "db_endpoint": {
      "name": "production-aurora-cluster.cluster-abc123xyz.us-east-1.rds.amazonaws.com",
      "port": 3306
    }
  }
}
```

雲端函數

無伺服器函數的雲端函數屬性，包括處理常式、layer 和執行時間組態。

需求

選用

Type

物件

OCSF 狀態

新增

雲端函數物件包含下列屬性：

- name - 雲端函數的名稱
- uid - 雲端函數的唯一識別符
- uid_alt - 資源的 Amazon Resource Name (ARN)
- encryption_details - 雲端函數加密詳細資訊
- handler - 函數程式碼中處理事件的方法
- layers - 包含補充程式碼或資料的雲端函數層清單
- runtime - 雲端函數語言特定環境
- security_groups - 與雲端函數相關聯的安全群組陣列
- subnet_info_list - 與雲端函數相關聯的子網路詳細資訊
- user - 授予 cloud_function 存取服務許可的 IAM 實體詳細資訊
- version - 雲端函數版本
- vpc_uid - 如果雲端函數位於 VPC 中，VPC 的唯一識別符

範例

```
{
  "cloud_function": {
    "name": "my-lambda-function",
    "uid": "my-lambda-function",
    "uid_alt": "arn:aws:lambda:us-east-1:123456789012:function:my-lambda-function",
```

```
{
  "handler": "index.handler",
  "runtime": "python3.11",
  "version": "$LATEST",
  "layers": [
    {
      "name": "my-layer",
      "uid_alt": "arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1",
      "version": "1"
    }
  ],
  "security_groups": [
    {
      "name": "lambda-security-group",
      "uid": "sg-0123456789abcdef0"
    }
  ],
  "subnet_info_list": [
    {
      "uid": "subnet-0a1b2c3d4e5f6g7h8"
    }
  ],
  "vpc_uid": "vpc-0ef6045717b0362f6"
}
```

Databucket

S3 儲存貯體或資料儲存屬性。

需求

選用

Type

物件

OCSF 狀態

已新增至 resource_details。請參閱 OCSF [Databucket](#) 物件定義。

注意：AWS 延伸項目會將此物件新增至 resource_details。核心 OCSF Databucket 物件不使用其他屬性。

範例

```
{
  "databucket": {
    "type": "S3",
    "type_id": 1,
    "uid": "my-bucket-name"
  }
}
```

影像

運算資源的影像資訊，包括平台和用量詳細資訊。

需求

選用

Type

物件

OCSF 狀態

已新增至 `resource_details`。請參閱 OCSF [Image](#) 物件定義。

AWS 延伸項目會將下列屬性新增至此物件：

- `platform` - 映像的作業系統平台
- `in_use_count` - 使用此映像的資源計數

範例

```
{
  "image": {
    "uid": "ami-0abcdef1234567890",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:image/ami-0abcdef1234567890",
    "name": "my-custom-ami",
    "platform": "AMAZON_LINUX_2",
    "in_use_count": 2
  }
}
```



```
}
```

子網路資訊

資源所在的子網路詳細資訊。

需求

選用

Type

物件

OCSF 狀態

新增

子網路資訊物件包含下列屬性：

- uid - 子網路的唯一識別符
- uid_alt - 資源的 Amazon Resource Name (ARN)
- name - 子網路的名稱
- zone - 可用區域
- ip_count - 子網路中的 IP 地址數量
- cidr_block - 子網路的 CIDR 區塊
- is_default - 這是否為預設子網路
- is_public - 子網路是否可公開存取
- state - 子網路的狀態
- vpc_uid - 子網路所在的 VPC ID

範例

```
{  
  "subnet_info": {  
    "uid": "subnet-0a1b2c3d4e5f6g7h8",
```

```
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:subnet/subnet-0a1b2c3d4e5f6g7h8",
    "name": "production-web-subnet-1a",
    "zone": "us-east-1a",
    "ip_count": 251,
    "cidr_block": "10.0.1.0/24",
    "is_default": false,
    "is_public": true,
    "state": "available",
    "vpc_uid": "vpc-0123456789abcdef0"
  }
}
```

使用者

IAM 使用者屬性，包括執行個體描述檔和政策。

需求

選用

Type

物件

OCSF 狀態

已新增至 resource_details。請參閱 OCSF [使用者](#) 物件定義。

使用者物件包含下列屬性：

- instance_profiles - 連接至雲端執行個體的執行個體描述檔清單
- policies - 為使用者、群組、角色和資源指派許可的政策

範例

```
{
  "user": {
    "type_id": 1,
    "uid": "AIDACKCEVSQ6C2EXAMPLE",
    "uid_alt": "arn:aws:iam::123456789012:user/developers/john.doe",
    "name": "john.doe",
```

```
{
  "type": "User",
  "groups": [
    {
      "name": "Developers"
    },
    {
      "name": "ReadOnlyAccess"
    }
  ],
  "policies": [
    {
      "name": "AmazonS3ReadOnlyAccess"
    },
    {
      "name": "AmazonEC2ReadOnlyAccess"
    }
  ]
}
```

Security Hub 中的涵蓋範圍調查結果

Security Hub 的涵蓋範圍調查結果可讓您了解哪些 AWS 安全功能已啟用，以及獨立帳戶或組織成員帳戶中的涵蓋範圍可能存在差距之處。涵蓋範圍調查結果目前支援報告針對 Amazon GuardDuty、Amazon Inspector、Amazon Macie 和 AWS Security Hub CSPM 啟用哪些服務和功能。這些問題清單會出現在 Security Hub 儀表板的安全涵蓋範圍小工具中，能夠依特定安全功能深入了解更詳細的檢視。

限制

- 對於成員帳戶，涵蓋範圍資訊會跨連結彙總 AWS 區域，但僅適用於該成員帳戶。
- 未加入 Security Hub 的帳戶不會顯示涵蓋範圍資訊。

AWS Security Hub CSPM 的涵蓋範圍調查結果

Security Hub CSPM 涵蓋範圍調查結果會評估帳戶中是否啟用合格的狀態管理安全標準。啟用任何 Security Hub CSPM 標準將符合資格，但 AWS Control Tower 和 資源標記標準除外。

啟用 Security Hub CSPM 時，最多可能需要 24 小時才能偵測預設啟用的標準。

Amazon GuardDuty 的涵蓋範圍調查結果

GuardDuty 涵蓋範圍調查結果會評估是否啟用 GuardDuty，以及在 中啟用哪些 GuardDuty 功能 AWS 帳戶：

- 適用於 Amazon EC2 的 GuardDuty 惡意軟體防護 – 掃描 Amazon EC2 執行個體是否有潛在的惡意軟體
- GuardDuty Amazon EKS 保護 – 監控 Kubernetes 稽核日誌是否有 Amazon EKS 叢集中的威脅
- GuardDuty Lambda 保護 – 分析 Lambda 函數叫用是否有潛在威脅
- GuardDuty Amazon S3 保護 – 分析對 Amazon S3 儲存貯體的潛在威脅的資料事件
- GuardDuty Amazon RDS 保護 – 監控對 Amazon RDS 資料庫的威脅
- GuardDuty 執行期監控 – 即時監控 Amazon EC2 執行個體中的執行期行為
- GuardDuty 基礎涵蓋 – 啟用 GuardDuty 時自動開啟的基準 GuardDuty 功能

Note

對於 GuardDuty 基礎涵蓋範圍，表示功能已關閉的涵蓋範圍調查結果在帳戶中未啟用平均 GuardDuty。

GuardDuty 涵蓋範圍的更新最多可能需要 24 小時，才能反映組織中所有成員帳戶。

Amazon Inspector 的涵蓋範圍調查結果

Amazon Inspector 涵蓋範圍調查結果會評估 Amazon Inspector 是否已啟用，以及在帳戶中啟用哪些功能：

- Inspector EC2 掃描 – 掃描 Amazon EC2 執行個體是否有漏洞
- Inspector ECR 掃描 – 掃描 Amazon ECR 容器映像是否有漏洞
- Inspector Lambda 標準掃描 – 掃描 Lambda 函數是否有漏洞
- Inspector Lambda 程式碼掃描 – 掃描 Lambda 程式碼函數是否有程式碼漏洞

Amazon Macie 的涵蓋範圍調查結果

Macie 涵蓋範圍調查結果會評估 Macie 是否已啟用 AWS 帳戶：

- Macie 自動化敏感資料探索涵蓋範圍 – 持續評估 Amazon S3 資料資產的敏感資料。

更新涵蓋範圍問題清單的 Macie 自動化敏感資料探索最多可能需要 24 小時，才能反映組織中所有成員帳戶。

隱藏涵蓋範圍調查結果

根據預設，安全性涵蓋範圍調查結果會評估為帳戶和區域啟用哪些 Amazon GuardDuty、Amazon Inspector、Amazon Macie 和 AWS Security Hub CSPM 功能。如果某些安全功能不適用於您或屬於可接受的風險，您可以使用隱藏功能來隱藏涵蓋範圍問題清單，類似於所有其他問題清單。禁止涵蓋範圍調查結果時，不會包含在安全涵蓋範圍小工具內的涵蓋範圍計算中，而且小工具會顯示已透過禁止涵蓋範圍調查結果排除安全功能涵蓋範圍訊息，後面接著已禁止的調查結果數量計數。

在 Security Hub 中隱藏涵蓋範圍調查結果

1. 檢視安全涵蓋範圍小工具時，請選擇涵蓋的百分比連結。
2. 從涵蓋範圍快顯視窗中選擇檢視涵蓋範圍問題清單。狀態為 New 的每個問題清單都將是概述觀察到的涵蓋範圍差距的問題清單。
3. 按一下您要隱藏的每個調查結果旁邊的核取方塊。
4. 在頁面頂端，選擇更新狀態，然後選擇隱藏。
5. 在將狀態設定為隱藏對話方塊中，選擇性地輸入備註，詳細說明變更狀態的原因。然後選擇設定狀態。

Security Hub 中的暴露問題清單

Security Hub 中的公開調查結果代表多個安全訊號的相互關聯，這些訊號可識別您 AWS 環境中的潛在安全風險。公開調查結果透過自動分析漏洞、組態、威脅和資源關係的組合，協助您了解並排定安全風險的優先順序。曝光問題清單包含特徵和訊號。訊號可以包含一或多個類型的曝光特徵。當來自 Security Hub CSPM、Amazon Inspector、GuardDuty、Macie 或其他 AWS 服務的訊號指出存在暴露時，Security Hub 會產生暴露調查結果。資源最多可以是一個暴露調查結果中的主要資源。如果資源沒有任何暴露特徵或特徵不足，Security Hub 不會為該資源產生暴露調查結果。

公開調查結果的運作方式

Security Hub 會透過以下方式產生公開調查結果：

- 分析來自多個 AWS 安全服務的訊號：Security Hub 會持續收集和分析來自多個安全服務 AWS 的安全訊號。它會從 GuardDuty 擷取問題清單以進行威脅偵測、Amazon Inspector 用於漏洞評估、Security Hub CSPM 用於組態檢查，以及 Macie 用於敏感資料暴露。這些訊號是透過進階相互關聯引擎處理，以識別潛在的安全風險。
- 評估資源組態和關係：系統會根據安全最佳實務執行資源組態的詳細評估。它會檢查服務特定的設定、合規要求和安全控制。此分析有助於識別在與其他因素結合時可能導致安全漏洞的錯誤組態。
- 評估網路連線能力：暴露問題清單的重要組成部分是網路連線能力的評估。系統會評估網際網路暴露和內部網路存取路徑。它會分析安全群組組態和網路 ACL 設定，以判斷潛在的攻擊向量。此分析有助於識別可能不小心暴露於未經授權存取的資源。
- 相互關聯相關的安全問題：相互關聯引擎會映射 AWS 資源之間的關係，分析它們如何互動並識別潛在的安全問題。它會檢查 IAM 許可、角色和資源存取模式，以了解更廣泛的安全內容。此程序有助於識別由於看似無辜的個別組態組合而可能存在的安全風險。

公開調查結果的元件

每個公開調查結果包括：

- 潛在安全風險的標題和描述 - 每個暴露調查結果都包含明確、描述性的標題，可立即傳達安全風險的性質。描述提供有關潛在安全影響、受影響的資源，以及公開的更廣泛內容的詳細資訊。此資訊有助於安全團隊快速了解和評估風險。
- 嚴重性分類（關鍵、高、中、低）：
 - 嚴重嚴重性表示由於高度可能的入侵和重大的潛在影響，需要立即關注。這些調查結果通常代表容易發現和可利用的漏洞。
 - 高嚴重性表示需要優先關注，具有中度到高度的入侵可能性和重大的潛在影響。這些調查結果可能相對容易利用，但可能需要特定條件。
 - 中等嚴重性表示需要排程注意，具有較低的入侵可能性和中等的潛在影響。這些調查結果通常需要更複雜的利用方法。
 - 低嚴重性表示需要定期關注，但對漏洞的潛在影響有限。這些調查結果通常難以利用，並呈現最低風險。
- 導致曝光的貢獻特徵：貢獻特徵代表導致曝光調查結果的主要因素。這些包括直接安全漏洞、組態問題、網路暴露條件和資源許可設定。每個特徵都會提供有關它如何對整體安全風險做出貢獻的特定詳細資訊。
- 攻擊路徑視覺化：攻擊路徑視覺化提供互動式圖表，顯示潛在攻擊者如何利用已識別的暴露。它映射資源關係、網路路徑和潛在影響流程，協助安全團隊了解風險的完整範圍，並規劃有效的修補策略。

- 詳細的修補指引：每個暴露調查結果都包含詳細的修補指引，其中包含具體、可行的步驟，以解決已識別的風險。本指南包含最佳實務建議、組態校正步驟和優先動作項目。此指引專為特定暴露案例量身打造，並考慮涉及 AWS 的服務。
- 資源組態詳細資訊：建立調查結果時的資源組態，以及 Security Hub 資源庫存儀表板中資源的目前組態。
- 提供其他安全內容的上下文特徵：上下文特徵是由 Security Hub 識別但未用於建立公開調查結果的其他安全標記。

來自 IAM Access Analyzer 的未使用存取資訊可以在公開調查結果中顯示為內容特徵。當連接至資源的 IAM 角色具有未使用的許可時，Security Hub 會在公開詳細資訊檢視中包含此資訊作為內容特徵。例如，如果 Amazon EC2 執行個體具有軟體漏洞，且其連接的 IAM 角色在 5 個服務中有 47 個未使用的許可，則公開調查結果會顯示未使用的許可作為補充內容。這可協助您了解潛在的爆量半徑：具有高權限 IAM 角色的易受攻擊資源比具有最低權限許可的資源具有更高的風險，因為遭入侵的資源可能會使用這些未使用的許可來提升存取權。

下列資源類型可以在其公開調查結果中顯示未使用的存取內容特徵：

- Amazon Elastic Compute Cloud 執行個體
- AWS Lambda 函數
- Amazon Elastic Container Service 服務
- Amazon Elastic Kubernetes Service 叢集
- IAM 使用者（直接）

嚴重性分類

公開調查結果的分類依據如下：

- 易於探索
- 易於利用
- 入侵的可能性
- 公有意識
- 潛在影響

如需詳細資訊，請參閱[暴露問題清單嚴重性分類](#)。

公開調查結果的優點

- 透過自動化相互關聯減少手動分析：公開調查結果透過自動化相互關聯和智慧風險優先順序，大幅減少安全性分析所需的時間和精力。Security Hub 會持續監控您的 AWS 環境，自動識別和關聯手動審核可能遺漏的安全風險。
- 安全風險的優先順序檢視：Security Hub 採用複雜的風險評估演算法，根據嚴重性、影響、資源重要性和入侵可能性來排定暴露的優先順序。這有助於安全團隊先專注於最重要的風險，從而提高安全操作的效率。

公開問題清單的來源

公開調查結果包含來自以下項目的資料：

- Amazon GuardDuty 整合可在公開調查結果內提供持續的威脅偵測功能。它會監控惡意活動、潛在的帳戶入侵和行為異常。系統會將這些威脅調查結果納入更廣泛的暴露分析，協助識別威脅何時與其他安全問題結合，以產生重大風險。
- Amazon Inspector 會將重要的漏洞評估資料提供給公開調查結果。它提供有關網路連線能力、軟體漏洞和安全最佳實務違規的詳細資訊。此整合有助於了解如何透過已識別的攻擊路徑利用漏洞。
- AWS Security Hub CSPM 可確保在公開分析中考慮組態合規和安全標準。它根據已建立的安全控制和最佳實務評估資源，為了解以組態為基礎的風險奠定基礎。
- Amazon Macie 使用敏感資料探索和分類功能來增強公開調查結果。它可識別您 AWS 環境中存在的敏感資料，並評估潛在的隱私權風險，協助了解已識別暴露的潛在影響。

最佳實務

- 定期審查暴露調查結果：有效的暴露管理需要結構化的審查程序。組織應每日審查關鍵暴露、每週評估整體暴露狀態、每月趨勢分析，以及每季安全性狀態評估。這種分層方法可確保適當關注立即風險和長期安全趨勢。
- 排定關鍵和高嚴重性暴露的優先順序：成功的暴露管理取決於有效的風險優先順序。組織應先專注於關鍵暴露，同時考慮資源重要性和業務影響。這種以風險為基礎的方法有助於確保安全工作符合業務優先事項，並最大限度地降低風險。
- 實作建議的修補步驟：暴露修補應遵循系統性方法。組織應謹慎實作建議的修補步驟、維護詳細的變更文件、徹底測試修改，以及驗證實作修正的有效性。這種有條不紊的方法有助於確保成功降低風險，同時避免意外的後果。

- 設定自動化回應規則：最大化公開調查結果的值需要有效的自動化。組織應實作自動化回應規則、設定適當的通知、建立有效的工作流程，以及維護完整的稽核線索。此自動化有助於確保對已識別的暴露做出一致且及時的回應，同時減少手動工作量。

Security Hub 中公開調查結果的支援資源類型

AWS Security Hub 會為下列類型的 AWS 資源產生公開調查結果：

- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::ECS::Service
- AWS::EKS::Cluster
- AWS::IAM::User
- AWS::Lambda::Function
- AWS::RDS::DBInstance
- AWS::S3::Bucket

Security Hub 會為每個主要資源產生一個暴露問題清單。如果資源沒有任何暴露特徵或特徵不足，Security Hub 不會為該資源產生暴露調查結果。

Security Hub 中支援的特徵類型

AWS 當 Security Hub CSPM 控制調查結果以及 Amazon Inspector AWS 服務等其他支援的問題清單包含資源的暴露特徵時，AWS Security Hub 會產生暴露問題清單。下表提供有關支援特徵類型的資訊。

特徵類型	說明	來源	受影響的資源
可擔任性	指出具有已終止 AWS Identity and Access Management 許可的資源	來自 的資源組態 AWS Config	AWS 具有關聯 AWS Identity and Access Management 角 色的資源
設定錯誤	指出設定錯誤的資源	AWS Security Hub CSPM 控制	所有資源類型

特徵類型	說明	來源	受影響的資源
		調查結果、Amazon GuardDuty 威脅調查結果，以及中資源確認的相關資訊 AWS Config。	
可連線性	指出資源的開放式網路路徑	AWS Security Hub CSPM 控制調查結果、Amazon GuardDuty 威脅調查結果，以及 Amazon Inspector 網路連線能力調查結果。	Amazon EC2 執行個體、Amazon EKS 叢集、Lambda 函數和 Amazon S3 儲存貯體
敏感資料	表示資源包含敏感資料	Macie 敏感資料調查結果	Amazon S3 儲存貯體
漏洞	表示資源有弱點，而威脅來源可能會利用此弱點。	Amazon Inspector 套件漏洞調查結果和 Amazon GuardDuty Amazon EC2 惡意軟體調查結果。	Amazon EC2 執行個體、Amazon ECS 服務、Amazon EKS 叢集和 Lambda 函數

每個特徵都可以與多個標題相關聯，這些標題提供有關影響資源之暴露的詳細資訊。例如，您可能會在 EC2 暴露問題清單的詳細資訊中看到漏洞特徵的可用 Exploit 標題。

產生暴露問題清單

Security Hub 會以近乎即時的方式產生公開調查結果。擷取新的安全性問題清單並更新現有的問題清單時，Security Hub 會近乎即時地產生或更新公開問題清單。Security Hub 會為每個資源 ID 產生一個公開調查結果。

如果資源沒有任何暴露特徵或特徵不足，Security Hub 不會為該資源產生暴露調查結果。Security Hub 不會針對公開調查結果不支援的資源類型發佈公開調查結果。當資源具有大量特徵和組合時，Security Hub 會產生公開調查結果。特徵的數量和組合也會決定曝光調查結果的嚴重性等級。

範例曝光問題清單

AWS Security Hub 會將開放網路安全結構描述架構 (OCSF) 中的暴露問題清單標準化。

範例曝光問題清單

在下列範例公開調查結果中，`related_events` 參數包含公開調查結果的唯一詳細資訊，例如貢獻調查結果。貢獻調查結果是與暴露調查結果相關聯的特徵和訊號。單一貢獻調查結果可以包含一或多個特徵。`observables` 參數可識別與貢獻調查結果相關聯的資源。這可以與 `resources` 參數不同，參數會識別與公開調查結果相關聯的資源。

```
{
  "activity_id": 1,
  "activity_name": "Create",
  "category_name": "Findings",
  "category_uid": 2,
  "class_name": "Detection Finding",
  "class_uid": 2004,
  "cloud": {
    "account": {
      "uid": "123456789012",
      "name": "production-application"
    },
    "cloud_partition": "aws",
    "provider": "AWS",
    "region": "us-east-1"
  },
  "finding_info": {
    "analytic": {
      "name": "Exposure",
      "type": "Rule",
      "type_id": 1,
      "uid": "0.0.1"
    }
  }
}
```

```

    },
    "created_time_dt": "2024-11-15T21:39:26.337224100Z",
    "desc": "Publicly invocable Lambda function executed outside of VPC has
vulnerability with known exploit that can be exploited from remote network",
    "finding.info.modified_time_dt": "2024-11-15T21:39:26.337224100Z",
    "related_events_count": 3,
    "related_events": [
      {
        "tags": [
          {
            "name": "Vulnerability",
            "values": [
              "Attack Vector Network",
              "EPSS Level >= High",
              "EPSS Level >= Medium",
              "Exploit Available",
              "No Privileges Required",
              "No User Interaction Required",
              "Vulnerable"
            ]
          }
        ],
        "product": {
          "uid": "arn:aws:securityhub:us-east-1::productv2/aws/inspector"
        },
        "observables": [
          {
            "type": "Resource UID",
            "type_id": 10,
            "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
          }
        ],
        "type": "Finding",
        "title": "CVE-2023-33246 - org.apache.rocketmq:rocketmq-controller",
        "uid": "arn:aws:inspector2:us-
east-1:123456789012:finding/1234567890abcdef0"
      },
      {
        "tags": [
          {
            "name": "Reachability",
            "values": [
              "Publicly Invocable"
            ]
          }
        ]
      }
    ]
  }
}

```

```

        ]
      }
    ],
    "product": {
      "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
    },
    "observables": [
      {
        "type": "Resource UID",
        "type_id": 10,
        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
      }
    ],
    "type": "Finding",
    "title": "Lambda function policies should prohibit public access",
    "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
  },
  {
    "tags": [
      {
        "name": "Misconfiguration",
        "values": [
          "Deployed outside VPC"
        ]
      }
    ],
    "product": {
      "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
    },
    "observables": [
      {
        "type": "Resource UID",
        "type_id": 10,
        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
      }
    ],
    "type": "Finding",
    "title": "Lambda functions should be in a VPC",
    "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.3/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  }
}

```

```

    ],
    "title": "Publicly invocable Lambda function executed outside of VPC has
vulnerability with known exploit that can be exploited from remote network",
    "types": [
        "Exposure/Potential Impact/Resource Hijacking"
    ],
    "uid": "arn:aws:securityhub:us-
east-1:123456789012:risk:1234f781c7ae7507f01e2fb460f15ca8fe7f9c95e257698a092cb74a4ea84a42"
},
"metadata": {
    "product": {
        "name": "Security Hub Exposure Analysis",
        "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub-risk",
        "vendor_name": "Amazon"
    },
    "processed_time_dt": "2024-11-15T21:39:58.819Z",
    "profiles": [
        "cloud",
        "datetime"
    ],
    "version": "1.4.0-dev"
},
"resources": [
    {
        "cloud_partition": "aws",
        "region": "us-east-1",
        "tags": [
            {
                "name": "aws:cloudformation:stack-name",
                "value": "LambdaProdStack"
            },
            {
                "name": "aws:cloudformation:stack-id",
                "value": "arn:aws:cloudformation:us-east-1:123456789012:stack/
LambdaProdStack/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
            },
            {
                "name": "aws:cloudformation:logical-id",
                "value": "lambdar3function94D10D40"
            }
        ],
        "type": "AwsLambdaFunction",
        "uid": "arn:aws:lambda:us-east-1:123456789012:application-function"
    }
]

```

```
],
"severity": "Critical",
"severity_id": 5,
"status": "New",
"status_id": 1,
"time": 1731706766337,
"time_dt": "2024-11-15T21:39:26.337224100Z",
"type_name": "Detection Finding: Create",
"type_uid": 200401,
"vendor_attributes": {
  "severity_id": 5,
  "severity": "Critical"
}
}
```

判斷暴露問題清單的嚴重性等級

AWS Security Hub 會為每個曝光調查結果指派預設嚴重性 CRITICAL、MEDIUM、HIGH 或 LOW。嚴重性為 INFORMATIONAL 的公開調查結果不會發佈。Security Hub 使用幾個因素來判斷暴露調查結果的預設嚴重性等級：

- 意識 – 公開程度不是理論上，但具有公開可用或自動化的入侵。這適用於 EC2 執行個體和 Lambda 函數的公開調查結果。
- 易於探索 – 自動化工具，例如連接埠掃描或網際網路搜尋，是否可用於探索具有風險的資源。
- 易於利用 – 威脅行為者可以利用暴露的容易程度。例如，如果存在開放網路路徑或設定錯誤的中繼資料，威脅行為者可以更輕鬆地利用暴露。
- 入侵的可能性 – 曝光在未來 30 天內被利用的可能性。此因素對應於 Exploit Protection Scoring System (EPSS)，並適用於 Amazon EC2 執行個體和 Lambda 函數的公開調查結果。
- 影響 – 執行入侵時的傷害。例如，暴露可能會導致責任損失、可用性損失、因資料暴露而失去機密性，或因資料損毀而失去完整性。

檢閱暴露問題清單

您可以在 Security Hub 主控台和 API 中檢閱所有公開調查結果 [GetFindingsV2](#)。Security Hub 主控台中的公開頁面會顯示所有作用中的公開調查結果。暴露問題清單會透過降低嚴重性來列出。您可以使用新增篩選條件搜尋列新增和移除篩選條件，以篩選您的曝光問題清單。您可以使用依群組下拉式清單來分組您的暴露問題清單。您也可以使用快速篩選條件選單來篩選您的曝光問題清單。

公開調查結果的詳細資訊

您可以檢視公開調查結果的許多詳細資訊。這些詳細資訊在 Security Hub 主控台中分割為標籤。概觀索引標籤提供公開調查結果的金鑰詳細資訊。特徵索引標籤列出與曝光問題清單相關聯的特徵和訊號。資源索引標籤提供與公開調查結果相關聯的資源和資源標籤的詳細資訊。下列清單提供公開調查結果詳細資訊的說明。

- 調查結果標題 – 公開調查結果的標題。
- 嚴重性等級 – 暴露問題清單的嚴重性等級。Security Hub 使用資源的特徵數量和組合來判斷公開調查結果的嚴重性等級。嚴重性等級可以是 CRITICAL、MEDIUM、HIGH 或 LOW。Security Hub 不會發佈嚴重性為 INFORMATIONAL 的公開調查結果。您可以透過 Security Hub Severity 主控台或使用 [BatchUpdateFindingsV2](#) API 操作更新。
- 描述 – 公開調查結果的描述。
- 類型 – 公開調查結果類型的名稱。例如，名稱可能類似 Exposure/Potential Impact/Resource Hijacking。
- 帳戶 – 產生公開調查結果 AWS 帳戶的 ID。
- 年齡 – 指出曝光問題清單處於作用中狀態的時間長度。
- 建立時間 – 指出何時建立公開調查結果的時間戳記。
- 修改時間 – 時間戳記，指出上次更新暴露調查結果的時間。
- 區域 – 產生公開調查結果 AWS 區域的。
- 產品名稱 – 產生公開調查結果的產品名稱。這一律是 Security Hub 暴露偵測。
- 公司名稱 – 產生公開調查結果的公司名稱。這一律是 AWS。
- 活動名稱 – 上次針對調查結果執行的活動名稱。
- 狀態 – 此暴露問題清單的狀態。
- 調查結果 ID – 與公開調查結果相關聯的唯一識別符。
- 潛在攻擊路徑（僅限主控台）– 互動式視覺化，顯示潛在攻擊者如何存取和控制與公開調查結果相關聯的資源。如需詳細資訊，請參閱[使用潛在攻擊路徑圖檢視 Security Hub 中的暴露](#)。
- 特徵 – 識別與曝光調查結果相關聯的特徵類型和特徵標題。在 Security Hub 主控台中，您可以依特徵類型或訊號檢視特徵。這可協助您分析相關公開內容中的貢獻調查結果。
- 修復 – 連結至暴露中識別特徵的特定修復文件。
- 資源 – 識別與公開調查結果相關聯的資源。

檢閱公開調查結果的詳細資訊

本主題說明如何檢閱 AWS Security Hub 主控台和 API 中有關暴露問題清單的詳細資訊。

在 Security Hub 主控台中檢閱公開調查結果的詳細資訊

在 Security Hub 主控台中檢視公開調查結果的詳細資訊

1. 使用您的登入資料登入，然後開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從導覽窗格中，選擇曝光。
3. 選擇您要檢視詳細資訊的公開調查結果。

使用 API 檢閱公開調查結果的詳細資訊

您可以使用 [GetFindingsV2](#) API 或 檢閱暴露問題清單 AWS CLI。您可以使用 `metadata.product.feature.uid` 欄位的 `security-hub/Exposure` 值來篩選所有曝光問題清單。如需詳細資訊，請參閱 [GetFindingsV2](#)。

範例 命令

以下是擷取您帳戶中最近產生的 10 個公開調查結果 AWS CLI 的範例。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
aws securityhub get-findings-v2 \
--max-results '10' \
--filter '{"CompositeFilters": [{"StringFilters":
  [{"FieldName": "metadata.product.feature.uid", "Filter": {"Value": "security-hub/
Exposure", "Comparison": "EQUALS"}} ]}]}'
```

使用潛在攻擊路徑圖檢視 Security Hub 中的暴露

潛在攻擊路徑圖是一種互動式視覺化，顯示潛在攻擊者如何存取和控制與公開調查結果相關聯的資源。您只能在 Security Hub 主控台和公開頁面中存取此圖表。當您檢視公開調查結果的詳細資訊時，概觀索引標籤會包含稱為潛在攻擊路徑的區段。

在概觀索引標籤的此區段中，您可以選擇並拖曳潛在攻擊路徑圖表中的 AWS 資源。您可以使用放大和縮小圖示，專注於攻擊路徑圖的特定區域。您可以透過全螢幕圖示，在全螢幕模式內外展開攻擊路徑圖。圖例會依顏色編碼主要資源、參與資源和貢獻性特徵計數，並在攻擊路徑圖表中顯示特徵類別和特

徵數量。您可以透過選擇資源並選擇檢視資源詳細資訊來檢視資源的詳細資訊。您也可以複製與資源相關聯的 ID 和 AWS 帳戶號碼。具有可連線性特徵的公開調查結果會在攻擊路徑圖表中顯示公有網際網路和收合的網路路徑。您可以選擇折疊的網路路徑節點來檢視此詳細資訊。

修復暴露問題清單

本節中的主題說明不同暴露問題清單的修復步驟 AWS 服務。

[OCSF 格式](#) Remediation 的欄位包含兩個欄位：remediation 和 references。

```
"Remediation": {
  "Recommendation": {
    "remediation":{"desc":"String",
    "references":["string array"]}
  }
},
```

Note

以下各節提供的修補指引可能需要在其他 AWS 資源中進行額外諮詢。

修復 DynamoDB 資料表的曝光

AWS Security Hub 可以產生 DynamoDB 資料表的公開調查結果。

在 Security Hub 主控台上，涉及公開調查結果的 DynamoDB 資料表及其識別資訊會列在調查結果詳細資訊的資源區段中。您可以使用 Security Hub CSPM API [GetFindingsV2](#) 的操作，以程式設計方式擷取資源詳細資訊。

識別暴露調查結果中涉及的資源之後，如果不需要，您可以刪除資源。刪除非必要的資源可以降低您的暴露描述檔和 AWS 成本。如果資源是必要的，請遵循這些建議的修補步驟，以協助降低風險。修復主題會根據特徵類型分割。

單一公開調查結果包含多個修復主題中識別的問題。相反地，您可以透過僅解決一個修補主題來解決暴露問題並降低其嚴重性等級。您的風險修補方法取決於您的組織需求和工作負載。

Note

本主題提供的修補指引可能需要對其他 AWS 資源進行額外諮詢。

內容

- [DynamoDB 中的設定錯誤特性](#)
 - [DynamoDB 資料表已停用point-in-time復原](#)
 - [DynamoDB 資料表未涵蓋在備份計畫中](#)
 - [DynamoDB 資料表已停用刪除保護](#)

DynamoDB 中的設定錯誤特性

以下說明 DynamoDB 資料表的錯誤組態特性和修復步驟。

DynamoDB 資料表已停用point-in-time復原

啟用 DynamoDB point-in-time復原

DynamoDB point-in-time復原可為 DynamoDB 資料表資料提供持續的自動化備份。如需有關如何將 DynamoDB 資料表還原至某個時間點的資訊，請參閱《Amazon [DynamoDB 使用者指南](#)》中的[將 DynamoDB 資料表還原至某個時間點](#)。 DynamoDB

DynamoDB 資料表未涵蓋在備份計畫中

AWS 備份提供集中式服務來設定、管理和自動化跨 AWS 服務的備份，包括 DynamoDB。如果沒有備份計畫，您的資料表會缺少具有可自訂保留期的排程自動備份，進而產生重大的安全風險。攻擊者可能會惡意損毀或刪除您的資料表資料。如果沒有適當的備份，您可能沒有超過Point-in-Time復原時段（如果啟用）的復原選項，可能會導致永久資料遺失。遵循資料保護最佳實務，我們建議您使用備份計畫來涵蓋 DynamoDB 資料表。

建立備份計畫

在建立備份計畫之前，請判斷資料的適當備份頻率和保留期間。如需如何建立備份計畫的資訊，請參閱《Amazon DynamoDB 使用者指南》中的[將資源指派給備份計畫](#)。

DynamoDB 資料表已停用刪除保護

刪除保護可防止意外刪除 DynamoDB 資料表。停用刪除保護時，DynamoDB 資料表很容易透過主控台動作、API 呼叫、CLI 命令或自動化程序進行意外刪除。這可能會讓您的 AWS 環境面臨資料遺失，因為有權存取您 AWS 環境的未經授權實體可能會刻意刪除資料表，導致服務中斷和永久資料遺失。遵循資料保護最佳實務，我們建議為 DynamoDB 資料表啟用資料保護。

啟用刪除保護

如果您管理多個資料表，請考慮使用大量 CloudFormation 更新資料表屬性。您可以修改 CloudFormation 範本以包含 `DeletionProtectionEnabled` 屬性並更新您的堆疊。完成修復後，請確認已在資料表設定索引標籤的額外資訊下拉式清單中啟用刪除保護。

修復 EC2 執行個體的暴露

AWS Security Hub 可以產生 Amazon Elastic Compute Cloud (EC2) 執行個體的公開調查結果。

在 Security Hub 主控台上，涉及公開調查結果的 EC2 執行個體及其識別資訊會列在調查結果詳細資訊的資源區段中。您可以使用 Security Hub CSPM API [GetFindingsV2](#) 的操作，以程式設計方式擷取資源詳細資訊。

識別暴露調查結果中涉及的資源之後，如果不需要，您可以刪除資源。刪除非必要資源可以降低您的暴露描述檔和 AWS 成本。如果資源是必要的，請遵循這些建議的修補步驟，以協助降低風險。修復主題會根據特徵類型分割。

單一公開調查結果包含多個修復主題中識別的問題。相反地，您可以透過僅解決一個修補主題來解決暴露問題並降低其嚴重性等級。您的風險修補方法取決於您的組織需求和工作負載。

Note

本主題提供的修補指引可能需要對其他 AWS 資源進行額外諮詢。

內容

- [EC2 執行個體的錯誤組態特性](#)
 - [EC2 執行個體允許使用第 1 版存取 IMDS](#)
 - [與 Amazon EC2 執行個體相關聯的 IAM 角色具有管理存取政策](#)
 - [與 Amazon EC2 執行個體相關聯的 IAM 角色具有服務管理員政策](#)
 - [Amazon EC2 執行個體具有允許 SSH 或 RDP 存取的安全群組或網路 ACL](#)
 - [Amazon EC2 執行個體具有開啟的安全群組](#)
- [EC2 執行個體的連線能力特性](#)
 - [EC2 執行個體可透過網際網路連線](#)
- [EC2 執行個體的漏洞特性](#)
 - [EC2 執行個體具有網路可攻擊的軟體漏洞，具有高利用率的可能性](#)
 - [Amazon EC2 執行個體具有軟體漏洞](#)

- [EC2 執行個體具有End-Of-Life作業系統](#)
- [EC2 執行個體具有惡意軟體套件](#)
- [EC2 執行個體具有惡意檔案](#)

EC2 執行個體的錯誤組態特性

以下是 EC2 執行個體的錯誤組態特性和建議的修復步驟。

EC2 執行個體允許使用第 1 版存取 IMDS

執行個體中繼資料是 Amazon EC2 執行個體的資料，應用程式可用來設定或管理執行中的執行個體。執行個體中繼資料服務 (IMDS) 是一種執行個體上的元件，可供執行個體上的程式碼用來安全地存取執行個體中繼資料。如果 IMDS 未正確保護，它可能會成為潛在的攻擊媒介，因為它可以存取臨時登入資料和其他敏感組態資料。IMDSv2 透過工作階段導向身分驗證，為中繼資料請求提供更強大的入侵保護，並限制工作階段持續時間。遵循標準安全原則，AWS 建議您將 Amazon EC2 執行個體設定為使用 IMDSv2 並停用 IMDSv1。

測試應用程式相容性

在實作 IMDSv2 之前，請先測試您的執行個體，以確保其與 IMDSv2 的相容性。有些應用程式或指令碼可能需要核心功能的 IMDSv1，並且需要額外的組態。如需測試應用程式相容性之工具和建議路徑的詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[轉換為使用執行個體中繼資料服務第 2 版](#)。

更新執行個體以使用 IMDSv2

修改現有執行個體以使用 IMDSv2。如需詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[修改現有執行個體的執行個體中繼資料選項](#)。

將更新套用至 Auto Scaling 群組中的執行個體

如果您的執行個體是 Auto Scaling 群組的一部分，請使用新組態更新您的啟動範本或啟動組態，並執行執行個體重新整理。

與 Amazon EC2 執行個體相關聯的 IAM 角色具有管理存取政策

管理存取政策為 Amazon EC2 執行個體提供 AWS 服務和資源的廣泛許可。這些政策通常包含執行個體功能不需要的許可。如果 Amazon EC2 執行個體遭到入侵，在 Amazon EC2 執行個體上提供具有管理存取政策的 IAM 身分（而非連接至執行個體描述檔所需的最低許可集）可能會增加攻擊範圍。Amazon EC2 如果執行個體遭到入侵，攻擊者可能會利用這些過多的許可，在您的環境中橫向移動、

存取資料或操作資源。遵循標準安全原則，我們建議您授予最低權限，這表示您只授予執行任務所需的許可。

檢閱和識別管理政策

在 IAM 儀表板中，尋找具有角色名稱的角色。檢閱連接至 IAM 角色的許可政策。如果政策是 AWS 受管政策，請尋找 AdministratorAccess 或 IAMFullAccess。否則，請在政策文件中，尋找具有 "Effect": "Allow", "Action": "*"、和 的陳述式 "Resource": "*"。

實作最低權限存取

將管理政策取代為僅授予執行個體運作所需的特定許可的政策。如需 IAM 角色安全最佳實務的詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的在安全最佳實務中[套用最低權限許可](#)。若要識別不必要的許可，您可以使用 IAM Access Analyzer 來了解如何根據存取歷史記錄修改政策。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[外部和未使用存取的調查結果](#)。或者，您可以建立新的 IAM 角色，以避免使用現有角色影響其他應用程式。在此案例中，建立新的 IAM 角色，然後將新的 IAM 角色與執行個體建立關聯。如需取代執行個體 IAM 角色的說明，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[將 IAM 角色連接至執行個體](#)。

安全組態考量

如果執行個體需要服務層級管理許可，請考慮實作這些額外的安全控制來降低風險：

- 安全組態考量
 - 多重要素驗證 (MFA) – MFA 需要其他形式的身分驗證來新增額外的安全層。即使登入資料遭到入侵，這也有助於防止未經授權的存取。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[需要多重要素驗證 \(MFA\)](#)。
 - IAM 條件 – 設定條件元素可讓您根據來源 IP 或 MFA 存留期等因素，限制何時及如何使用管理許可。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[使用 IAM 政策中的條件來進一步限制存取](#)。
 - 許可界限 – 許可界限會建立角色可擁有的最大許可，為具有管理存取權的角色提供護欄。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[使用許可界限來委派帳戶中的許可管理](#)。

將更新套用至自動擴展群組中的執行個體

對於 AWS 自動擴展群組中的 Amazon EC2 執行個體，請使用新的執行個體描述檔更新啟動範本或啟動組態，並執行執行個體重新整理。如需有關更新啟動範本的資訊，請參閱《Amazon Elastic

Compute Cloud 使用者指南》中的[修改啟動範本（管理啟動範本版本）](#)。如需詳細資訊，請參閱[使用執行個體重新整理來更新 Auto Scaling 群組中的執行個體](#)。如需搭配 Auto Scaling 群組使用 IAM 角色的詳細資訊，請參閱《[Amazon EC2 Auto Scaling 使用者指南](#)》中的在 Amazon EC2 執行個體上執行之應用程式的 IAM 角色。 Amazon EC2 Auto Scaling

與 Amazon EC2 執行個體相關聯的 IAM 角色具有服務管理員政策

服務存取政策為 Amazon EC2 執行個體提供對 AWS 服務和資源的廣泛許可。這些政策通常包含執行個體功能不需要的許可。在 Amazon EC2 執行個體上提供具有管理存取政策的 IAM 身分，而非連接至執行個體描述檔所需的最低許可集，可能會在執行個體遭到入侵時增加攻擊範圍。遵循標準安全原則，我們建議您授予最低權限，這表示您僅授予執行任務所需的許可。

檢閱和識別管理政策

在 IAM 儀表板中，尋找具有角色名稱的角色。檢閱連接至 IAM 角色的許可政策。如果政策是 AWS 受管政策，請尋找 AdministratorAccess 或 IAMFullAccess。否則，請在政策文件中，尋找具有 "Effect": "Allow", "Action": "*"、和 的陳述式 "Resource": "*"。

實作最低權限存取

將服務管理員政策取代為僅授予執行個體運作所需特定許可的政策。如需 IAM 角色安全最佳實務的詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的在安全最佳實務中[套用最低權限許可](#)。若要識別不必要的許可，您可以使用 IAM Access Analyzer 來了解如何根據存取歷史記錄修改政策。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[外部和未使用存取的調查結果](#)。或者，您可以建立新的 IAM 角色，以避免影響使用現有角色的其他應用程式。在此案例中，建立新的 IAM 角色，然後將新的 IAM 角色與執行個體建立關聯。如需取代執行個體 IAM 角色的詳細資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[將 IAM 角色連接至執行個體](#)

安全組態考量

如果執行個體需要服務層級管理許可，請考慮實作這些額外的安全控制來降低風險：

安全組態考量

如果執行個體需要服務層級管理許可，請考慮實作這些額外的安全控制來降低風險：

- 多重要素驗證 (MFA) – MFA 需要其他形式的身分驗證來新增額外的安全層。即使登入資料遭到入侵，這也有助於防止未經授權的存取。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[需要多重要素驗證 \(MFA\)](#)。

- IAM 條件 – 設定條件元素可讓您根據來源 IP 或 MFA 存留期等因素，限制何時及如何使用管理許可。如需詳細資訊，請參閱AWS Identity and Access Management 《使用者指南》中的[使用 IAM 政策中的條件來進一步限制存取](#)。
- 許可界限 – 許可界限會建立角色可擁有的最大許可，為具有管理存取權的角色提供護欄。如需詳細資訊，請參閱AWS Identity and Access Management 《使用者指南》中的[使用許可界限來委派帳戶中的許可管理](#)。

將更新套用至 Auto Scaling 群組中的執行個體

對於 AWS 自動擴展群組中的 Amazon EC2 執行個體，請使用新的執行個體描述檔更新啟動範本或啟動組態，並執行執行個體重新整理。如需有關更新啟動範本的資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[修改啟動範本（管理啟動範本版本）](#)。如需詳細資訊，請參閱[使用執行個體重新整理來更新 Auto Scaling 群組中的執行個體](#)。如需搭配 Auto Scaling 群組使用 IAM 角色的詳細資訊，請參閱《[Amazon EC2 Auto Scaling 使用者指南](#)》中的在 [Amazon EC2 執行個體上執行之應用程式的 IAM 角色](#)。 Amazon EC2 Auto Scaling

Amazon EC2 執行個體具有允許 SSH 或 RDP 存取的安全群組或網路 ACL

SSH 和 RDP 等遠端存取通訊協定可讓使用者從外部位置連線至和管理 Amazon EC2 執行個體。當安全群組允許從網際網路無限制存取這些通訊協定時，它們會允許網際網路存取您的執行個體，以增加 Amazon EC2 執行個體的攻擊面。遵循標準安全原則，AWS 建議您限制遠端存取特定、信任的 IP 地址或範圍。

1. 修改安全群組規則

將對 Amazon EC2 執行個體的存取限制為特定的信任 IP 地址。限制 SSH 和 RDP 對特定信任 IP 地址的存取，或使用 CIDR 表示法指定 IP 範圍（例如 198.168.1.0/24）。若要修改安全群組規則，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[設定安全群組規則](#)。

Amazon EC2 執行個體具有開啟的安全群組

安全群組可做為 Amazon EC2 執行個體的虛擬防火牆，以控制傳入和傳出流量。允許從任何 IP 地址不受限制存取的開放安全群組，可能會讓您的執行個體遭受未經授權的存取。遵循標準安全原則，AWS 建議限制安全群組對特定 IP 地址和連接埠的存取。

檢閱安全群組規則並評估目前的組態

評估哪些連接埠可從廣泛的 IP 範圍開啟和存取，例如 (0.0.0.0/0 or ::/0)。如需檢視安全群組詳細資訊的說明，請參閱 .NET API 參考的移植助理中的 [DescribeSecurityGroups](#)。

修改安全群組規則

修改您的安全群組規則，以限制對特定信任 IP 地址或範圍的存取。更新安全群組規則時，請考慮透過為每個必要的來源 IP 範圍建立規則或限制對特定連接埠的存取，來區隔不同網路區段的存取需求。若要修改安全群組規則，請參閱《Amazon EC2 使用者指南》中的[設定安全群組規則](#)。

EC2 執行個體的連線能力特性

以下是 EC2 執行個體的可達性特性和建議的修補步驟。

EC2 執行個體可透過網際網路連線

Amazon EC2 執行個體具有可透過網際網路閘道（包括 Application Load Balancer 或 Classic Load Balancer 後方的執行個體）、VPC 互連連線或 VPN 虛擬閘道從網際網路連線的連接埠，可能會將您的執行個體公開至網際網路。遵循標準安全原則，我們建議透過將傳入流量限制為僅必要的來源和連接埠，來實作最低權限的網路存取控制。

修改或移除安全群組規則

在資源索引標籤中，開啟 Amazon EC2 安全群組的資源。檢閱執行個體是否需要網際網路存取才能運作。修改或移除允許無限制存取的傳入安全群組規則 (0.0.0.0/0 或 ::/0)。根據特定 IP 範圍或安全群組實作更嚴格的規則。如果需要有限的公開存取，請限制存取執行個體函數所需的特定連接埠和通訊協定。如需管理安全群組規則的指示，請參閱《Amazon EC2 使用者指南》中的[設定安全群組規則](#)。

更新網路 ACLs

檢閱和修改與執行個體子網路相關聯的網路存取控制清單 (ACLs)。確認 ACL 設定符合安全群組變更，且不要意外允許公開存取。如需修改網路 ACLs 的說明，請參閱《Amazon VPC 使用者指南》中的[使用網路 ACLs](#)。

替代存取方法

請考慮下列替代存取方法的選項：

- 使用 NAT Gateway 進行傳出網際網路連線 – 對於私有子網路中需要存取網際網路的執行個體（例如，下載更新），請考慮使用 NAT Gateway，而不是指派公有 IP 地址。NAT Gateway 允許私有子網路中的執行個體啟動網際網路的傳出連線，同時防止網際網路的傳入連線。
- 使用 Systems Manager Session Manager – Session Manager 提供對 Amazon EC2 執行個體的安全殼層存取，而不需要傳入連接埠、管理 SSH 金鑰或維護堡壘主機。
- 使用 WAF 和 Elastic Load Balancing 或 Application Load Balancer – 對於執行 Web 應用程式的執行個體，請考慮使用 LB 結合 AWS Web Application Firewall (WAF)。LBs 可設定為允許執行個體在私

有子網路中執行，而 LB 在公有子網路中執行並處理網際網路流量。將 WAF 新增至負載平衡器可提供額外的 Web 入侵和機器人防護。

EC2 執行個體的漏洞特性

以下是 EC2 執行個體的漏洞特徵和建議的修復步驟。

EC2 執行個體具有網路可攻擊的軟體漏洞，具有高利用率的可能性

安裝在 EC2 執行個體上的軟體套件可能會公開到常見漏洞與暴露 (CVEs)。關鍵 CVEs 對您的 AWS 環境構成重大的安全風險。未經授權的主體可以利用這些未修補的漏洞來損害資料的機密性、完整性或可用性，或存取其他系統。具有高入侵可能性的關鍵漏洞代表立即的安全威脅，因為攻擊者或自動化掃描工具可能已經公開提供並主動使用入侵程式碼。建議您修補這些漏洞，以保護執行個體。

更新受影響的執行個體

檢閱特徵漏洞索引標籤中的參考區段。廠商文件可能包含特定的修補指引。使用以下一般準則，遵循適當的補救措施：

使用 Systems Manager Patch Manager 將修補程式套用至作業系統和應用程式。修補程式管理員可協助您在大型執行個體群組上自動選取和部署作業系統和軟體修補程式。如果您沒有設定修補程式管理員，請手動更新每個受影響執行個體上的作業系統。

依照廠商建議的程序，將受影響的應用程式更新為最新的安全版本。若要跨多個執行個體管理應用程式更新，請考慮使用 Systems Manager State Manager 讓您的軟體保持一致狀態。如果更新不可用，請考慮移除或停用易受攻擊的應用程式，直到修補程式發佈或其他緩解措施，例如限制應用程式的網路存取或停用易受攻擊的功能。

遵循 Amazon Inspector 調查結果中提供的特定修復建議。這可能包括變更安全群組規則、修改執行個體組態或調整應用程式設定。

檢查執行個體是否屬於 Auto Scaling 群組。AMI 取代修補會在不可變的基礎設施上完成，方法是更新設定為在 Auto Scaling 群組中部署新 Amazon EC2 執行個體的 AMI ID。如果您使用的是自訂/黃金 AMI，請使用新的 AMI 建立執行個體，然後自訂執行個體並建立新的黃金 AMI 如需詳細資訊，請參閱 [AMI 更新修補 \(使用 Auto Scaling 群組的修補 AMIs\)](#)。

未來考量事項

為了防止未來發生，請考慮實作漏洞管理計畫。Amazon Inspector 可設定為自動掃描執行個體上的 CVEs。Amazon Inspector 也可以與 Security Hub 整合，以進行自動修復。請考慮使用 Systems Manager 維護 Windows 實作定期修補排程，將對執行個體的干擾降至最低。

Amazon EC2 執行個體具有軟體漏洞

安裝在 Amazon EC2 執行個體上的軟體套件可能會暴露於常見漏洞與暴露 (CVEs)。非關鍵 CVEs 代表與關鍵 CVEs 相比，嚴重性或可攻擊性較低的安全弱點。雖然這些漏洞帶來的風險較低，但攻擊者仍然可以利用這些未修補的漏洞來損害資料的機密性、完整性或可用性，或存取其他系統。遵循安全最佳實務，AWS 建議修補這些漏洞，以保護執行個體免受攻擊。

更新受影響的執行個體

使用 AWS Systems Manager Patch Manager 將修補程式套用至作業系統。修補程式管理員可協助您在大型執行個體群組上自動選取和部署作業系統和軟體修補程式。如果您沒有設定修補程式管理員，請手動更新每個受影響執行個體上的作業系統。

依照廠商建議的程序，將受影響的應用程式更新為最新的安全版本。若要跨多個執行個體管理應用程式更新，請考慮使用 AWS Systems Manager State Manager 讓您的軟體保持一致狀態。如果更新不可用，請考慮移除或停用易受攻擊的應用程式，直到修補程式發佈或其他緩解措施，例如限制應用程式的網路存取或停用易受攻擊的功能。

遵循 Amazon Inspector 調查結果中提供的特定修復建議。這可能包括變更安全群組規則、修改執行個體組態或調整應用程式設定。

檢查執行個體是否屬於 Auto Scaling 群組。AMI 取代修補會在不可變的基礎設施上完成，方法是更新設定為在 Auto Scaling 群組中部署新 Amazon EC2 執行個體的 AMI ID。如果您使用的是自訂/黃金 AMI，請使用新的 AMI 建立執行個體，然後自訂執行個體並建立新的黃金 AMI 如需詳細資訊，請參閱 [AMI 更新修補 \(使用 Auto Scaling 群組的修補 AMIs\)](#)。

未來考量事項

為了防止未來發生，請考慮實作漏洞管理計畫。Amazon Inspector 可設定為自動掃描執行個體上的 CVEs。Amazon Inspector 也可以與 Security Hub 整合，以進行自動修復。請考慮使用 Systems Manager 維護 Windows 實作定期修補排程，將對執行個體的干擾降至最低。

EC2 執行個體具有End-Of-Life作業系統

EC2 執行個體會執行原始開發人員不再支援或維護的end-of-life作業系統。這會使執行個體暴露在安全漏洞和潛在攻擊中。當作業系統達到end-of-life，廠商通常會停止發佈新的安全建議。現有的安全建議也可能從廠商摘要中移除。因此，Amazon Inspector 可能會停止為已知 CVEs 產生問題清單，進而造成安全涵蓋範圍的進一步差距。

請參閱《Amazon Inspector 使用者指南》中的 [已停止作業系統](#)，以取得 Amazon Inspector 可偵測到之生命週期結束的相關資訊。

更新至支援的作業系統版本

我們建議您更新至支援的作業系統版本。在公開調查結果中，開啟 資源以存取受影響的資源。更新執行個體上的作業系統版本之前，請在 Amazon Inspector 使用者指南中的[支援的作業系統](#)中檢閱可用的版本，以取得目前支援的作業系統版本清單。

EC2 執行個體具有惡意軟體套件

惡意套件是包含有害程式碼的軟體元件，旨在損害系統和資料的機密性、完整性和可用性。惡意套件會對執行個體構成主動且重要的威脅，因為攻擊者可以在不利用漏洞的情況下自動執行惡意程式碼。遵循安全最佳實務，AWS 建議移除惡意套件，以保護執行個體免受潛在攻擊。

移除惡意套件

檢閱特徵漏洞索引標籤參考區段中的惡意套件詳細資訊，以了解威脅。使用適當的套件管理員移除已識別的惡意套件。如需範例，請參閱《Amazon Linux 2023 使用者指南》中的[套件管理工具](#)。移除惡意套件之後，請考慮執行掃描，以確保已移除可能由惡意程式碼安裝的所有套件。如需詳細資訊，請參閱《[中的在 GuardDuty 中啟動隨需惡意軟體掃描](#)》。

EC2 執行個體具有惡意檔案

惡意檔案包含有害程式碼，旨在損害系統和資料的機密性、完整性和可用性。惡意檔案會對執行個體構成主動且重要的威脅，因為攻擊者可以在不利用漏洞的情況下自動執行惡意程式碼。遵循安全最佳實務，AWS 建議移除惡意檔案，以保護執行個體免受潛在攻擊。

移除惡意檔案

若要識別具有惡意檔案的特定 Amazon Elastic Block Store (Amazon EBS) 磁碟區，請檢閱特徵調查結果詳細資訊的資源區段。使用惡意檔案識別磁碟區後，請移除已識別的惡意檔案。移除惡意檔案後，請考慮執行掃描，以確保所有可能由惡意檔案安裝的檔案都已移除。如需詳細資訊，請參閱《[中的在 GuardDuty 中啟動隨需惡意軟體掃描](#)》。

修復 Amazon ECS 服務的暴露

AWS Security Hub 可以產生 Amazon Elastic Container Service (Amazon ECS) 服務的公開調查結果。

涉及公開調查結果的 Amazon ECS 服務及其識別資訊會列在調查結果詳細資訊的資源區段中。您可以在 Security Hub 主控台上擷取這些資源詳細資訊，或使用 Security Hub CSPM API [GetFindingsV2](#) 的操作以程式設計方式擷取這些資源詳細資訊。

識別暴露調查結果中涉及的資源之後，如果不需要，您可以刪除資源。刪除非必要資源可以降低您的暴露描述檔和 AWS 成本。如果資源是必要的，請遵循這些建議的修補步驟，以協助降低風險。修復主題會根據特徵類型分割。

單一公開調查結果包含多個修復主題中識別的問題。相反地，您可以透過僅解決一個修補主題來解決暴露問題並降低其嚴重性等級。您的風險修補方法取決於您的組織需求和工作負載。

Note

本主題提供的修補指引可能需要對其他 AWS 資源進行額外諮詢。

內容

- [Amazon ECS 服務的錯誤組態特徵](#)
 - [Amazon ECS 服務使用任務定義，允許容器存取根檔案系統](#)
 - [Amazon ECS 服務使用設定為共用主機程序命名空間的任務定義](#)
 - [Amazon ECS 服務使用使用環境變數中純文字登入資料設定的任務定義](#)
 - [Amazon ECS 服務具有開放的安全群組](#)
 - [Amazon ECS 服務具有公有 IP 地址](#)
 - [Amazon ECS 服務使用啟用主機聯網模式的任務定義](#)
 - [與 Amazon ECS 服務相關聯的 IAM 角色具有管理存取政策](#)
 - [與 ECS 服務相關聯的 IAM 角色具有服務管理政策](#)
- [Amazon ECS 服務的漏洞特性](#)
 - [Amazon ECS 服務具有一個容器，具有網路可攻擊的軟體漏洞，具有高利用可能性](#)
 - [Amazon ECS 服務具有具有軟體漏洞的容器](#)
 - [Amazon ECS 服務具有具有End-Of-Life作業系統的容器](#)
 - [Amazon ECS 服務具有具有惡意軟體套件的容器](#)

Amazon ECS 服務的錯誤組態特徵

以下是 Amazon ECS 服務和建議的修復步驟的錯誤組態特性。

Amazon ECS 服務使用任務定義，允許容器存取根檔案系統

可存取主機根檔案系統的 Amazon ECS 容器可能會在主機系統上讀取、修改或執行關鍵檔案。此組態會增加遭入侵的容器可用來存取或修改其預期範圍外資源的風險，進而可能的主機檔案系統上公開敏感資料。遵循標準安全原則，AWS 建議您授予最低權限，這表示您僅授予執行任務所需的許可。

檢閱和修改具有主機檔案系統存取權的容器

在公開調查結果中，識別任務定義 ARN。在 Amazon ECS 主控台中開啟任務定義。在定義主機路徑映射的任務定義中尋找磁碟區區段。檢閱任務定義，以判斷容器功能是否需要主機檔案系統存取。如果不需要主機檔案系統存取，請建立新的任務定義修訂，並移除任何使用主機路徑的磁碟區定義。如果需要主機檔案系統存取，請考慮將容器設定為使用唯讀檔案系統，以防止未經授權的修改。

Amazon ECS 服務使用設定為共用主機程序命名空間的任務定義

使用公開命名空間執行的 Amazon ECS 容器可能會存取主機系統資源和其他容器命名空間。此組態可能允許遭入侵的容器逸出其隔離界限，這可能會導致存取程序、網路介面或其他超出其預期範圍的資源。程序 ID (PID) 命名空間可在程序之間進行區隔。它可防止系統程序可見，並允許重複使用 PIDs，包括 PID 1。如果主機的 PID 命名空間與容器共用，則可讓容器查看主機系統上的所有程序。這可減少主機和容器之間程序層級隔離的好處。這些因素可能會導致未經授權存取主機本身的程序，包括操作和終止它們的能力。遵循標準安全原則，AWS 建議維持容器的適當命名空間隔離。

使用公開的命名空間更新任務定義

開啟公開的資源索引標籤，以公開的命名空間識別任務定義。在 Amazon ECS 主控台中開啟任務定義。尋找具有主機值的 pidMode 設定，這會與主機共用程序 ID 命名空間。從任務定義中移除 pidMode：主機設定，以確保容器以適當的命名空間隔離執行。

Amazon ECS 服務使用使用環境變數中純文字登入資料設定的任務定義

環境變數中具有純文字登入資料的 Amazon ECS 容器會公開敏感身分驗證資訊，如果攻擊者取得任務定義、容器環境或容器日誌的存取權，可能會遭到入侵。這會產生重大的安全風險，因為洩漏的登入資料可用來存取其他 AWS 服務或資源。

取代純文字登入資料

在公開調查結果中，使用純文字登入資料來識別任務定義。在 Amazon ECS 主控台中開啟任務定義。在容器定義中尋找包含敏感值的環境變數，例如 AWS 存取金鑰、資料庫密碼或 API 字符。

請考慮下列傳遞登入資料的替代方案：

- 使用 IAM 任務執行角色和任務角色來授予容器許可，而不是使用 AWS 存取金鑰。
- 將登入資料儲存為 中的秘密，AWS Secrets Manager 並在任務定義中參考它們。

更新任務定義

為您的任務定義建立新的修訂，以安全地處理登入資料。然後，更新您的 Amazon ECS 服務以使用新的任務定義修訂版。

Amazon ECS 服務具有開放的安全群組

安全群組可做為 Amazon ECS 任務的虛擬防火牆，以控制傳入和傳出流量。允許從任何 IP 地址不受限制存取的開放安全群組，可能會讓您的容器暴露於未經授權的存取，進而增加暴露於自動化掃描工具和目標性攻擊的風險。遵循標準安全原則，AWS 建議限制安全群組對特定 IP 地址和連接埠的存取。

檢閱安全群組規則並評估目前的組態

開啟 Amazon ECS 安全群組的資源。評估哪些連接埠可從廣泛的 IP 範圍開啟和存取，例如 (0.0.0.0/0 or ::/0)。

修改安全群組規則

修改您的安全群組規則，以限制對特定信任 IP 地址或範圍的存取。更新安全群組規則時，請考慮透過為每個必要的來源 IP 範圍建立規則或限制對特定連接埠的存取，來區隔不同網路區段的存取需求。

修改安全群組規則

請考慮下列替代存取方法的選項：

- Session Manager 可讓您安全地存取 Amazon EC2 執行個體，而不需要傳入連接埠、管理 SSH 金鑰或維護堡壘主機。
- NACLs 在子網路層級提供額外的安全層。與安全群組不同，NACLs 是無狀態的，需要明確定義傳入和傳出規則。

Amazon ECS 服務具有公有 IP 地址

指派給其任務的公有 IP 地址的 Amazon ECS 服務可以直接從網際網路存取。雖然這對於需要可公開取得的服務而言可能是必要的，但它會增加攻擊面和潛在的未經授權存取。

識別具有公有 IP 地址的服務

在公開調查結果中，識別已為其任務指派公有 IP 地址的 Amazon ECS 服務。在服務組態ENABLED中尋找值為 assignPublicIp的設定。

更新任務定義

為您的任務定義建立新的修訂，以停用公有 IP 地址。然後，更新您的 Amazon ECS 服務以使用新的任務定義修訂版。

實作私有網路存取模式

對於執行 Web 應用程式的執行個體，請考慮使用Load Balancer (LB)。LBs可設定為允許執行個體在私有子網路中執行，而 LB 在公有子網路中執行並處理網際網路流量。

Amazon ECS 服務使用啟用主機聯網模式的任務定義

使用主機聯網模式執行的 Amazon ECS 容器與主機共用網路命名空間，允許直接存取主機的網路介面、連接埠和路由表。此組態會略過容器提供的網路隔離，可能會將容器上執行的服務直接暴露到外部網路，並允許容器修改主機網路設定。遵循標準安全原則，AWS 建議維持容器的適當網路隔離。

停用主機聯網模式

在公開調查結果中，使用主機聯網模式識別任務定義。在 Amazon ECS 主控台中開啟任務定義。在任務定義中尋找值為 主機的网络Mode 設定。

請考慮下列停用主機聯網模式的選項：

- awsvpc 網路模式透過為每個任務提供自己的彈性網路界面，提供最強的網路隔離層級。
- bridge 網路模式提供隔離，同時允許連接埠映射向主機公開特定容器連接埠。

更新任務定義

使用更新的網路模式組態建立新的任務定義修訂版。然後，更新您的 Amazon ECS 服務以使用新的任務定義修訂版。

與 Amazon ECS 服務相關聯的 IAM 角色具有管理存取政策

具有連接到 Amazon ECS 任務的管理存取政策的 IAM 角色提供廣泛的許可，這些許可超過容器操作通常需要的許可。此組態會增加遭入侵的容器可用來在整個 AWS 環境中存取或修改資源的風險。遵循標準安全原則，AWS 建議僅授予任務運作所需的許可，以實作最低權限存取。

檢閱和識別管理政策

在資源 ID 中，識別 IAM 角色名稱。前往 IAM 儀表板，然後選取已識別的角色。檢閱連接至 IAM 角色的許可政策。如果政策是 AWS 受管政策，請尋找 AdministratorAccess。否則，請在政策文件中尋找具有陳述式的陳述式 "Effect": "Allow", "Action": "*", and "Resource": "*"。

實作最低權限存取

將管理政策取代為僅授予執行個體運作所需特定許可的政策。若要識別不必要的許可，您可以使用 IAM Access Analyzer 了解如何根據存取歷史記錄修改政策。或者，您可以建立新的 IAM 角色，以避免影響使用現有角色的其他應用程式。在此案例中，建立新的 IAM 角色，然後將新的 IAM 角色與執行個體建立關聯。

安全組態考量

如果執行個體需要服務層級管理許可，請考慮實作這些額外的安全控制來降低風險：

- MFA 需要其他形式的身分驗證來新增額外的安全層。即使登入資料遭到入侵，這也有助於防止未經授權的存取。
- 設定條件元素可讓您根據來源 IP 或 MFA 存留期等因素，限制何時及如何使用管理許可。

更新任務定義

為您的任務定義建立新的修訂，以參考新的或更新的 IAM 角色。然後，更新您的 Amazon ECS 服務以使用新的任務定義修訂版。

與 ECS 服務相關聯的 IAM 角色具有服務管理政策

服務管理員政策為 Amazon ECS 任務和服務提供在特定 AWS 服務內執行所有動作的許可。這些政策通常包含 Amazon ECS 任務功能所需的許可。為 IAM 角色提供 Amazon ECS 任務的服務管理政策，而不是所需的最低許可集，如果容器遭到入侵，則可能會增加攻擊範圍。遵循標準安全原則，AWS 建議您授予最低權限，這表示僅授予執行任務所需的許可。

檢閱和識別管理政策

在資源 ID 中，識別 Amazon ECS 任務角色和執行角色名稱。前往 [IAM 儀表板](#)，然後選取已識別的角色。檢閱連接到這些 IAM 角色的許可政策。尋找授予服務完整存取權的政策陳述式（例如 "s3": "*", "ecr": "*"）。如需編輯 IAM 政策的說明，請參閱 [《IAM 使用者指南》中的編輯 IAM 政策](#)。

實作最低權限存取

將服務管理員政策取代為僅授予 Amazon ECS 任務運作所需特定許可的政策。若要識別不必要的許可，您可以使用 IAM Access Analyzer 了解如何根據存取歷史記錄修改政策。或者，您可以建立新的

IAM 角色，以避免影響使用現有角色的其他應用程式。在此案例中，建立新的 IAM 角色，然後將新的 IAM 角色與執行個體建立關聯。

安全組態考量

如果 Amazon ECS 任務需要服務層級管理許可，請考慮實作這些額外的安全控制：

- IAM 條件 – 設定條件元素，根據 VPC 端點或特定 Amazon ECS 叢集等因素，限制何時及如何使用管理許可。如需詳細資訊，請參閱 [《IAM 使用者指南》中的使用 IAM 政策中的條件來進一步限制存取](#)。
- 許可界限 – 建立角色可以擁有的最大許可，為具有管理存取權的角色提供護欄。如需詳細資訊，請參閱 [《IAM 使用者指南》中的使用許可界限來委派帳戶中的許可管理](#)。

更新任務定義

為您的任務定義建立新的修訂，以參考新的或更新的 IAM 角色。然後，更新您的 Amazon ECS 服務以使用新的任務定義修訂版。

Amazon ECS 服務的漏洞特性

以下是 Amazon ECS 的漏洞特徵和建議的修復步驟。

Amazon ECS 服務具有一個容器，具有網路可攻擊的軟體漏洞，具有高利用可能性

1. 了解暴露

套件漏洞調查結果可識別您 AWS 環境中暴露於常見漏洞與暴露 (CVEs) 的軟體套件。攻擊者可以利用這些未修補的漏洞來損害資料的機密性、完整性或可用性，或存取其他系統。ECR 容器映像可以有套件漏洞問題清單。

2. 修復曝光

a. 更新套件版本

檢閱 ECR 容器映像的套件漏洞問題清單。依照 Amazon Inspector 的建議更新套件版本。如需詳細資訊，請參閱 [《Amazon Inspector 使用者指南》中的檢視 Amazon Inspector 問題清單的詳細資訊](#)。Amazon Inspector 主控台中調查結果詳細資訊的修復區段會告訴您可執行哪些命令來更新套件。

b. 更新基礎容器映像

定期重建和更新基礎容器映像，讓您的容器保持最新狀態。重建映像時，請勿包含不必要的元件來減少攻擊面。如需重建容器映像的指示，請參閱 [經常重建映像](#)。

Amazon ECS 服務具有具有軟體漏洞的容器

安裝在 Amazon ECS 容器上的軟體套件可能會暴露於常見漏洞與暴露 (CVEs)。相較於高優先順序漏洞，低優先順序漏洞代表嚴重性或可攻擊性較低的安全弱點。雖然這些漏洞帶來的風險較低，但攻擊者仍然可以利用這些未修補的漏洞來損害資料的機密性、完整性或可用性，或存取其他系統。

更新受影響的容器映像

檢閱特徵漏洞索引標籤中的參考區段。廠商文件可能包含特定的修補指引。

遵循下列一般準則套用適當的修補：

- 更新您的容器映像，以使用受影響套件的修補版本。
- 將應用程式中受影響的相依性更新為最新的安全版本。

更新容器映像後，將其推送到您的容器登錄檔，並更新您的 Amazon ECS 任務定義以使用新映像。

未來考量事項

若要進一步強化容器映像的安全狀態，請考慮遵循 Amazon ECS 任務和容器安全最佳實務。Amazon Inspector 可設定為自動掃描容器上的 CVEs。Amazon Inspector 也可以與 Security Hub 整合，以進行自動修復。考慮使用 Systems Manager 維護 Windows 實作定期修補排程，將對容器的干擾降至最低。

Amazon ECS 服務具有具有End-Of-Life作業系統的容器

Amazon ECS 容器依賴原始開發人員不再支援或維護的end-of-life作業系統。這會使容器暴露在安全漏洞和潛在攻擊中。當作業系統達到end-of-life，廠商通常會停止發佈新的安全建議。現有的安全建議也可能從廠商摘要中移除。因此，Amazon Inspector 可能會停止為已知 CVEs 產生問題清單，進而造成安全涵蓋範圍的進一步差距。

請參閱《Amazon Inspector 使用者指南》中的[已停止作業系統](#)，以取得 Amazon Inspector 可偵測到之生命週期結束的相關資訊。

更新至支援的作業系統版本

我們建議您更新至支援的作業系統版本。在公開調查結果中，開啟 資源以存取受影響的資源。在更新容器映像中的作業系統版本之前，請在 Amazon Inspector 使用者指南中的[支援的作業系統](#)中檢閱可用的版本，以取得目前支援的作業系統版本清單。更新容器映像後，將其推送到您的容器登錄檔，並更新您的 Amazon ECS 任務定義以使用新映像。

Amazon ECS 服務具有具有惡意軟體套件的容器

惡意套件是包含有害程式碼的軟體元件，旨在損害系統和資料的機密性、完整性和可用性。惡意套件會對 Amazon ECS 容器映像構成主動且重要的威脅，因為攻擊者可以在不利用漏洞的情況下自動執行惡意程式碼。遵循安全最佳實務，AWS 建議移除惡意套件，以保護容器免受潛在攻擊。

移除惡意套件

檢閱特徵漏洞索引標籤參考區段中的惡意套件詳細資訊，以了解威脅。從容器映像中移除已識別的惡意套件，然後重建它們。如需詳細資訊，請參閱《AWS Amazon ECS API 參考》中的 [ContainerDependency](#)。更新容器映像後，將其推送到您的容器登錄檔，並更新您的 Amazon ECS 任務定義以使用新映像。如需詳細資訊，請參閱《[Amazon ECS 開發人員指南](#)》中的[使用主控台更新 Amazon ECS 任務定義](#)。AWS

修復 Amazon EKS 叢集的暴露

AWS Security Hub 可以產生 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集的公開調查結果。

涉及公開調查結果的 Amazon EKS 叢集及其識別資訊會列在調查結果詳細資訊的資源區段中。您可以在 Security Hub 主控台上擷取這些資源詳細資訊，或使用 Security Hub CSPM API [GetFindingsV2](#) 的操作以程式設計方式擷取這些資源詳細資訊。

識別暴露調查結果中涉及的資源之後，如果不需要，您可以刪除資源。刪除非必要資源可以降低您的暴露設定檔和 AWS 成本。如果資源是必要的，請遵循這些建議的修補步驟，以協助降低風險。修復主題會根據特徵類型進行分割。

單一公開調查結果包含多個修復主題中識別的問題。相反地，您可以解決暴露問題清單，並透過僅解決一個修補主題來降低其嚴重性。您的風險修補方法取決於您的組織需求和工作負載。

Note

本主題提供的修補指引可能需要在其他 AWS 資源中進行額外諮詢。

內容

- [Amazon EKS 叢集的錯誤組態特性](#)
- [Amazon EKS 叢集允許公開存取](#)
- [Amazon EKS 叢集使用不支援的 Kubernetes 版本](#)

- [Amazon EKS 叢集使用未加密的 Kubernetes 秘密](#)
- [Amazon EKS 叢集的漏洞特性](#)
 - [Amazon EKS 叢集的容器具有網路可攻擊的軟體漏洞，具有高利用率的可能性](#)
 - [Amazon EKS 叢集具有具有軟體漏洞的容器](#)
 - [Amazon EKS 叢集具有具有End-Of-Life作業系統的容器](#)
 - [Amazon EKS 叢集具有具有惡意軟體套件的容器](#)
 - [EKS 叢集具有惡意檔案](#)

Amazon EKS 叢集的錯誤組態特性

以下是 Amazon EKS 叢集的錯誤組態特性和建議的修復步驟。

Amazon EKS 叢集允許公開存取

Amazon EKS 叢集端點是您用來與叢集 Kubernetes API 伺服器通訊的端點。根據預設，此端點對網際網路是公有的。公有端點會增加您的攻擊面區域，以及未經授權存取 Kubernetes API 伺服器的風險，可能允許攻擊者存取或修改叢集資源或存取敏感資料。遵循安全最佳實務，AWS 建議將 EKS 叢集端點的存取限制為僅限必要的 IP 範圍。

修改端點存取

在公開調查結果中，開啟 資源。這會開啟受影響的 Amazon EKS 叢集。您可以設定叢集使用私有存取、公有存取或兩者。透過私有存取，源自叢集 VPC 的 Kubernetes API 請求會使用私有 VPC 端點。透過公有存取，源自叢集 VPC 外部的 Kubernetes API 請求會使用公有端點。

修改或移除叢集的公有存取權

若要修改現有叢集的端點存取，請參閱《Amazon Elastic Kubernetes Service 使用者指南》中的[修改叢集端點存取](#)。根據特定 IP 範圍或安全群組實作更嚴格的規則。如果需要有限的公開存取，請限制對特定 CIDR 區塊範圍的存取，或使用字首清單。

Amazon EKS 叢集使用不支援的 Kubernetes 版本

Amazon EKS 在有限的時間內支援每個 Kubernetes 版本。使用不支援的 Kubernetes 版本執行叢集可能會讓您的環境暴露在安全漏洞中，因為 CVE 修補程式將停止針對過期的版本發佈。不支援的版本可能包含攻擊者可能利用的已知安全漏洞，且缺少較新版本中可用的安全功能。遵循安全最佳實務，AWS 建議更新您的 Kubernetes 版本。

更新 Kubernetes 版本

在公開調查結果中，開啟 資源。這會開啟受影響的 Amazon EKS 叢集。更新叢集之前，請參閱《Amazon Elastic Kubernetes Service 使用者指南》中的[標準支援可用的版本](#)，以取得目前支援的 Kubernetes 版本清單。

Amazon EKS 叢集使用未加密的 Kubernetes 秘密

根據預設，Kubernetes 秘密會未加密存放在 API 伺服器的基礎資料存放區 (etcd)。任何具有 API 存取權或具有等存取權的人都可以擷取或修改秘密。為了避免這種情況，您應該加密靜態 Kubernetes 秘密。如果 Kubernetes Secrets 未加密，則如果 Kubernetes Secrets 洩漏，它們容易受到未經授權的存取。由於秘密通常包含敏感資訊，例如密碼和 API 字串，因此其公開可能導致未經授權存取其他應用程式和資料。遵循安全最佳實務，AWS 建議加密存放在 Kubernetes 秘密中的所有敏感資訊。

加密 Kubernetes 秘密

Amazon EKS 支援透過信封加密使用 KMS 金鑰加密 Kubernetes 秘密。若要啟用 EKS 叢集的 Kubernetes 秘密加密，請參閱《Amazon EKS 使用者指南》中的[在現有叢集上使用 KMS 加密 Kubernetes 秘密](#)。

Amazon EKS 叢集的漏洞特性

以下是 Amazon EKS 叢集的漏洞特徵。

Amazon EKS 叢集的容器具有網路可攻擊的軟體漏洞，具有高利用率的可能性

安裝在 EKS 叢集上的軟體套件可能會公開到常見漏洞與暴露 (CVEs)。關鍵 CVEs 對您的 AWS 環境構成重大的安全風險。未經授權的使用者可以利用這些未修補的漏洞來危害資料的機密性、完整性或可用性，或存取其他系統。具有高入侵可能性的關鍵漏洞代表立即的安全威脅，因為攻擊者或自動化掃描工具可能已經公開提供並主動使用入侵程式碼。遵循安全最佳實務，AWS 建議修補這些漏洞，以保護執行個體免受攻擊。

更新受影響的執行個體

將您的容器映像更新為較新版本，其中包含已識別漏洞的安全修正。這通常涉及使用更新的基礎映像或相依性重建容器映像，然後將新映像部署到您的 Amazon EKS 叢集。

Amazon EKS 叢集具有具有軟體漏洞的容器

安裝在 Amazon EKS 叢集上的軟體套件可能會公開到常見漏洞與暴露 (CVEs)。非關鍵 CVEs 代表與關鍵 CVEs 相比，嚴重性或可利用性較低的安全弱點。雖然這些漏洞的立即風險較低，但攻擊者仍然可以利用這些未修補的漏洞來損害資料的機密性、完整性或可用性，或存取其他系統。遵循安全最佳實務，AWS 建議修補這些漏洞，以保護執行個體免受攻擊。

更新受影響的執行個體

將您的容器映像更新為較新版本，其中包含已識別漏洞的安全修正。這通常涉及使用更新的基礎映像或相依性重建容器映像，然後將新映像部署到您的 Amazon EKS 叢集。

Amazon EKS 叢集具有具有End-Of-Life作業系統的容器

Amazon EKS 容器映像依賴原始開發人員不再支援或維護的end-of-life作業系統。這會使容器暴露在安全漏洞和潛在攻擊中。當作業系統達到end-of-life，廠商通常會停止發佈新的安全建議。現有的安全建議也可能從廠商摘要中移除。因此，Amazon Inspector 可能會停止為已知 CVEs 產生問題清單，進而造成安全涵蓋範圍的進一步差距。

請參閱《Amazon Inspector 使用者指南》中的[已停止作業系統](#)，以取得 Amazon Inspector 可偵測到之生命週期結束的相關資訊。

更新至支援的作業系統版本

建議您更新至支援的作業系統版本。在公開調查結果中，開啟 資源以存取受影響的資源。在更新容器映像中的作業系統版本之前，請在 Amazon Inspector 使用者指南中的[支援的作業系統](#)中檢閱可用的版本，以取得目前支援的作業系統版本清單。更新容器映像後，請將容器重建並重新部署至 Amazon EKS 叢集。

Amazon EKS 叢集具有具有惡意軟體套件的容器

惡意套件是包含有害程式碼的軟體元件，旨在損害系統和資料的機密性、完整性和可用性。惡意套件會對 Amazon EKS 叢集構成主動且重要的威脅，因為攻擊者可以在不利用漏洞的情況下自動執行惡意程式碼。遵循安全最佳實務，AWS 建議移除惡意套件，以保護叢集免受潛在攻擊。

移除惡意套件

檢閱特徵漏洞索引標籤參考區段中的惡意套件詳細資訊，以了解威脅。從容器映像中移除已識別的惡意套件。然後，刪除映像遭到入侵的 Pod。更新您的 Kubernetes 部署以使用更新的容器映像。然後，部署您的變更並重新部署您的 Pod。

EKS 叢集具有惡意檔案

惡意檔案包含有害程式碼，旨在損害系統和資料的機密性、完整性和可用性。惡意檔案會對叢集構成主動且重要的威脅，因為攻擊者可以在不利用漏洞的情況下自動執行惡意程式碼。遵循安全最佳實務，AWS 建議移除惡意檔案，以保護叢集免受潛在攻擊。

移除惡意檔案

若要識別具有惡意檔案的特定 Amazon Elastic Block Store (Amazon EBS) 磁碟區，請檢閱特徵調查結果詳細資訊的資源區段。使用惡意檔案識別磁碟區後，請移除已識別的惡意檔案。移除惡意檔案後，請考慮執行掃描，以確保可能由惡意檔案安裝的所有檔案都已移除。如需詳細資訊，請參閱《[中的在 GuardDuty 中啟動隨需惡意軟體掃描](#)》。

修復 IAM 使用者的曝光

AWS Security Hub 可以為 AWS Identity and Access Management (IAM) 使用者產生公開調查結果。

在 Security Hub 主控台上，涉及公開調查結果的 IAM 使用者及其識別資訊會列在調查結果詳細資訊的資源區段中。您可以使用 Security Hub CSPM API [GetFindingsV2](#) 的操作，以程式設計方式擷取資源詳細資訊。

識別暴露調查結果中涉及的資源之後，如果不需要，您可以刪除資源。刪除非必要的資源可以降低您的暴露描述檔和 AWS 成本。如果資源是必要的，請遵循這些建議的修補步驟，以協助降低風險。修復主題會根據特徵類型分割。

單一公開調查結果包含多個修復主題中識別的問題。相反地，您可以透過僅解決一個修補主題來解決暴露問題並降低其嚴重性等級。您的風險修補方法取決於您的組織需求和工作負載。

Note

本主題提供的修補指引可能需要對其他 AWS 資源進行額外諮詢。

IAM 最佳實務建議您建立 IAM 角色，或與身分提供者使用聯合身分來使用臨時憑證存取 AWS，而不是建立個別 IAM 使用者。如果這是您組織和使用案例的選項，建議您切換到角色或聯合，而不是使用 IAM 使用者。如需詳細資訊，請參閱「IAM 使用者指南」中的 [IAM 使用者](#)。

內容

- [IAM 使用者的錯誤組態特性](#)
 - [IAM 使用者具有具有管理存取權的政策](#)
 - [IAM 使用者未啟用 MFA](#)
 - [IAM 使用者具有 管理存取權的政策 AWS 服務](#)
 - [IAM 使用者 AWS 的帳戶具有較弱的密碼政策](#)
 - [IAM 使用者具有未使用的登入資料](#)
 - [IAM 使用者具有未輪換的存取金鑰](#)
 - [IAM 使用者具有允許無限制存取 KMS 金鑰解密的政策](#)

• [IAM 使用者的未使用存取特徵](#)

IAM 使用者的錯誤組態特性

以下是 IAM 使用者的錯誤組態特性和建議的修復步驟。

IAM 使用者具有具有管理存取權的政策

存取資源時，IAM 政策會將一組權限授予 IAM 使用者。管理政策為 IAM 使用者提供對 AWS 服務和資源的廣泛許可。如果登入資料遭到入侵，提供完整的管理權限，而不是使用者所需的最低許可集，可以增加攻擊範圍。遵循標準安全原則，AWS 建議您授予最低權限，這表示您僅授予執行任務所需的許可。

1. 檢閱並識別管理政策 – 在資源 ID 中，識別 IAM 角色名稱。前往 IAM 儀表板，然後選取已識別的角色。檢閱連接至 IAM 使用者的許可政策。如果政策是 AWS 受管政策，請尋找 AdministratorAccess 或 IAMFullAccess。否則，在政策文件中，尋找具有 "Action": "*" 陳述 "Effect": "Allow" 式超過 的陳述式 "Resource": "*"。
2. 實作最低權限存取 – 將服務管理政策取代為僅授予使用者運作所需特定許可的政策。如需 IAM 政策安全最佳實務的詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的 [套用最低權限許可](#)。若要識別不必要的許可，您可以使用 IAM Access Analyzer 來了解如何根據存取歷史記錄修改政策。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的 [外部和未使用存取的調查結果](#)。
3. 安全組態考量 – 如果執行個體需要服務管理許可，請考慮實作這些額外的安全控制來降低風險：
 - 多重要素驗證 (MFA) – MFA 需要其他形式的身分驗證來新增額外的安全層。即使登入資料遭到入侵，這也有助於防止未經授權的存取。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的 [需要多重要素驗證 \(MFA\)](#)。
 - IAM 條件 – 設定條件元素可讓您根據來源 IP 或 MFA 存留期等因素，限制何時及如何使用管理許可。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的 [使用 IAM 政策中的條件](#) 來進一步限制存取。
 - 許可界限 – 許可界限會建立角色可擁有的最大許可，為具有管理存取權的角色提供護欄。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的 [使用許可界限來委派帳戶中的許可管理](#)。

IAM 使用者未啟用 MFA

Multi-Factor authentication (MFA) 在使用者名稱和密碼之外，多增加一層保護。啟用 MFA 且 IAM 使用者登入 AWS 網站時，系統會提示他們輸入使用者名稱、密碼和 AWS MFA 裝置的驗證碼。身分驗

證委託人必須擁有發出時效性金鑰的裝置，並且必須擁有登入資料的知識。如果沒有 MFA，如果使用者的密碼洩露，攻擊者會取得使用者 AWS 許可的完整存取權。遵循標準安全原則，AWS 建議為所有 AWS 管理主控台 可存取的帳戶和使用者啟用 MFA。

檢閱 MFA 類型

AWS 支援下列 [MFA 類型](#)：

- 通行密鑰和安全金鑰
- 虛擬驗證器應用程式
- 硬體 TOTP 權杖

雖然使用實體裝置的身分驗證通常提供更嚴格的安全性保護，但使用任何類型的 MFA 比停用 MFA 更安全。

啟用 MFA

若要啟用符合您需求的 MFA 類型，請參閱 [《AWS IAM 使用者指南》中的 IAM 中的多重要素驗證](#)。請遵循您要實作之特定 MFA 類型的步驟。對於管理許多使用者的組織，您可能需要 MFA 存取敏感資源，以強制執行 MFA 用量。

IAM 使用者具有 管理存取權的政策 AWS 服務

服務管理員政策為 IAM 使用者提供在特定 AWS 服務內執行所有動作的許可。這些政策通常包含使用者執行其任務功能不需要的許可。為 IAM 使用者提供服務管理員權限，而不是所需的最低許可集，可在憑證洩露時增加攻擊範圍。遵循標準安全原則，AWS 建議您授予最低權限，這表示您僅授予執行任務所需的許可。

檢閱和識別服務管理員政策

在資源 ID 中，識別 IAM 角色名稱。前往 IAM 儀表板，然後選取已識別的角色。檢閱連接至 IAM 使用者的許可政策。如果政策是 AWS 受管政策，請尋找 AdministratorAccess 或 IAMFullAccess。否則，請在政策文件中尋找具有陳述式 "Effect": "Allow" with "Action": "*" over "Resource": "*"。

實作最低權限存取

將服務管理政策取代為僅授予使用者運作所需特定許可的政策。若要識別不必要的許可，您可以使用 IAM Access Analyzer 來了解如何根據存取歷史記錄修改政策。

安全組態考量

如果執行個體需要服務管理許可，請考慮實作這些額外的安全控制，以減少暴露：

- MFA 需要其他形式的身分驗證來新增額外的安全層。即使登入資料遭到入侵，這也有助於防止未經授權的存取。
- 使用條件元素，根據來源 IP 或 MFA 存留期等因素，限制何時及如何使用管理許可。
- 使用許可界限來建立角色可擁有的最大許可，為具有管理存取權的角色提供護欄。

IAM 使用者 AWS 的帳戶具有較弱的密碼政策

密碼政策透過強制執行 IAM 使用者密碼的最低複雜性要求，協助防止未經授權的存取。如果沒有強大的密碼政策，使用者帳戶可能會因為密碼猜測或暴力破解攻擊而遭到入侵的風險會增加。遵循標準安全原則，AWS 建議實作強大的密碼政策，以確保使用者建立難以猜測的複雜密碼。

設定強式密碼政策

前往 IAM 儀表板並導覽至帳戶設定。檢閱您帳戶的目前密碼政策設定，包括長度下限、所需的字元類型，以及密碼過期設定。

設定密碼政策時，建議至少 AWS 遵循這些最佳實務：

- 至少需要一個大寫字元。
- 至少需要一個小寫字元。
- 至少需要一個符號。
- 至少需要一個數字。
- 至少需要八個字元。

其他安全考慮事項

除了強式密碼政策之外，請考慮以下額外的安全措施：

- MFA 需要其他形式的身分驗證來新增額外的安全層。即使登入資料遭到入侵，這也有助於防止未經授權的存取。
- 設定條件元素，根據來源 IP 或 MFA 存留期等因素，限制何時及如何使用管理許可。

IAM 使用者具有未使用的登入資料

未使用的登入資料，包括已閒置 90 天或更長時間的密碼和存取金鑰，都會對您的 AWS 環境造成安全風險。這些未使用的登入資料會為攻擊者建立潛在的攻擊媒介，並增加組織的整體攻擊面。遵循安全最佳實務，AWS 建議停用或移除在 90 天或更長時間內未使用的登入資料，以減少您的攻擊面。

停用或移除未使用的登入資料

在公開調查結果中，開啟 資源。這會開啟使用者詳細資訊視窗。在對未使用的登入資料採取動作之前，請評估對您環境的潛在影響。在沒有適當評估的情況下移除登入資料可能會中斷背景程序、排程任務等。在永久移除之前，請考慮短暫停用期間，以驗證移除未使用登入資料的影響。

根據登入資料類型採取適當的動作：

- 對於未使用的主控制台密碼，請考慮先變更密碼並暫時停用。如果沒有發生問題，請繼續永久停用或刪除。
- 對於未使用的存取金鑰，請考慮先停用金鑰。確認沒有任何系統受到影響後，請繼續永久停用或刪除。
- 對於未使用的使用者，請考慮在完全刪除之前連接限制性政策來暫時停用使用者。

IAM 使用者具有未輪換的存取金鑰

存取金鑰包含存取金鑰 ID 和私密存取金鑰，以程式設計方式存取 AWS 資源。當存取金鑰長時間保持不變時，如果遭到入侵，它們會增加未經授權的存取風險。遵循安全最佳實務，AWS 建議每 90 天輪換存取金鑰，將攻擊者使用遭入侵憑證的機會降至最低。

輪換存取金鑰

在公開調查結果中，開啟 資源。這會開啟使用者詳細資訊視窗。若要輪換存取金鑰，請參閱 [《IAM 使用者指南》中的管理 IAM 使用者的存取金鑰](#)。

IAM 使用者具有允許無限制存取 KMS 金鑰解密的政策

AWS KMS 可讓您建立和管理用於保護資料的密碼編譯金鑰。允許所有 KMS 金鑰上不受限制 AWS KMS 解密許可（例如 `kms:Decrypt` 或 `kms:ReEncryptFrom`）的 IAM 政策，如果 IAM 使用者的登入資料遭到洩漏，可能會導致未經授權的資料存取。如果攻擊者取得這些登入資料的存取權，他們可能會解密您環境中的任何加密資料，其中可能包含敏感資料。遵循安全最佳實務，AWS 建議將 AWS KMS 解密許可限制為使用者工作職能所需的特定金鑰，以實作最低權限。

實作最低權限存取

在公開調查結果中，開啟 資源。這會開啟 IAM 政策視窗。尋找 KMS 中允許 kms:Decrypt kms:ReEncryptFrom 或 資源規格 KMS:* 為 的許可 "*"。更新政策，將 AWS KMS 解密許可限制為僅需要的特定金鑰。修改政策，將 "*" 資源取代為必要 AWS KMS 金鑰的特定 ARNs。

安全組態考量

考慮新增條件以進一步限制何時可以使用這些許可。例如，您可以將解密操作限制在特定 VPC 端點或來源 IP 範圍。您也可以設定金鑰政策，進一步限制誰可以使用特定的 KMS 金鑰。

IAM 使用者的未使用存取特徵

當 IAM 使用者具有未使用的許可、存取金鑰或密碼時，Security Hub 可能會在該使用者的公開調查結果中包含這些作為內容特徵。這些特徵是由服務管理的 IAM Access Analyzer 產生，並提供使用者安全狀態的其他內容。未使用的存取特徵不是公開調查結果的主要原因，但它們表示使用者具有比所需更多的許可，這會在使用者的登入資料洩露時增加潛在影響。

對於特別未使用的許可，您可以產生最低權限的政策建議，顯示縮小範圍的替代政策。如需詳細資訊，請參閱 [the section called “政策建議”](#)。

修復 Lambda 函數的曝光

AWS Security Hub 可以產生 AWS Lambda (Lambda) 函數的公開調查結果。

在 Security Hub 主控台上，涉及公開調查結果的 Lambda 函數及其識別資訊會列在調查結果詳細資訊的資源區段中。您可以使用 Security Hub CSPM API [GetFindingsV2](#) 的操作，以程式設計方式擷取資源詳細資訊。

識別暴露調查結果中涉及的資源之後，如果不需要，您可以刪除資源。刪除非必要的資源可以降低您的暴露描述檔和 AWS 成本。如果資源是必要的，請遵循這些建議的修補步驟，以協助降低風險。修復主題會根據特徵類型分割。

單一公開調查結果包含多個修復主題中識別的問題。相反地，您可以透過僅解決一個修補主題來解決暴露問題並降低其嚴重性等級。您的風險修補方法取決於您的組織需求和工作負載。

Note

本主題提供的修補指引可能需要對其他 AWS 資源進行額外諮詢。

內容

- [Lambda 函數的錯誤組態特性](#)
 - [Lambda 函數部署在 Amazon VPC 外部](#)
 - [與 Lambda 函數相關聯的 IAM 角色具有管理存取政策](#)
 - [與 Lambda 函數相關聯的 IAM 角色具有管理存取 AWS 服務的政策](#)
 - [Lambda 函數可透過 API Gateway 存取，無需授權](#)
- [Lambda 函數的可達性特性](#)
 - [可公開叫用 Lambda 函數](#)
- [Lambda 函數的漏洞特性](#)
 - [Lambda 函數具有網路可攻擊的軟體漏洞](#)
 - [Lambda 函數具有軟體漏洞](#)
 - [Lambda 函數具有惡意軟體套件](#)
 - [Lambda 函數具有程式碼漏洞](#)

Lambda 函數的錯誤組態特性

以下是 Lambda 函數的錯誤組態特性和建議的修復步驟。

Lambda 函數部署在 Amazon VPC 外部

根據預設，Lambda 函數會部署為可存取公有網際網路。此預設組態可讓 Lambda 函數連線到 AWS 服務端點和外部 APIs，但也會讓它們面臨潛在的安全風險。具有網際網路存取的函數可用來滲透資料、與未經授權的伺服器通訊，或在遭到入侵時成為外部演員的進入點。Amazon VPC 透過限制 Lambda 函數僅與定義的私有網路中的資源通訊，來提供網路隔離。遵循標準安全原則，我們建議在 VPC 中部署 Lambda 函數，以透過網路隔離提高安全性。

將函數連接至 VPC

在公開調查結果中，開啟具有超連結的資源。這會開啟 Lambda 函數視窗。若要限制 Lambda 函數的網路存取，請將其連接到具有適當網路控制的 VPC。將您的函數連接至 VPC 之前，請規劃其可能需要的任何 AWS 服務存取，因為在沒有 NAT 閘道或 VPC 端點的私有子網路中的函數將無法連線 AWS 服務 APIs。如需有關如何將 Lambda 函數連接至您帳戶中 Amazon VPC 的資訊，請參閱[將 Lambda 函數連接至您帳戶中的 Amazon VPC AWS 帳戶](#)。如果您的函數需要 AWS 從私有子網路內存取服務，請考慮使用 VPC 端點進行服務連線，而不需要網際網路存取。如果您需要從私有子網路傳出網際網路連線，請設定 NAT Gateway。

與 Lambda 函數相關聯的 IAM 角色具有管理存取政策

管理存取政策為 Lambda 函數提供對 AWS 服務和資源的廣泛許可。這些政策通常包含功能不需要的許可。在 Lambda 函數上提供具有管理存取政策的 IAM 身分，而不是執行角色所需的最低許可集，可以在函數遭到入侵時增加攻擊範圍。遵循標準安全原則，AWS 建議您授予最低權限，這表示您僅授予執行任務所需的許可。

1. 檢閱和識別管理政策

在公開調查結果中，識別角色名稱。前往 IAM 儀表板，並使用先前識別的角色名稱來尋找角色。檢閱連接至 IAM 角色的許可政策。如果政策是 AWS 受管政策，請尋找 AdministratorAccess 或 IAMFullAccess。否則，請在政策文件中尋找具有陳述式 "Effect": "Allow", "Action": "*" 和 "Resource": "*" 的陳述式。

2. 實作最低權限存取

將管理政策取代為僅授予函數操作所需特定許可的政策。如需 IAM 角色安全最佳實務的詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[套用最低權限許可](#)。若要識別不必要的許可，您可以使用 IAM Access Analyzer 了解如何根據存取歷史記錄修改政策。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[外部和未使用存取的調查結果](#)。或者，您可以建立新的 IAM 角色，以避免使用現有角色影響其他 Lambda 函數。在此案例中，建立新的 IAM 角色。然後將新角色與執行個體建立關聯。如需有關取代函數的 IAM 角色的資訊，請參閱《AWS Lambda 開發人員指南》中的[更新函數的執行角色](#)。

3. 安全組態考量

如果執行個體需要管理存取許可，請考慮實作這些額外的安全控制來降低風險：

- 多重要素驗證 (MFA) – MFA 需要其他形式的身分驗證來新增額外的安全層。即使登入資料遭到入侵，這也有助於防止未經授權的存取。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[需要多重要素驗證 \(MFA\)](#)。
- IAM 條件 – 設定條件元素可讓您根據來源 IP 或 MFA 存留期等因素，限制何時及如何使用管理許可。如需詳細資訊，請參閱《[IAM 使用者指南](#)》中的[使用 IAM 政策中的條件來進一步限制存取](#)。
- 許可界限 – 許可界限會建立角色可擁有的最大許可，為具有管理存取權的角色提供護欄。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[使用許可界限來委派帳戶中的許可管理](#)。

與 Lambda 函數相關聯的 IAM 角色具有管理存取 AWS 服務的政策

服務管理員政策允許 Lambda 函數在特定 AWS 服務內執行所有動作。這些政策通常會授予比函數操作所需的更多許可。如果具有服務管理員政策的 Lambda 函數遭到入侵，攻擊者可能會使用這些許可來存取或修改 AWS 環境中的敏感資料或服務。遵循標準安全原則，我們建議您授予最低權限，這表示您僅授予執行任務所需的許可。

1. 檢閱和識別管理政策

在公開調查結果中，識別 ARN 中的角色名稱。前往 IAM 儀表板，並尋找角色名稱。檢閱連接至角色的許可政策。如果政策是 AWS 受管政策，請尋找 AdministratorAccess 或 IAMFullAccess。否則，請在政策文件中尋找具有 陳述式 "Effect": "Allow", "Action": "*" 和 "Resource": "*" 的陳述式。

2. 實作最低權限存取

將管理政策取代為僅授予函數操作所需特定許可的政策。如需詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的[套用最低權限許可](#)。若要識別不必要的許可，您可以使用 IAM Access Analyzer 了解如何根據存取歷史記錄修改政策。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[外部和未使用存取的調查結果](#)。或者，您可以建立新的 IAM 角色，以避免影響使用現有角色的其他 Lambda 函數。在此案例中，建立新的 IAM 角色，然後將新的 IAM 角色與執行個體建立關聯。如需為函數取代 IAM 角色的說明，請參閱《AWS Lambda 開發人員指南》中的[更新函數的執行角色](#)。

3. 安全組態考量

如果執行個體需要服務層級管理許可，請考慮實作這些額外的安全控制來降低風險：

- 多重要素驗證 (MFA) – MFA 需要其他形式的身分驗證來新增額外的安全層。即使登入資料遭到入侵，這也有助於防止未經授權的存取。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[需要多重要素驗證 \(MFA\)](#)。
- IAM 條件 – 設定條件元素可讓您根據來源 IP 或 MFA 存留期等因素，限制何時及如何使用管理許可。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[使用 IAM 政策中的條件來進一步限制存取](#)。
- 許可界限 – 許可界限會建立角色可擁有的最大許可，為具有管理存取權的角色提供護欄。如需詳細資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[使用許可界限來委派許可管理](#)。

Lambda 函數可透過 API Gateway 存取，無需授權

未授權的 API Gateway 方法允許任何具有 API Gateway 存取權的發起人叫用整合的 Lambda 函數，而無需身分驗證。此組態會產生安全風險，因為呼叫者可以在沒有適當授權的情況下叫用 Lambda 函數，這可能會導致濫用函數功能、資源耗用、存取敏感資料或未經授權的操作。雖然 API Gateway 可能具有網路層級存取控制，但缺少方法層級授權可能會允許具有 API Gateway 網路存取權的任何發起人免費叫用函數。遵循安全最佳實務，AWS 建議針對與 Lambda 函數整合的 API Gateway 方法實作適當的授權機制。

設定 API Gateway 身分驗證

在公開的資源索引標籤中，按一下開啟資源超連結以存取 API Gateway 方法。檢閱目前的授權組態，並實作適當的身分驗證機制。API Gateway 支援多種身分驗證選項，包括 AWS IAM、Amazon Cognito 使用者集區、Lambda 授權方和 API 金鑰。選擇最符合您安全需求和使用案例的身分驗證方法。如需設定身分驗證的詳細說明，請參閱 [《API Gateway 開發人員指南》中的在 API Gateway 中控制和管理對 REST API 的存取](#)。

Lambda 函數的可達性特性

以下是 Lambda 函數的可達性特性和建議的修復步驟。

可公開叫用 Lambda 函數

Lambda 資源型政策決定誰可以叫用您的函數。包含「*」做為委託人（或完全沒有委託人）的資源政策函數，允許任何已驗證 AWS 的使用者叫用它。這會產生重大風險，特別是處理敏感資料、修改資源或具有更高許可的函數。未經授權的使用者可以利用此組態來執行不需要的操作、可能暴露資料、操縱資源或濫用函數功能。遵循安全最佳實務，我們建議將 Lambda 函數存取限制為僅限授權的主體。

修改函數的資源型政策

在公開的資源索引標籤中，使用超連結開啟資源。這會開啟 Lambda 函數視窗。在資源型政策中僅指定授權 AWS 的帳戶 IDs 或特定 IAM 主體（使用者、角色或服務），以限制對 Lambda 函數的存取。您只能以程式設計方式修改資源型政策。

Lambda 函數的漏洞特性

以下是 Lambda 函數的漏洞特徵和建議的修復步驟。

Lambda 函數具有網路可攻擊的軟體漏洞

Lambda 函數程式碼中使用的軟體套件可以包含常見漏洞和暴露 (CVEs)，這些軟體套件具有很高被利用的機會。關鍵 CVEs 對您的 AWS 環境構成重大的安全風險。攻擊者可以利用這些未修補的漏洞來損害資料的機密性、完整性或可用性，或存取其他系統。具有高入侵可能性的關鍵漏洞代表立即的安全威脅。

脅，因為攻擊者或自動化掃描工具可能已經公開提供並主動使用入侵程式碼。遵循安全最佳實務，我們建議您修補這些漏洞，以保護函數免於遭受攻擊。

更新受影響的函數

檢閱 特性漏洞索引標籤中的參考區段。廠商文件可能包含特定的修補指引。依照廠商建議的程序，將易受攻擊的程式庫更新為最新的安全版本。一般而言，修補工作流程取決於您是否透過上傳 zip 檔案或使用容器映像建立 Lambda 函數來部署 Lambda 套件。更新程式庫之後，請更新 Lambda 函數程式碼以使用固定版本。之後，請部署更新的版本。

Lambda 函數具有軟體漏洞

相較於關鍵 CVEs，Lambda 函數通常會使用第三方程式庫和相依性，其中可能包含嚴重性或可利用性較低的安全漏洞。雖然這些非關鍵漏洞可能無法立即被利用，但仍代表安全弱點，這些弱點可能會與其他漏洞串連在一起以入侵您的函數。隨著時間的推移，新的入侵技術也可能出現，提高這些漏洞的風險。遵循標準安全原則，我們建議您修補這些漏洞，以維護安全的環境。

檢閱 特性漏洞索引標籤中的參考區段。廠商文件可能包含特定的修補指引。依照廠商建議的程序，將易受攻擊的程式庫更新為最新的安全版本。一般而言，修補工作流程取決於您是否透過上傳 zip 檔案或使用容器映像建立 Lambda 函數來部署 Lambda 套件。更新程式庫之後，請更新 Lambda 函數程式碼以使用固定版本。之後，請部署更新的版本。

Lambda 函數具有惡意軟體套件

惡意套件是包含有害程式碼的軟體元件，旨在損害系統和資料的機密性、完整性和可用性。惡意套件會對 Lambda 函數構成主動和關鍵的威脅，因為攻擊者可以在不利用漏洞的情況下自動執行惡意程式碼。遵循安全最佳實務，AWS 建議移除惡意套件，以保護 Lambda 函數免受潛在攻擊。

移除惡意套件

檢閱特徵漏洞索引標籤參考區段中的惡意套件詳細資訊，以了解威脅。從函數程式碼和相依性中移除已識別的惡意套件。對於使用 layer 的函數，請檢查惡意套件是否安裝在任何 layer 中，並將其移除。更新您的部署套件或容器映像以排除惡意套件，然後部署更新的版本。如需說明，請參閱[將 Lambda 函數部署為 .zip 檔案封存](#)的 .zip 檔案封存，或使用[容器映像的容器映像建立 Lambda 函數](#)。

Lambda 函數具有程式碼漏洞

Lambda 函數應用程式程式碼包含威脅執行者可能利用的安全漏洞。程式碼漏洞包括資料洩漏、注入漏洞、遺失加密，以及透過自動化程式碼分析識別的脆弱密碼編譯。這些漏洞對您的 AWS 環境構成安全風險，因為攻擊者可以利用它們來危害資料的機密性、完整性或可用性，或存取其他系統。程式碼漏洞代表可能與其他攻擊向量連結以入侵函數的安全弱點。遵循安全最佳實務，AWS 建議解決這些程式碼漏洞，以保護函數免受攻擊。

更新受影響的函數

檢閱特徵漏洞索引標籤中的參考區段。Amazon Inspector 調查結果可能包含特定的修補指引和程式碼片段，其中顯示易受攻擊的程式碼位置。使用提供的plug-and-play程式碼區塊或實作安全編碼實務，解決函數程式碼中已識別的安全問題。請務必先檢閱程式碼修復建議，再採用這些建議，因為您可能需要編輯這些建議，以確保程式碼如預期般執行。修正漏洞後，請更新 Lambda 函數程式碼以使用更正的版本。如需說明，請參閱《AWS Lambda 開發人員指南》中的[更新函數程式碼](#)。之後，請部署更新的版本。如需說明，請參閱[將 Lambda 函數部署為 .zip 檔案封存](#)的 .zip 檔案封存，或使用[容器映像的容器映像建立 Lambda 函數](#)。如需 Amazon Inspector 程式碼掃描的詳細資訊，請參閱《[Amazon Inspector 使用者指南](#)》中的[Amazon Inspector Lambda 程式碼掃描](#)。Amazon Inspector

修復 Amazon RDS 執行個體和叢集的暴露

AWS Security Hub 可以產生 Amazon RDS 執行個體和叢集的公開調查結果。

在 Security Hub 主控台上，涉及公開調查結果的 Amazon RDS 執行個體或叢集及其識別資訊會列在調查結果詳細資訊的資源區段中。您可以使用 Security Hub CSPM API [GetFindingsV2](#) 的操作，以程式設計方式擷取資源詳細資訊。

識別暴露調查結果中涉及的資源之後，如果不需要，您可以刪除資源。刪除非必要資源可以降低您的暴露描述檔和 AWS 成本。如果資源是必要的，請遵循這些建議的修補步驟，以協助降低風險。修復主題會根據特徵類型分割。

單一公開調查結果包含多個修復主題中識別的問題。相反地，您可以透過僅解決一個修補主題來解決暴露問題並降低其嚴重性等級。您的風險修補方法取決於您的組織需求和工作負載。

Note

本主題提供的修補指引可能需要對其他 AWS 資源進行額外諮詢。

內容

- [Amazon RDS 執行個體和叢集的錯誤組態特性](#)
 - [Amazon RDS 資料庫執行個體已設定為公開存取](#)
 - [Amazon RDS 資料庫叢集具有公開共用的快照](#)
 - [Amazon RDS 資料庫執行個體具有公開共用的快照](#)
 - [Amazon RDS 資料庫執行個體具有未靜態加密的快照](#)

- [Amazon RDS 資料庫叢集具有未靜態加密的快照](#)
- [Amazon RDS 資料庫執行個體具有開啟的安全群組](#)
- [Amazon RDS 資料庫執行個體已停用 IAM 資料庫身分驗證](#)
- [Amazon RDS 資料庫執行個體使用預設的管理員使用者名稱](#)
- [Amazon RDS 資料庫叢集使用預設的管理員使用者名稱](#)
- [Amazon RDS 資料庫執行個體已停用自動次要版本升級](#)
- [Amazon RDS 資料庫執行個體已停用自動備份](#)
- [Amazon RDS 資料庫執行個體已停用刪除保護](#)
- [Amazon RDS 資料庫叢集已停用刪除保護](#)
- [Amazon RDS 資料庫執行個體使用資料庫引擎的預設連接埠](#)
- [備份計畫未涵蓋 Amazon RDS 資料庫執行個體](#)

Amazon RDS 執行個體和叢集的錯誤組態特性

以下說明 Amazon RDS 執行個體和叢集的錯誤組態特性和修復步驟。

Amazon RDS 資料庫執行個體已設定為公開存取

具有公有存取權的 Amazon RDS 執行個體可能可以透過其端點透過網際網路存取。雖然執行個體功能有時需要公開存取，但此組態可以用作未經授權的使用者嘗試存取資料庫的潛在攻擊媒介。可公開存取的資料庫可能會暴露於連接埠掃描、暴力破解攻擊和入侵嘗試。遵循標準安全原則，我們建議您限制資料庫資源的公開暴露。

1. 修改公開存取設定

在公開調查結果中，開啟具有超連結的資源。這會開啟受影響的資料庫執行個體。根據您的應用程式架構，評估資料庫執行個體是否需要公有可存取性。如需詳細資訊，請參閱在 [Amazon RDS 中設定公有或私有存取](#)。

Amazon RDS 資料庫叢集具有公開共用的快照

任何 都可以存取公有快照 AWS 帳戶，可能將敏感資料暴露給未經授權的使用者。任何 AWS 帳戶 都有複製這些公有快照並從中建立資料庫執行個體的許可，這可能會導致資料外洩或未經授權的資料存取。遵循安全最佳實務，建議您將 Amazon RDS 快照的存取限制為僅受信任 AWS 帳戶 和組織。

1. 設定 Amazon RDS 快照以進行私有存取

在公開調查結果中，透過超連結開啟資源。如需有關如何修改快照共用設定的資訊，請參閱《Amazon Aurora 使用者指南》中的[共用快照](#)。如需有關如何停止共用快照的資訊，請參閱《Amazon Aurora 使用者指南》中的[停止快照共用](#)。

Amazon RDS 資料庫執行個體具有公開共用的快照

任何 都可以存取公有快照 AWS 帳戶，可能將敏感資料暴露給未經授權的使用者。任何 AWS 帳戶 都有複製這些公有快照並從中建立資料庫執行個體的許可，這可能會導致資料外洩或未經授權的資料存取。遵循安全最佳實務，建議您將 Amazon RDS 快照的存取限制為僅受信任 AWS 帳戶 和組織。

設定 Amazon RDS 快照以進行私有存取

在公開調查結果中，透過超連結開啟資源。如需有關如何修改快照共用設定的資訊，請參閱《Amazon RDS 使用者指南》中的[共用資料庫快照](#)。如需有關如何停止共用快照的資訊，請參閱《Amazon RDS 使用者指南》中的[停止共用資料庫快照](#)。

Amazon RDS 資料庫執行個體具有未靜態加密的快照

如果未經授權存取儲存層，未加密的 Amazon RDS 資料庫執行個體快照可能會公開敏感資料。如果沒有加密，快照中的資料可能會透過未經授權的存取公開。這會產生資料外洩和違反合規的風險。遵循安全最佳實務，我們建議加密所有資料庫資源及其備份，以維護資料機密性。

在公開調查結果中，開啟具有超連結的資源。這會開啟受影響的快照。您無法直接加密現有的未加密快照。反之，請建立未加密快照的加密複本。如需詳細說明，請參閱 [《Amazon Aurora 使用者指南》中的資料庫叢集快照複製和加密 Amazon RDS 資源](#)。

Amazon RDS 資料庫叢集具有未靜態加密的快照

如果未經授權存取儲存層，未加密的 Amazon RDS 資料庫叢集快照可能會公開敏感資料。如果沒有加密，快照中的資料可能會透過未經授權的存取公開。這會產生資料外洩和違反合規的風險。遵循安全最佳實務，我們建議加密所有資料庫資源及其備份，以維護資料機密性。

1. 建立快照的加密複本

在公開調查結果中，開啟具有超連結的資源。這會開啟受影響的快照。您無法直接加密現有的未加密快照。反之，請建立未加密快照的加密複本。如需詳細說明，請參閱 [《Amazon Aurora 使用者指南》中的資料庫叢集快照複製和加密 Amazon RDS 資源](#)。

Amazon RDS 資料庫執行個體具有開啟的安全群組

安全群組可做為 Amazon RDS 執行個體的虛擬防火牆，以控制傳入和傳出流量。允許從任何 IP 地址不受限制存取的開放安全群組，可能會讓您的資料庫執行個體遭受未經授權的存取和潛在的攻擊。遵循標準安全原則，我們建議限制安全群組對特定 IP 地址和連接埠的存取，以維護最低權限原則。

檢閱安全群組規則並評估目前的組態

在公開調查結果中，開啟資料庫執行個體安全群組的資源。評估哪些連接埠可從廣泛的 IP 範圍開啟和存取，例如 (0.0.0.0/0 or ::/0)。如需有關檢視安全群組詳細資訊的資訊，請參閱《Amazon Elastic Compute Cloud API 參考》中的 [DescribeSecurityGroups](#)。

修改安全群組規則

修改您的安全群組規則，以限制對特定信任 IP 地址或範圍的存取。更新安全群組規則時，請考慮透過為每個必要的來源 IP 範圍建立規則或限制對特定連接埠的存取，來區隔不同網路區段的存取需求。若要修改安全群組規則，請參閱《Amazon EC2 使用者指南》中的[設定安全群組規則](#)。若要修改現有 Amazon RDS 資料庫執行個體的預設連接埠，請參閱《Amazon Aurora 使用者指南》中的[使用主控台、CLI 和 API 修改資料庫叢集](#)。

Amazon RDS 資料庫執行個體已停用 IAM 資料庫身分驗證

IAM 資料庫身分驗證可讓您使用 IAM 登入資料而非資料庫密碼，對 Amazon RDS 資料庫進行身分驗證。這提供數種安全優勢，例如集中式存取管理、臨時登入資料，以及消除在應用程式程式碼中存放資料庫密碼。IAM 資料庫身分驗證允許使用身分驗證字符而非密碼對資料庫執行個體進行身分驗證。因此，進出資料庫執行個體的網路流量會使用 SSL 加密。如果沒有 IAM 身分驗證，資料庫通常依賴密碼型身分驗證，這可能會導致密碼重複使用和較弱的密碼。遵循安全最佳實務，我們建議啟用 IAM 資料庫身分驗證。

啟用 IAM 資料庫身分驗證

在公開調查結果中，開啟具有超連結的資源。這會開啟受影響的資料庫執行個體。您可以在資料庫選項中啟用 IAM 資料庫身分驗證。如需詳細資訊，請參閱《Amazon RDS 使用者指南》中的[啟用和停用 IAM 資料庫身分驗證](#)。啟用 IAM 身分驗證後，請更新您的資料庫執行個體以使用 IAM 身分驗證，而非密碼型身分驗證。

Amazon RDS 資料庫執行個體使用預設的管理員使用者名稱

對資料庫執行個體使用預設使用者名稱（例如，「admin」、「root」）會增加安全風險，因為這些都是廣為人知且常見於暴力攻擊。預設使用者名稱是可預測的，可讓未經授權的使用者更輕鬆地嘗試存取您的資料庫。使用預設使用者名稱時，攻擊者只需要取得密碼，而不需要同時取得兩者，即可存取您的資料庫。遵循安全最佳實務，我們建議您為資料庫執行個體使用唯一的管理員使用者名稱，透過模糊性來增強安全性，並降低未經授權的存取嘗試風險。

設定唯一的管理員使用者名稱

在公開調查結果中，開啟具有超連結的資源。這會開啟受影響的資料庫執行個體。考慮哪種備份頻率、保留期和生命週期規則最適合您的應用程式。

Amazon RDS 資料庫叢集使用預設的管理員使用者名稱

對資料庫執行個體使用預設使用者名稱（例如，「admin」、「root」）會增加安全風險，因為這些都是廣為人知且常見於暴力攻擊。預設使用者名稱是可預測的，可讓未經授權的使用者更輕鬆地嘗試存取您的資料庫。使用預設使用者名稱時，攻擊者只需要取得密碼，而不需要同時取得兩者，即可存取您的資料庫。遵循安全最佳實務，我們建議您為資料庫執行個體使用唯一的管理員使用者名稱，透過模糊性來增強安全性，並降低未經授權存取嘗試的風險。

設定唯一的管理員使用者名稱

在公開調查結果中，開啟具有超連結的資源。這會開啟受影響的資料庫執行個體。您無法變更現有 Amazon RDS 資料庫執行個體的管理員使用者名稱。若要建立唯一的管理員名稱，您需要使用自訂使用者名稱建立新的資料庫執行個體，並遷移您的資料。

Amazon RDS 資料庫執行個體已停用自動次要版本升級

自動次要版本升級可確保您的 Amazon RDS 執行個體在可用時自動接收次要引擎版本升級。這些升級通常包括重要的安全修補程式和錯誤修正，以協助維護資料庫的安全性和穩定性。您的資料庫有執行的風險，其中包含已在較新的次要版本中修正的已知安全漏洞。如果沒有自動更新，資料庫執行個體可以在發現新的 CVEs 時累積安全漏洞。遵循安全最佳實務，我們建議為所有 Amazon RDS 執行個體啟用自動次要版本升級。

啟用自動次要版本升級

在公開調查結果中，開啟具有超連結的資源。這會開啟受影響的資料庫執行個體。您可以在維護與備份索引標籤中檢視自動次要升級設定。如需詳細資訊，請參閱 [Amazon RDS for MySQL 的自動次要版本升級](#)。您也可以將維護時段設定為在低資料庫活動期間發生。

Amazon RDS 資料庫執行個體已停用自動備份

自動化備份可為您的 Amazon RDS 執行個體提供point-in-time復原，讓您能夠將資料庫還原至保留期間內的任何時間點。停用自動備份時，若發生惡意刪除、資料損毀或其他資料遺失情況，您可能會遺失資料。如果發生惡意活動，例如勒索軟體攻擊、資料庫資料表刪除或損毀，可在事件發生之前還原至某個時間點，從而縮短從事件復原所需的時間。遵循安全最佳實務，我們建議為所有 [生產資料庫](#) 啟用具有適當保留期的自動備份。

Amazon RDS 資料庫執行個體已停用刪除保護

資料庫刪除保護是一項功能，可協助防止刪除資料庫執行個體。停用刪除保護時，具有足夠許可的任何使用者都可以刪除您的資料庫，這可能會導致資料遺失或應用程式停機。攻擊者可以刪除您的資料庫，

導致服務中斷、資料遺失和增加復原時間。遵循安全最佳實務，我們建議您為 RDS 資料庫執行個體啟用刪除保護，以防止惡意刪除。

為您的 Amazon RDS 資料庫叢集啟用刪除保護

在公開調查結果中，開啟具有超連結的資源。這會開啟受影響的資料庫叢集。

Amazon RDS 資料庫叢集已停用刪除保護

資料庫刪除保護是一項功能，可協助防止刪除資料庫執行個體。停用刪除保護時，具有足夠許可的任何使用者都可以刪除您的資料庫，這可能會導致資料遺失或應用程式停機。攻擊者可以刪除您的資料庫，導致服務中斷、資料遺失和增加復原時間。遵循安全最佳實務，我們建議您為 RDS 資料庫叢集啟用刪除保護，以防止惡意刪除。

為您的 Amazon RDS 資料庫叢集啟用刪除保護

在公開調查結果中，開啟具有超連結的資源。這會開啟受影響的資料庫叢集。

Amazon RDS 資料庫執行個體使用資料庫引擎的預設連接埠

使用資料庫引擎預設連接埠的 Amazon RDS 執行個體可能會面臨更高的安全風險，因為這些預設連接埠廣為人知，且通常是以自動化掃描工具為目標。修改資料庫執行個體以使用非預設連接埠，透過模糊性增加一層額外的安全性，讓未經授權的使用者更難以對資料庫執行自動化或目標式攻擊。預設連接埠通常由未經授權的人員掃描，並可能導致您的資料庫執行個體成為目標。遵循安全最佳實務，建議您將預設連接埠變更為自訂連接埠，以降低自動化或目標式攻擊的風險。

在公開調查結果中，開啟具有超連結的資源。這會開啟受影響的資料庫執行個體。

更新應用程式連線字串

變更連接埠後，請更新連線至 Amazon RDS 執行個體的所有應用程式和服務，以使用新的連接埠號碼。

備份計畫未涵蓋 Amazon RDS 資料庫執行個體

AWS Backup 是一種全受管備份服務，可集中和自動化跨的資料備份 AWS 服務。如果備份計畫未涵蓋您的資料庫執行個體，在惡意刪除、資料損毀或其他資料遺失的情況下，您可能會遺失資料。如果發生惡意活動，例如勒索軟體攻擊、資料庫資料表刪除或損毀，可在事件發生之前還原至某個時間點，從而縮短從事件復原所需的時間。遵循安全最佳實務，建議您在備份計畫中包含 Amazon RDS 執行個體，以確保資料保護。

為您的資料庫執行個體建立和指派備份計劃

在公開調查結果中，開啟具有超連結的資源。這會開啟受影響的資料庫執行個體。考慮哪些備份頻率、保留期和生命週期規則最適合您的應用程式。

修復 Amazon S3 儲存貯體的暴露

AWS Security Hub 可以產生 Amazon Simple Storage Service (S3) 儲存貯體的公開調查結果。

在 Security Hub 主控台上，涉及公開調查結果的 Amazon S3 儲存貯體及其識別資訊會列在調查結果詳細資訊的資源區段中。您可以使用 Security Hub CSPM API [GetFindingsV2](#) 的操作，以程式設計方式擷取資源詳細資訊。

識別暴露調查結果中涉及的資源之後，如果不需要，您可以刪除資源。刪除非必要的資源可以降低您的暴露描述檔和 AWS 成本。如果資源是必要的，請遵循這些建議的修補步驟，以協助降低風險。修復主題會根據特徵類型分割。

單一公開調查結果包含多個修復主題中識別的問題。相反地，您可以透過僅解決一個修補主題來解決暴露問題並降低其嚴重性等級。您的風險修補方法取決於您的組織需求和工作負載。

Note

本主題提供的修補指引可能需要對其他 AWS 資源進行額外諮詢。

內容

- [Amazon S3 儲存貯體的錯誤組態特性](#)
 - [Amazon S3 儲存貯體已停用版本控制](#)
 - [Amazon S3 儲存貯體已停用物件鎖定](#)
 - [Amazon S3 儲存貯體不會使用 AWS KMS 金鑰靜態加密](#)
 - [已在版本控制的 Amazon S3 儲存貯體上停用多重要素驗證 \(MFA\) 刪除](#)
 - [Amazon S3 儲存貯體允許其他 AWS 帳戶的主體修改儲存貯體許可](#)
- [Amazon S3 儲存貯體的連線能力特性](#)
 - [Amazon S3 儲存貯體具有公有讀取存取權](#)
 - [Amazon S3 儲存貯體具有公有寫入存取權](#)
- [Amazon S3 儲存貯體的敏感資料特徵](#)
 - [Amazon S3 儲存貯體的敏感資料特徵](#)

Amazon S3 儲存貯體的錯誤組態特性

以下是 Amazon S3 儲存貯體的錯誤組態特性和建議的修復步驟。

Amazon S3 儲存貯體已停用版本控制

Amazon S3 版本控制可協助您將物件的多個變體保留在同一個儲存貯體中。停用版本控制時，Amazon S3 只會儲存每個物件的最新版本，這表示如果物件被意外或惡意刪除或覆寫，則無法復原。啟用版本控制的儲存貯體可提供保護，防止意外刪除、應用程式故障，以及勒索軟體攻擊等安全事件，而這些事件可能會發生未經授權的資料修改或刪除。遵循安全最佳實務，我們建議為包含重要資料的儲存貯體啟用版本控制，這些資料在遺失時難以或無法重新建立。

1. 啟用版本控制 – 若要在儲存貯體上啟用 Amazon S3 版本控制，請參閱《Amazon Simple Storage Service 使用者指南》中的在[儲存貯體上啟用版本控制](#)。啟用版本控制時，請考慮實作生命週期規則來管理儲存體，因為版本控制會維護多個物件複本。

Amazon S3 儲存貯體已停用物件鎖定

Amazon S3 物件鎖定為 Amazon S3 物件提供write-once-read-many(WORM) 模型，防止它們在固定期間或無限期遭到刪除或覆寫。當停用物件鎖定时，您的物件可能容易受到勒索軟體意外或惡意刪除、修改或加密的影響。物件鎖定對於符合需要不可變資料儲存法規要求，以及防範可能嘗試加密資料的複雜威脅尤其重要。透過啟用物件鎖定，您可以強制執行保留政策作為多一層資料保護，並為關鍵資料建立不可變的備份策略。遵循安全最佳實務，我們建議您啟用物件鎖定，以防止惡意修改物件。

1. 請注意，物件鎖定只能在建立新儲存貯體時啟用，因此您需要在啟用物件鎖定的情況下建立新的儲存貯體。對於大型遷移，請考慮使用批次操作將物件複製到新的儲存貯體。在鎖定任何物件之前，您還必須在儲存貯體上啟用 Amazon S3 版本控制和物件鎖定。由於物件鎖定只能在新儲存貯體上啟用，因此您需要將現有資料遷移至啟用物件鎖定的新儲存貯體。設定 Amazon S3 物件鎖定 – 如需有關如何在儲存貯體上設定物件鎖定的資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》中的設定 Amazon S3 物件鎖定](#)。設定物件鎖定後，根據您的環境選擇適當的保留模式。

Amazon S3 儲存貯體不會使用 AWS KMS 金鑰靜態加密

Amazon S3 會使用 Amazon S3 受管金鑰套用伺服器端加密，作為所有新儲存貯體的預設加密層級。雖然 Amazon S3 受管金鑰提供強大的加密保護，但它不提供與 AWS Key Management Service 金鑰相同的存取控制和稽核功能層級。使用 KMS 金鑰時，存取物件需要 Amazon S3 儲存貯體和加密物件之 KMS 金鑰的許可。對於您需要精細控制誰可以存取加密物件的敏感資料，以及加密金鑰用量的完整稽核記錄，這尤其重要。遵循安全最佳實務，我們建議您使用 KMS 金鑰來加密包含敏感資料的儲存貯體，或用於具有嚴格合規要求的環境。

1. 設定 Amazon S3 儲存貯體金鑰

若要設定儲存貯體以將 Amazon S3 儲存貯體金鑰用於新物件，請參閱《Amazon Simple Storage Service [使用者指南](#)》中的[設定儲存貯體以將 Amazon S3 儲存貯體金鑰與 SSE-KMS 搭配使用](#)。如需如何加密現有物件的資訊，請參閱 AWS 儲存部落格中的[使用 Amazon S3 批次操作加密物件](#)。

實作 AWS KMS 加密時，請考慮下列事項：

- 金鑰管理 – 決定要使用 AWS 受管金鑰還是客戶受管金鑰 (CMK)。CMKs 可為客戶提供對其金鑰生命週期和用量的完全控制。如需這兩種金鑰類型之間差異的詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的[AWS KMS 金鑰](#)。
- 金鑰輪換 – 如需其他安全措施，請啟用 KMS 金鑰的自動金鑰輪換。如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的[啟用自動金鑰輪換](#)。

已在版本控制的 Amazon S3 儲存貯體上停用多重要素驗證 (MFA) 刪除

多重要素驗證 (MFA) 刪除為您的 Amazon S3 儲存貯體提供額外的安全層。它需要對破壞性 Amazon S3 操作進行多重驗證。停用 MFA 刪除時，具有適當許可的使用者可以永久刪除物件版本，或暫停儲存貯體上的版本控制，而不需要額外的身分驗證挑戰。啟用 MFA 刪除有助於防止未經授權或意外刪除您的資料，並增強對勒索軟體攻擊、內部威脅和操作錯誤的保護。對於包含關鍵或合規敏感資料的儲存貯體而言，MFA 刪除特別重要，這些資料必須受到保護，以防未經授權的刪除。遵循安全最佳實務，我們建議您為 Amazon S3 儲存貯體啟用 MFA。

1. 檢閱 MFA 類型

AWS 支援下列 [MFA 類型](#)。雖然使用實體裝置的身分驗證通常提供更嚴格的安全性保護，但使用任何類型的 MFA 比停用 MFA 更安全。

2. 在資源政策層級強制執行 MFA

使用儲存貯體政策中的 `aws:MultiFactorAuthAge` 條件索引鍵，要求 MFA 進行敏感操作。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[需要 MFA](#)。

3. 啟用 MFA

若要啟用 MFA 刪除，請先確定您的 Amazon S3 儲存貯體已啟用版本控制。只有已啟用版本控制的儲存貯體才支援 MFA 刪除。如需如何啟用 Amazon S3 版本控制的資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的在[儲存貯體上啟用版本控制](#)。MFA 刪除無法透過 Amazon S3 主控台啟用。您必須使用 Amazon S3 API 或 AWS CLI。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[設定 MFA 刪除](#)。

Amazon S3 儲存貯體允許其他 AWS 帳戶的主體修改儲存貯體許可

Amazon S3 儲存貯體政策控制對儲存貯體和物件的存取。當儲存貯體政策允許其他 AWS 帳戶的主體修改儲存貯體許可時，未經授權的使用者可以重新設定您的儲存貯體。如果外部主體憑證洩露，未經授權的使用者可以控制您的儲存貯體，導致資料外洩或服務中斷。遵循標準安全原則，AWS 建議您僅將許可管理動作限制為信任的主體。

1. 檢閱和識別儲存貯體政策

在公開中，識別 ARN 欄位中的 Amazon S3 儲存貯體。在 Amazon S3 主控台中，選取儲存貯體，然後導覽至許可索引標籤以檢閱儲存貯體政策。檢閱連接至儲存貯體的許可政策。尋找授予動作的政策陳述式，例如允許存取您帳戶外部主體 `s3:PutBucketPolicy`，`s3:PutBucketAcl`，`s3:DeleteBucketPolicy`，`s3:*` 的政策陳述式，如主體陳述式中所述。

2. 修改儲存貯體政策

修改儲存貯體政策以移除或限制授予其他 AWS 帳戶的動作：

- 移除授予外部帳戶許可管理動作的政策陳述式。
- 如果需要跨帳戶存取，請將廣泛的許可取代 (`s3:*`) 為不包含儲存貯體許可管理的特定動作。

如需修改儲存貯體政策的相關資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》中的使用 Amazon S3 主控台新增儲存貯體政策](#)。

Amazon S3 儲存貯體的連線能力特性

以下是 Amazon S3 儲存貯體的連線能力特性和建議的修補步驟。

Amazon S3 儲存貯體具有公有讀取存取權

具有公開讀取存取權的 Amazon S3 儲存貯體可讓網際網路上的任何人檢視儲存貯體的內容。雖然這對於公開存取的網站或共用資源而言可能是必要的，但如果儲存貯體包含敏感資料，則可能會產生安全風險。公開讀取存取可能會導致未經授權的檢視和下載，如果敏感資料存放在這些儲存貯體中，可能會導致資料外洩。遵循標準安全原則，AWS 建議將 Amazon S3 儲存貯體的存取權限制為必要的使用者和系統。

1. 在儲存貯體層級封鎖公開存取

Amazon S3 提供可在儲存貯體和帳戶層級設定的封鎖公開存取設定，以防止公開存取，無論儲存貯體政策或 ACLs 為何。如需詳細資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》中的封鎖對 Amazon S3 儲存體的公開存取](#)。封鎖公開存取後，請檢閱您的儲存貯體存取控制組態，以

確保其符合您的存取需求。然後檢閱您的 Amazon S3 儲存貯體政策，明確定義誰可以存取您的儲存貯體。如需儲存貯體政策的範例，請參閱 [《Amazon Simple Storage Service 使用者指南》中的 Amazon S3 儲存貯體政策範例](#)。

2. 替代存取方法

如果需要公有讀取存取權，請考慮這些更安全的替代方案：

- CloudFront – 搭配原始存取身分 (OAI) 或原始存取控制 (OAC) 使用 CloudFront，以允許從私有 Amazon S3 儲存貯體進行讀取存取。此替代方案會限制直接存取您的 Amazon S3 儲存貯體，同時允許透過 CloudFront 公開存取內容。如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[限制對 Amazon S3 原始伺服器的存取](#)。
- 預先簽章URLs – 使用預先簽章URLs 暫時存取特定物件。如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[使用預先簽章URLs 共用物件](#)。Amazon CloudFront

Amazon S3 儲存貯體具有公有寫入存取權

具有公有寫入存取權的 Amazon S3 儲存貯體可讓網際網路上的任何人上傳、修改或刪除儲存貯體中的物件。這會產生重大的安全風險，包括有人上傳惡意檔案、修改現有檔案和刪除資料的可能性。公有寫入存取會建立可供攻擊者利用的安全漏洞。遵循標準安全原則，AWS 建議將 Amazon S3 儲存貯體的寫入存取權限制為僅限必要的使用者和系統。

1. 在帳戶和儲存貯體層級封鎖公開存取

Amazon S3 提供封鎖公開存取設定，可在儲存貯體和帳戶層級進行設定，以防止公開存取，無論儲存貯體政策或 ACLs 為何。如需詳細資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》中的封鎖對 Amazon S3 儲存體的公開存取](#)。

2. 修改儲存貯體政策

如需更精細的方法來移除公有寫入存取，請檢閱儲存貯體政策。您可以尋找 `s3:PutObject`、`s3:DeleteObject` 或 `s3:*`。如需管理儲存貯體政策的詳細資訊，請參閱 [《Amazon Simple Storage Service 使用者指南》中的 Amazon S3 儲存貯體政策](#)。

3. 替代存取方法

如果需要公有讀取存取權，請考慮這些更安全的替代方案：

- CloudFront – 搭配原始存取身分 (OAI) 或原始存取控制 (OAC) 使用 CloudFront，以允許從私有 Amazon S3 儲存貯體進行讀取存取。此替代方案會限制直接存取您的 Amazon S3 儲存貯體，同時允許透過 CloudFront 公開存取內容。如需詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[限制對 Amazon S3 原始伺服器的存取](#)。

- 預先簽章URLs – 使用預先簽章URLs 暫時存取特定物件。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[使用預先簽章URLs 共用物件](#)。

Amazon S3 儲存貯體的敏感資料特徵

以下是 Amazon S3 儲存貯體的敏感資料特性和建議的修復步驟。

Amazon S3 儲存貯體的敏感資料特徵

當 Macie 識別 Amazon S3 儲存貯體中的敏感資料時，表示需要立即注意的潛在安全和合規暴露。

敏感資料可能包括：

- 憑證
- 個人身分識別資訊
- 財務資訊
- 需要保護的機密內容

如果敏感資料因組態錯誤或未經授權的存取而公開，可能會導致違規、資料外洩、身分盜竊或財務損失。遵循安全最佳實務，AWS 建議正確分類資料，並持續監控 Amazon S3 儲存貯體中的敏感資料。

實作敏感資料的控制項

在公開調查結果中，選擇開啟資源。檢閱偵測到的敏感資料類型及其在儲存貯體中的位置。如需解譯 Macie 問題清單的說明，請參閱《Amazon Macie [Macie 使用者指南](#)》中的 [Macie 問題清單類型](#)。

根據發現的敏感資料類型，實作適當的安全控制：

- 限制對儲存貯體的存取 – 檢閱儲存貯體許可，以確保它們遵循最低權限原則。使用 IAM 政策、儲存貯ACLs 來限制存取。如需詳細資訊，請參閱《[Amazon Simple Storage Service 使用者指南](#)》中的 [Amazon S3 的 Identity and Access Management](#)。
- 啟用伺服器端加密 – 使用 KMS 金鑰啟用伺服器端加密，以提供額外的保護。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[使用伺服器端加密搭配 AWS KMS 金鑰 \(SSE-KMS\)](#)。
- Use AWS Glue DataBrew – Glue DataBrew用於資料準備和清理。如需詳細資訊，請參閱《AWS Glue DataBrew 開發人員指南》中的[什麼是 AWS Glue DataBrew](#)。

了解 Security Hub 中未使用的存取調查結果

Security Hub 使用 IAM Access Analyzer 來識別您帳戶中未使用的 IAM 許可、角色、存取金鑰和密碼。這些調查結果透過強調未主動使用的 IAM 主體和許可，協助您實作最低權限存取的安全性最佳實務。此功能會提供給所有 Security Hub 客戶，無需額外費用。

未使用的存取分析如何運作

當您啟用 Security Hub 時，服務會自動在您的帳戶中建立服務連結 IAM Access Analyzer。此分析器會根據 AWS CloudTrail 活動資料評估所有 IAM 主體（角色和使用者），以判斷哪些主體和許可未在 90 天的回顧期間內使用。回顧期間無法設定。

IAM Access Analyzer 每 24 小時會重新評估所有作用中的問題清單。當先前未使用的委託人或許可變為作用中時，會自動解析對應的調查結果。

未使用的存取分析器會在美國東部（維吉尼亞北部）執行，因為 IAM 是全球服務。Security Hub 會將問題清單複寫到您已啟用 Security Hub 的所有區域。您不需要在美國東部（維吉尼亞北部）啟用 Security Hub，分析器才能執行。

未使用的存取問題清單類型

Security Hub 會產生四種未使用的存取調查結果：

調查結果類型	說明	評估的資源
UnusedIAMRole	尚未在 90 天回顧期間內擔任的 IAM 角色。	IAM 角色
UnusedIAM UserAccessKey	尚未用於在 90 天回顧期間內簽署 API 請求的 IAM 使用者存取金鑰。	IAM 使用者
UnusedIAM UserPassword	尚未在 90 天回顧期間內用於主控台登入的 IAM 使用者密碼。	IAM 使用者
UnusedPermission	授予角色或使用者的特定 IAM 動作，但尚未在 90 天的回顧期間內調用。	IAM 角色或 IAM 使用者

服務連結分析器

Security Hub 建立的 IAM Access Analyzer 是服務連結分析器。您可以在 IAM Access Analyzer 主控台中檢視它，但在 Security Hub 啟用時無法修改或刪除它。

當您在所有區域中停用 Security Hub 時，服務連結分析器會自動刪除。如果自動刪除失敗，您可以呼叫 IAM Access Analyzer `DeleteServiceLinkedAnalyzer` API 操作來刪除分析器。只有在您帳戶的 Security Hub 完全停用之後，此操作才會成功。

服務連結分析器與您可能在 IAM Access Analyzer 中獨立建立的任何客戶受管分析器是分開的。建立或刪除客戶受管分析器不會影響服務連結分析器，反之亦然。

檢視未使用的存取調查結果

未使用的存取調查結果與其他 Security Hub 調查結果一起顯示在 Security Hub 主控台中。您可以依類型篩選問題清單，僅檢視未使用的存取問題清單。未使用的存取問題清單格式採用開放式網路安全結構描述架構 (OCSF)，與所有 Security Hub 問題清單所使用的格式相同。

對於 `UnusedPermission` 調查結果，如果您從過度寬鬆政策中移除一些未使用的許可，但並非所有許可，則 Security Hub 會關閉現有的調查結果，並在仍然過度寬鬆的情況下為修訂的政策建立新的調查結果。

您也可以從 IAM Access Analyzer 主控台存取未使用的存取調查結果。IAM Access Analyzer 主控台中未使用的存取問題清單是唯讀的，並且僅在美國東部（維吉尼亞北部）區域可見。

公開調查結果中未使用的存取權

未使用的存取資訊可以在 Security Hub 公開調查結果中顯示為內容特徵。當連接至資源的 IAM 角色具有未使用的許可時，公開調查結果會包含此作為補充內容。這可協助您了解漏洞的潛在爆量半徑 — 具有高權限 IAM 角色的資源比具有最低權限許可的資源具有更高的風險。

下列資源類型可以在其公開調查結果中顯示未使用的存取內容特徵：

- Amazon Elastic Compute Cloud 執行個體
- AWS Lambda 函數
- Amazon Elastic Container Service 服務
- Amazon Elastic Kubernetes Service 叢集
- IAM 使用者（直接）

如需公開調查結果的詳細資訊，請參閱 [Security Hub 中的暴露問題清單](#)。

未使用許可的政策建議

對於 UnusedPermission 調查結果，Security Hub 可以產生最低權限政策建議。這些建議會顯示縮小範圍的替換政策，只保留委託人實際使用的許可。如需詳細資訊，請參閱 [針對未使用的存取問題清單產生政策建議](#)。

定價

服務連結的 IAM Access Analyzer 會提供給所有 Security Hub 客戶，無需額外費用。您不需要另外支付分析器或未使用的存取問題清單的費用。

針對未使用的存取問題清單產生政策建議

對於未使用的許可調查結果，Security Hub 可以產生最低權限政策建議，以顯示縮小範圍的取代政策。建議會評估連接至 IAM 主體的每個政策，並產生取代，只保留主體實際使用的許可。此功能會提供給所有 Security Hub 客戶，無需額外費用。

政策建議的運作方式

政策建議產生是非同步操作。若要產生和擷取建議：

1. 使用 GetFindingsV2 API 操作從 Security Hub 擷取未使用的許可調查結果。記下調查結果中的 `metadata.uid` 欄位。
2. GenerateRecommendedPolicyV2 使用問題清單的 呼叫 `metadata.uid`。這會啟動建議產生，這通常會在 20 秒內完成。
3. GetRecommendedPolicyV2 輪詢相同的 `metadata.uid`直到 `status` 欄位傳回 SUCCEEDED。
4. 回應包含一或多個建議步驟。每個步驟都會指定 `CREATE_POLICY`（建立和連接縮小範圍的取代政策）或 `DETACH_POLICY`（刪除過度特權原始政策）`recommendedAction`的。對於 `CREATE_POLICY`步驟，回應同時包含 `existingPolicy JSON` 和 `recommendedPolicy JSON`，因此您可以比較它們。

GetRecommendedPolicyV2 如果先前尚未針對該調查結果產生建議，您必須在呼叫 GenerateRecommendedPolicyV2之前呼叫。

誰可以產生建議

帳戶擁有者和委派管理員都可以呼叫這些 API 操作：

- 帳戶擁有者可以在自己的帳戶中產生和檢視未使用的許可調查結果的建議。
- 委派管理員可以針對其組織內任何成員帳戶未使用的許可調查結果產生和檢視建議。

如果您不是委派管理員，且調查結果屬於不同的帳戶，則 API 操作會傳回 `AccessDeniedException` 錯誤。

建議生命週期

- 建議會快取 90 天，只要問題清單處於作用中狀態（非關閉），就會保持可用狀態。不過，`GenerateRecommendedPolicyV2` 多次呼叫 會使快取失效，並啟動新的任務，以取代快取的政策。建議您每個問題清單只呼叫 `GenerateRecommendedPolicyV2` 一次。
- 建議遵循 detach-and-attach 模式。它不會修改您現有的 IAM 政策。您可以檢閱建議的政策，並透過 IAM API 在 IAM 主控台中手動套用。
- 如果問題清單已解決（例如，因為先前未使用的許可現在正在使用中），則不再提供建議。

錯誤案例

API 操作會在下列情況下傳回錯誤：

- 問題清單已解決 — `InvalidInputException(HTTP 400)`。
- 調查結果不是未使用的許可調查結果 — `InvalidInputException(HTTP 400)`。
- IAM 主體是透過 IAM Identity Center 許可集建立的。許可集主體的政策無法直接修改。建議會傳回具有說明 `FAILED` 的狀態。
- 發起人不是委派管理員，問題清單屬於不同的帳戶 — `AccessDeniedException(HTTP 403)`。
- 尚未產生建議，而且您 `GetRecommendedPolicyV2` 未先呼叫 即呼叫 `GenerateRecommendedPolicyV2` - `ResourceNotFoundException(HTTP 404)`。

使用主控台

在 Security Hub 主控台中，您可以透過檢視未使用的許可調查結果並選擇修復索引標籤來產生政策建議。建立建議時，主控台會顯示載入旋轉器。當建議準備就緒時，您可以選擇預覽來查看目前政策和建議的最低權限取代的 side-by-side 比較。您可以複製 JSON 格式的建議政策。

API 參考

- `GenerateRecommendedPolicyV2` — 針對未使用的許可調查結果啟動非同步產生最低權限政策建議。將調查結果 `metadata.uid` 做為輸入。傳回成功時具有空白內文的 HTTP 200。
- `GetRecommendedPolicyV2` — 擷取產生的政策建議。將調查結果 `metadata.uid` 做為輸入。支援使用 `maxResults(1–100)` 和 `nextToken` 參數進行分頁。傳回建議狀態 (IN_PROGRESS、或 FAILED) SUCCEEDED、建議步驟、資源 ARN 和任何錯誤。

如需詳細的 API 文件，請參閱 [Security Hub API 參考](#)。

Security Hub 中的自動化

Security Hub 包含可根據您的規格自動修改問題清單並對其採取動作的功能。

Security Hub 目前支援下列類型的自動化：

- 自動化規則 – 根據定義的條件，以近乎即時的方式自動更新和隱藏問題清單，以及將問題清單傳送至票證工具。
- 自動化回應和修復 – 建立自訂 Amazon EventBridge 規則，以定義針對特定調查結果和洞見採取的自動動作。

當您想要自動更新開放網路安全結構描述架構 (OCSF) 中的調查結果欄位時，自動化規則很有幫助。例如，您可以使用自動化規則來更新具有特定標籤之資源的問題清單嚴重性層級。使用自動化規則不需要手動更新與特定標籤相關的每個調查結果的嚴重性等級。您可以設定自動化規則，在問題清單符合特定屬性 ServiceNow 時，在 Jira Cloud 和 等工具中建立票證。這可讓問題清單在傳送至 Security Hub 或在 Security Hub 中建立後立即建立到票證中。

當您想要在 Security Hub CSPM 之外對特定調查結果採取動作，或將特定調查結果傳送至第三方工具以進行修復或其他調查時，EventBridge 規則很有用。這些規則可用來觸發支援的動作，例如叫用 AWS Lambda 函數或將特定問題清單通知 Amazon Simple Notification Service (Amazon SNS) 主題。

自動化規則會在套用 EventBridge 規則之前生效。也就是說，自動化規則會在 EventBridge 收到問題清單之前觸發並更新問題清單。然後 EventBridge 規則會套用至更新的調查結果。

Security Hub 中的自動化規則

使用 Security Hub，您可以自動化任務，例如更新問題清單詳細資訊和為第三方整合建立票證。

自動化規則和 AWS 區域

自動化規則可以在一個中建立 AWS 區域，然後套用至所有設定的規則 AWS 區域。使用區域彙總時，您只能在主區域中建立規則。在主區域中建立規則時，您定義的任何規則都會套用至所有連結區域，除非您的規則條件排除特定連結區域。您必須為任何非連結區域的區域建立自動化規則。

規則動作和條件

Security Hub 中的自動化規則使用條件來參考 Security Hub 調查結果中的 OCSF 屬性。例如，中 Criteria 參數支援的篩選條件[CreateAutomationRuleV2](#)符合中 Criteria 參數支援的篩選條件[GetFindingsV2](#)。這表示自動化規則中使用的篩選條件可用來取得問題清單。Security Hub 支援下列自動化規則條件的 OCSF 欄位。

OCSF 欄位	主控台篩選條件值	篩選條件運算子	欄位類型
activity_name	Activity name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
class_name	Finding class name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.account.uid	Account ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
cloud.provider	Cloud provider	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF 欄位	主控台篩選條件值	篩選條件運算子	欄位類型
cloud.region	Region	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
comment	Comment	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.assessments.category	Assessment category	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.assessments.name	Assessment name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.control	Security control ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.standards	Applicable standards	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF 欄位	主控台篩選條件值	篩選條件運算子	欄位類型
<code>compliance.status</code>	Compliance status	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
<code>finding_info.desc</code>	Finding description	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
<code>finding_info.related_events.product.uid</code>	Related findings product ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
<code>finding_info.related_events.title</code>	Related findings title	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
<code>finding_info.related_events.uid</code>	Related findings ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
<code>finding_info.src_url</code>	Source URL	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF 欄位	主控台篩選條件值	篩選條件運算子	欄位類型
finding_info.types	Finding type	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.uid	Provider ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.feature.uid	Generator ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.name	Product name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.uid	Product ARN	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.vendor_name	Company name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF 欄位	主控台篩選條件值	篩選條件運算子	欄位類型
metadata.uid	Finding ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
remediation.desc	Recommendation text	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
remediation.references	Recommendation URL	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.cloud_partition	Resource partition	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.name	Resource name	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.region	Resource region	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

OCSF 欄位	主控台篩選條件值	篩選條件運算子	欄位類型
<code>resources.type</code>	Resource type	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
<code>resources.uid</code>	Resource ID	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
<code>severity</code>	Severity	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
<code>status</code>	Status	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
<code>vulnerabilities.fix_coverage</code>	Software vulnerabilities coverage	EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
<code>finding_info.first_seen_time_dt</code>	First observed at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)

OCSF 欄位	主控台篩選條件值	篩選條件運算子	欄位類型
finding_info.last_seen_time_dt	Last observed at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.modified_time_dt	Updated at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
compliance.assessments.meets_criteria	Compliance assessment meets criteria	True, False	Boolean
vulnerabilities.is_exploit_available	Software vulnerabilities with exploit available	True, False	Boolean
vulnerabilities.is_fix_available	Software vulnerabilities with fix available	True, False	Boolean
activity_id	Activity ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
compliance.status_id	Compliance status ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number

OCSF 欄位	主控台篩選條件值	篩選條件運算子	欄位類型
confidence_score	Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
severity_id	Severity ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
status_id	Status ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
finding_info.related_events_count	Related findings count	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
resources.tags	Resource tags	EQUALS	Map

對於標記為字串欄位的條件，在相同欄位上使用不同的篩選條件運算子會影響評估邏輯。如需詳細資訊，請參閱 Security Hub API 參考中的 [StringFilter](#)。

每個條件都支援可用於篩選相符問題清單的最大值。如需每個條件的限制，請參閱 Security Hub API 參考中的 [OcsfFindingFilters](#)

可更新的 OCSF 欄位

以下是可以使用自動化規則更新的 OCSF 欄位。

- Comment

- SeverityId
- StatusId

自動化規則如何評估問題清單

自動化規則會評估 Security Hub 在您建立規則後產生或擷取的新問題清單和更新的問題清單。

自動化規則會評估原始供應商提供的調查結果。供應商可以透過與 Security Hub 的整合，提供新的問題清單並更新現有的問題清單。當您在透過 BatchUpdateFindingsV2 操作建立規則之後更新問題清單欄位時，不會觸發規則。如果您建立自動化規則並進行同時影響相同調查結果欄位的 BatchUpdateFindingsV2 更新，則上次更新會設定該欄位的值。採用下列範例：

您可以使用 將問題清單 Status 的欄位從 BatchUpdateFindingsV2 更新 New 為 In Process。如果您呼叫 GetFindingsV2，Status 欄位現在的值為 In Process。您可以建立自動化規則，將調查結果 Status 的欄位從 變更為 NewSuppressed (請回想規則忽略使用 所做的更新 BatchUpdateFindingsV2)。問題清單提供者會更新問題清單，並將 Status 欄位變更為 New。如果您呼叫 GetFindingsV2，Status 欄位現在的值為 Suppressed 因為已套用自動化規則，而規則是對調查結果採取的最後動作。

當您在 Security Hub 主控台上建立或編輯規則時，主控台會顯示符合規則條件的問題清單預覽。雖然自動化規則會評估問題清單提供者傳送的原始問題清單，但主控台預覽會以最終狀態反映問題清單，如同 GetFindingsV2 API 操作的回應所示 (也就是套用規則動作或其他更新至問題清單之後)。

自動化規則的排序方式

每個自動化規則都會指派一個規則順序。這決定 Security Hub 套用自動化規則的順序，並在多個規則與相同的調查結果或調查結果欄位相關時變得重要。

當多個規則動作與相同的問題清單或問題清單欄位相關時，具有規則順序最高數值的規則會最後套用，並具有最終效果。

當您在 Security Hub 主控台中建立規則時，Security Hub 會根據規則建立的順序自動指派規則順序。您建立的第一個規則會有 1 的規則順序。當存在多個規則時，每個後續建立的規則將具有規則順序的下一個最高可用數值。

當您透過 [CreateAutomationRuleV2](#) API 或 建立規則時 AWS CLI，Security Hub 會 RuleOrder 先套用具有最低數值的規則。然後，它會以遞增順序套用後續規則。如果多個問題清單具有相同的 RuleOrder，Security Hub 會先為 UpdatedAt 欄位套用具有較早值的規則 (也就是最近編輯的規則最後套用)。

您可以隨時修改規則順序。

規則順序範例：

規則 A (規則順序為 1)：

- 規則 A 條件
 - `ProductName = Security Hub CSPM`
 - `Resources.Type` 是 S3 Bucket
 - `Compliance.Status = FAILED`
 - `RecordState` 是 NEW
 - `Workflow.Status = ACTIVE`
- 規則 A 動作
 - 更新Confidence至 95
 - 更新Severity至 CRITICAL
 - 更新Comment至 This needs attention

規則 B (規則順序為 2)：

- 規則 B 條件
 - `AwsAccountId = 123456789012`
- 規則 B 動作
 - 更新Severity至 INFORMATIONAL

首先，規則 A 動作適用於符合規則 A 條件的 Security Hub 調查結果。然後，規則 B 動作會套用到具有指定帳戶 ID 的 Security Hub 調查結果。在此範例中，由於規則 B 最後套用，因此來自指定帳戶 ID 之調查結果Severity中的 結束值為 INFORMATIONAL。根據規則 A 動作，相符調查結果Confidence中的 結束值為 95。

第三方整合

您可以使用自動化規則來建立與 Jira Cloud和 整合的票證ServiceNow ITSM。如需詳細資訊，請參閱[建立第三方整合的規則](#)。

自動化規則無法運作的案例

以下是自動化規則無法運作的情況。

- 獨立帳戶會成為具有委派管理員的組織成員
- 組織管理帳戶會移除委派管理員，並設定新的委派管理員
- 當取消連結的區域設為連結區域時，委派管理員或獨立帳戶的彙整工具組態會變更

在這些情況下，組織的成員可以使用 AWS CLI 或 APIs 中的清單、取得和刪除操作來管理自動化規則。

當取消連結的區域成為連結區域時，委派的管理員或獨立帳戶可以使用清單、取得和刪除操作來管理連結區域中的資源。

在 Security Hub 中建立自動化規則

本主題說明如何建立自動化規則。您可以使用自動化規則來更新問題清單的詳細資訊，或為第三方整合建立票證。您必須在您希望套用自動化規則 AWS 區域 的中個別建立自動化規則。不過，如果您在彙總區域中建立自動化規則，則會套用至所有區域。否則，如果您在非連結區域中建立自動化規則，它只會套用在該區域中。

建立更新問題清單詳細資訊的規則

下列程序說明如何建立更新問題清單詳細資訊的規則。

1. 登入 AWS 您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 在導覽窗格的管理下，選擇自動化。
3. 選擇建立規則。
4. 在詳細資訊下，輸入自動化規則的名稱。
 - （選用）輸入自動化規則的描述。
5. 在動作下，選擇更新問題清單詳細資訊。您可以在搜尋列中搜尋條件並新增條件。若要檢查任何問題清單是否符合您的條件，請選擇預覽相符問題清單。
6. 在更新問題清單詳細資訊下，選擇至少一個問題清單詳細資訊，以便在問題清單符合您的條件時更新。您可以選擇嚴重性、狀態或註解。
7. 在規則設定下，選取啟用或停用。如果您選取已啟用，則會啟用自動化規則，並將處理新的問題清單。如果您選取已停用，則自動化規則會停用，且不會處理任何問題清單。

8. (選用) 在標籤下，選擇新增標籤以輸入要套用至自動化規則的鍵值對。
9. 選擇建立規則。

為第三方整合建立規則

下列程序說明如何建立規則，為第三方整合建立票證。如需 Security Hub CSPM 支援的整合資訊，請參閱 [Security Hub CSPM 的第三方整合](#)。

1. 登入 AWS 您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 在導覽窗格的管理下，選擇自動化。
3. 選擇建立規則。
4. 在詳細資訊下，輸入自動化規則的名稱。
 - (選用) 輸入自動化規則的描述。
5. 在動作下，選擇建立票證。您可以在搜尋列中搜尋條件並新增條件。若要檢查任何問題清單是否符合您的條件，請選擇預覽相符問題清單。
6. 在建立票證下，從下拉式清單中選擇 IT 票證整合，然後選擇新增整合。
7. 在規則設定下，選取啟用或停用。如果您選取已啟用，則會啟用自動化規則，並將處理新的問題清單。如果您選取已停用，則自動化規則會停用，且不會處理任何問題清單。
8. (選用) 在標籤下，選擇新增標籤以輸入要套用至自動化規則的鍵/值對。
9. 選擇建立規則。

在 Security Hub 中檢視自動化規則的詳細資訊

本主題說明如何檢視自動化規則的詳細資訊。您可以檢視自動化規則的下列詳細資訊：

- 名稱和描述
- 動作和條件
- 規則狀態和現有調查結果
- Tags (標籤)

檢視自動化規則的詳細資訊

1. 登入 AWS 您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 在導覽窗格中的管理下，選擇自動化。此畫面會顯示您建立的所有自動化規則。
3. 選取您要檢視的自動化規則。請選擇檢視詳細資料。或者，您可以選擇要檢視的自動化規則名稱。

在 Security Hub 中更新規則順序

本主題說明如何更新 主控台中自動化規則的規則順序。如果您想要編輯自動化規則的條件，請參閱 [Security Hub 中的編輯自動化規則](#)。

您無法在未更新每個自動化規則的規則順序的情況下，更新一個自動化規則的規則順序。例如，您有四個自動化規則：規則 A (1)、規則 B (2)、規則 C (3) 和規則 D (4)。您希望先套用規則 D。若要這樣做，請將其數字從 4 變更為 1。因此，規則 A 得到 2，規則 B 得到 3，規則 C 得到 4。

更新自動化規則的規則順序

1. 登入 AWS 您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 在導覽窗格的管理下，選擇自動化。
3. 選取您要編輯的自動化規則。在訂單下，選擇訂單號碼旁的鉛筆圖示。使用箭頭來判斷新的訂單編號。選擇要確認的 ✓ 圖示。選擇要取消的 X 圖示。或者，您可以選擇變更順序，將自動化規則下移、上移或移至清單頂端。

在 Security Hub 中停用自動化規則

本主題說明如何停用自動化規則。當您停用自動化規則時，Security Hub 會停止套用它們。您可以隨時在建立自動化規則 AWS 區域 的中停用自動化規則。

停用規則

1. 登入 AWS 您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 在導覽窗格中的管理下，選擇自動化。
3. 選取您要停用的自動化規則。在狀態下，選擇已啟用旁的鉛筆圖示。選擇下拉式清單，然後選擇已停用。選擇要確認的 ✓ 圖示。選擇要取消的 X 圖示。您也可以從動作下拉式清單中選擇停用。

在 Security Hub 中啟用自動化規則

本主題說明如何啟用自動化規則。當您啟用自動化規則時，Security Hub 會繼續套用規則。您可以隨時在建立自動化規則 AWS 區域 的 中啟用自動化規則。

啟用規則

1. 登入 AWS 您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 在導覽窗格中的管理下，選擇自動化。
3. 選取您要啟用的自動化規則。在狀態下，選擇已停用旁的鉛筆圖示。選擇下拉式清單，然後選擇已啟用。選擇要確認的 ✓ 圖示。選擇要取消的 X 圖示。您也可以從動作下拉式清單中選擇啟用。

在 Security Hub 中複製自動化規則

本主題說明如何複製自動化規則。如果您想要避免從頭開始建立，複製自動化規則可協助您節省時間。當您複製自動化規則時，您可以更新詳細資訊、動作、規則設定和標籤。您可以在建立自動化規則 AWS 區域 的 中編輯自動化規則。

複製規則

1. 登入 AWS 您的帳戶，並在 <https://console.aws.amazon.com/securityhub/v2/home> 開啟 Security Hub 主控台。
2. 從導覽窗格中，選擇管理，然後選擇自動化。
3. 選取您要複製的自動化規則。然後選擇動作，然後選擇複製。
4. 進行並檢閱您的變更，然後選擇建立規則。

在 Security Hub 中編輯自動化規則

本主題說明如何編輯自動化規則。您可以在建立自動化規則 AWS 區域 的 中編輯自動化規則。

您可以針對自動化規則編輯下列項目：

- 名稱和描述
- 動作
- 規則設定

您無法編輯自動化規則的標籤。

編輯規則

1. 登入 AWS 您的帳戶。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 在導覽窗格中的管理下，選擇自動化。
3. 選取您要編輯的自動化規則。選擇動作，然後選擇編輯。
4. 進行並檢閱您的編輯。
5. 選擇儲存變更。

在 Security Hub 中刪除自動化規則

本主題說明如何刪除自動化規則。您可以在建立自動化規則 AWS 區域 的 中刪除自動化規則。

刪除規則

1. 登入 AWS 您的帳戶，並在 <https://console.aws.amazon.com/securityhub/v2/home> 開啟 Security Hub 主控台。
2. 從導覽窗格中，選擇管理，然後選擇自動化。
3. 選取您要刪除的自動化規則。選擇 Actions (動作)，然後選擇 Delete (刪除)。
4. 選擇刪除。

EventBridge 中的自動化規則

您可以使用 Amazon EventBridge 中的自動化規則來回應 Security Hub 問題清單。Security Hub 會以近乎即時的方式將調查結果傳送至 EventBridge。您可以撰寫基本規則，指出事件符合規則時要採取哪些自動化動作。可自動觸發的動作包括下列項目：

- 在 EventBridge 中設定 API 目的地。
- 叫用 Amazon EC2 執行命令
- 調用 Lambda 函式 ()
- 叫用 Step Functions 狀態機器
- 通知 Amazon SNS 主題或 Amazon SQS 佇列
- 將事件轉送至 Kinesis Data Streams

- 將問題清單傳送至第三方票證系統、聊天、SIEM 或事件反應及管理工具
- [將事件傳送至另一個 AWS 帳戶中的 EventBridge 匯流排](#)

Security Hub 會將新的問題清單和更新的問題清單以事件形式傳送至 EventBridge。然後，您可以設定 EventBridge 規則來回應每個 Security Hub 事件。如需詳細資訊，請參閱《[EventBridge 使用者指南](#)》中的[什麼是 EventBridge](#)？。

Note

如果您為 Security Hub CSPM 中的調查結果定義了 EventBridge 規則，則規則可能會與 Security Hub 定義的規則重疊。為了避免傳送重複的問題清單，請評估您為 Security Hub CSPM 定義的規則，以判斷它們是否與您為 Security Hub 定義的規則重疊。如適用，請停用由 Security Hub 規則取代的任何 Security Hub CSPM 規則。

Note

最佳實務是確保具有存取 EventBridge 許可的使用者使用授予最低必要許可 AWS Identity and Access Management 的政策。如需詳細資訊，請參閱《[EventBridge 使用者指南](#)》中的[EventBridge 和 AWS Identity and Access Management](#)。EventBridge

EventBridge 事件類型

Security Hub 使用以下 Amazon EventBridge 事件類型與 EventBridge 整合。

在 Security Hub 的 EventBridge 儀表板上，所有事件都包含所有這些事件類型。

已匯入的問題清單 V2

Security Hub 會自動將所有新調查結果和現有調查結果的所有更新作為 Findings Imported V2 事件傳送至 EventBridge。每個 Findings Imported V2 事件都包含單一調查結果。

透過[BatchUpdateFindingsV2](#)請求匯入的每個問題清單和更新的每個問題清單都會觸發 Findings Imported V2 事件。

對於管理員帳戶，EventBridge 中的事件饋送包含來自其帳戶及其成員帳戶的問題清單事件。

在彙總區域中，事件摘要包含來自彙總區域和連結區域的問題清單事件。跨區域調查結果會以近乎即時的方式包含在事件饋送中。

您可以在 EventBridge 中定義規則，自動將問題清單路由至修復工作流程、第三方工具[或其他支援的 EventBridge 目標](#)。這些規則可以包含篩選條件，只有在問題清單具有特定屬性值時才會套用規則。

您可以使用此方法自動將所有問題清單或具有特定特性的所有問題清單傳送至回應或修復工作流程。

Note

Security Hub 和 Security Hub CSPM 都會將問題清單傳送到來源下的 EventBridgeaws.securityhub。確保您的 EventBridge 規則使用 Security Hub 特有的詳細資訊類型，以避免與 Security Hub CSPM 問題清單相關的重複通知。

EventBridge 事件格式

Findings Imported V2 事件類型使用以下事件格式。

範例

當 Security Hub 將事件傳送至 EventBridge 時，會使用此格式。

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "Findings Imported V2",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T21:52:17Z",
  "region": "us-west-2",
  "resources": [
    "e51603d1054aad9d9f498d82d6e81acf4cf6bc88140e8ad2273123c73b81084"
  ],
  "detail": {
    "findings": [{
      <finding content>
    }]
  }
}
```

每個事件都會傳送單一調查結果。<finding content>是事件所傳送調查結果的 JSON 內容。

如需問題清單屬性的完整清單，請參閱[Security Hub CSPM 中的 OCSF 問題清單](#)。

設定 EventBridge 的規則

您可以在 Amazon EventBridge 中建立規則，定義在收到 Findings Imported V2 事件時要採取的動作。Findings Imported V2 事件是由透過的更新觸發 [BatchUpdateFindingsV2](#)。

每個規則都包含事件模式，可識別觸發規則的事件。事件模式一律包含事件來源 (aws.securityhub) 和事件類型 (調查結果匯入 V2)。事件模式也可以指定篩選條件，以識別規則套用的調查結果。

事件規則接著會識別規則目標。目標是當 EventBridge 收到調查結果匯入的 V2 事件，且調查結果符合篩選條件時要採取的動作。

此處提供的指示使用 EventBridge 主控台。當您使用主控台時，EventBridge 會自動建立必要的資源型政策，讓 EventBridge 能夠寫入 Amazon CloudWatch Logs。

您也可以使用 EventBridge API [PutRule](#) 的操作。不過，如果您使用 EventBridge API，則必須建立以資源為基礎的政策。如需所需政策的資訊，請參閱《Amazon EventBridge 使用者指南》中的 [CloudWatch Logs 許可](#)。

事件模式的格式

匯入的調查結果 V2 事件的事件模式格式如下：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Findings Imported V2"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- source 會將 Security Hub 識別為產生事件的服務。
- detail-type 會識別事件的類型。
- detail 是選用的，並提供事件模式的篩選條件值。如果事件模式不包含 detail 欄位，則所有調查結果都會觸發規則。

您可以根據任何問題清單屬性來篩選問題清單。對於每個屬性，您提供一或多個值的逗號分隔陣列。

```
"<attribute name>": [ "<value1>", "<value2>" ]
```

如果您為屬性提供多個值，則這些值會由 聯結OR。如果問題清單具有任何列出的值，則問題清單會比對個別屬性的篩選條件。例如，如果您同時提供 INFORMATIONAL 和 LOW 作為 的 Severity.Label，則如果問題清單的嚴重性標籤為 INFORMATIONAL 或 ，則問題清單會相符LOW。

屬性由 聯結AND。如果問題清單符合所有所提供屬性的篩選條件，則問題清單會相符。

當您提供屬性值時，它必須反映 AWS 開放網路安全結構描述架構 (OCSF) 結構中該屬性的位置。

在下列範例中，事件模式提供 ProductArn 和 的篩選條件值 Severity.Label，因此如果問題清單是由 Amazon Inspector 產生且嚴重性標籤為 INFORMATIONAL 或 ，則問題清單會相符LOW。

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Findings Imported V2"
  ],
  "detail": {
    "findings": {
      "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
      "Severity": {
        "Label": ["INFORMATIONAL", "LOW"]
      }
    }
  }
}
```

建立事件規則

您可以使用預先定義的事件模式或自訂事件模式，在 EventBridge 中建立規則。如果您選擇預先定義的模式，EventBridge 會自動填入 source 和 detail-type。EventBridge 也提供欄位，以指定下列調查結果屬性的篩選條件值：

- cloud.account.uid
- compliance.status

- `metadata.product.name`
- `resources.uid`
- `severity`
- `status`

建立 EventBridge 規則（主控台）

1. 前往 <https://console.aws.amazon.com/events/> 開啟 Amazon EventBridge 主控台。
2. 使用下列值，建立可監控調查結果事件的 EventBridge 規則：
 - 針對規則類型，選擇具有事件模式的規則。
 - 選擇如何建置事件模式。

若要使用 建置事件模式...	執行此作業...	
範本	在事件模式區段中，選擇下列選項： • 在事件來源欄位中，選擇 AWS 服務。 • 針對 AWS 服務，選擇 Security Hub。 • 針對事件類型，選擇已匯入的調查結果 V2。 • (選用) 若要使規則更具體，請新增篩選條件值。例如，若要將規則限制為具有作用中記錄狀態的問題清單（若為特定記錄狀態），請選擇作用中。	
自訂事件模式 （如果您想要根據 EventBridge 主控台中未顯示的屬性來	• 在事件模式區段中，選擇自訂模式 (JSON 編輯器)，然後將下列事件模式貼入文字區域：	

若要使用 建置事件模式...	執行此作業...	
篩選問題清單，請使用自訂模式。)	<pre data-bbox="690 220 1063 955"> { "source": ["aws.secu rityhub"], "detail-type": ["Findings Imported V2"], "detail": { "findings": { "<attribut e name> ": ["<value1>", "<value2>"] } } } </pre> • 更新事件模式，以包含您要用作篩選條件的屬性和屬性值。 例如，若要將規則套用至嚴重性為 的調查結果Critical，請使用下列模式範例： <pre data-bbox="690 1375 1063 1795"> { "source": ["aws.securityhub"], "detail-type": ["Findings Imported V2"], "detail":{ "findings": { </pre>	

若要使用 建置事件模式...	執行此作業...	
	<pre> "Severity ": ["Critical"] } } } </pre>	

- 對於目標類型，請選擇AWS 服務，對於選取目標，選擇目標，例如 Amazon SNS 主題或 AWS Lambda 函數。當接收到符合規則中定義之事件模式的事件時，就會觸發目標。

如需建立規則的詳細資訊，請參閱 [《Amazon EventBridge 使用者指南》](#) 中的 [建立對事件做出反應的 Amazon EventBridge 規則](#)。

Note

如果您已為 Security Hub CSPM 中的調查結果定義 EventBridge 規則，則規則可能會與 Security Hub 定義的規則重疊。為了避免傳送重複的問題清單，請評估您為 Security Hub CSPM 定義的規則，以判斷它們是否與您為 Security Hub 定義的規則重疊。如適用，請停用由 Security Hub 規則取代的任何 Security Hub CSPM 規則。

Security Hub 的第三方整合

您可以使用 Security Hub 的第三方整合來增強您的 AWS 安全狀態。透過此功能，您可以啟用使用 Security Hub 調查結果的整合，讓您將操作、調查和回應工具與 Security Hub 整合。目前 Security Hub 支援與 Jira Cloud 和 整合ServiceNow。

主題

- [AWS Security Hub 的整合 Jira Cloud](#)
- [的整合 ServiceNow](#)
- [Security Hub 票證整合的 KMS 金鑰政策](#)
- [測試設定的票證整合](#)

AWS Security Hub 的整合 Jira Cloud

本主題說明如何與 整合 Jira Cloud。在完成本主題中的任何程序之前，您必須購買 Jira Cloud 訂閱計劃。如需訂閱計劃的相關資訊，請參閱 Atlassian 網站上的 [定價](#)。

此整合可讓您手動或自動將 Security Hub 調查結果傳送至 Jira Cloud，以便在操作工作流程中加以管理。例如，您可以將所有權指派給需要調查和修復的問題。

對於組織中的帳戶，只有委派管理員可以設定整合。委派管理員可以針對任何成員帳戶調查結果手動使用建立票證功能。此外，委派管理員可以使用 [自動化規則](#)，自動為與成員帳戶相關聯的任何問題清單建立票證。定義自動化規則時，委派管理員可以設定條件，其中包含所有成員帳戶或特定成員帳戶。如需設定委派管理員的資訊，請參閱 [在 Security Hub 中設定委派管理員帳戶](#)。

對於不在組織中的帳戶，此功能的所有層面都可用。

先決條件

將 Security Hub 與您的 Jira Cloud 環境連線之前，您必須確保在 Jira 環境中完成下列組態步驟。

- 安裝適用於 Jira 雲端應用程式的 AWS Security Hub。
- 至少有一個由公司管理的軟體開發專案。
- 將 AWS 應用程式指派給您要從 Security Hub 接收問題清單的軟體開發專案。

以下列出每個先決條件的步驟。

1. 安裝適用於 Jira Cloud 應用程式的 AWS Security Hub

Security Hub 具有支援其與 Jira 整合的應用程式。此應用程式會安裝自訂欄位和自訂問題類型，允許 Security Hub 填入有關 Security Hub 問題清單的特定屬性。

1. 以管理員身分登入您的 Atlassian 網站。
2. 選擇設定，然後選擇應用程式。
3. 如果導向到市集頁面，請選擇尋找新的應用程式。如果導向應用程式頁面，請選擇探索應用程式，然後搜尋 AWS Security Hub for Jira Cloud。然後選擇立即取得。

2. 建立專案或驗證現有專案

如果您尚未建立專案，則需要此步驟。如需如何建立專案的詳細資訊，請參閱 Jira Cloud Support 文件中的 [建立新專案](#)。

建立專案的需求

建立新專案時，請務必執行下列動作。

- 選擇專案範本的軟體開發。
- 為專案類型選擇公司受管。

現有專案的需求

Jira 環境中將與 Security Hub 整合的任何現有專案都必須是公司管理的專案類型。

3. 將您的專案新增至適用於Jira Cloud應用程式的 AWS Security Hub

為了讓 Security Hub 能夠成功將問題清單傳送到您的 Jira 環境，您要與 Security Hub 搭配使用的每個專案都必須與適用於Jira Cloud應用程式的 AWS Security Hub 建立關聯。將 Jira 專案與應用程式建立關聯可確保的必要自訂欄位與專案建立關聯，並在 Security Hub 將問題清單傳送至專案時填入。

1. 以管理員身分登入您的Atlassian網站。
2. 選擇設定，然後選擇應用程式。
3. 從應用程式清單中，選擇適用於 AWS Jira Cloud 的 Security Hub。
4. 選擇連接器設定索引標籤。
5. 在啟用的專案下，選擇新增 Jira 專案。
 - a. 從下拉式清單中，選擇全部新增，或選取專案。如果您想要新增多個專案，但不是所有專案，請重複此步驟的這個部分。
 - b. 選擇儲存。

您可以從 Installation Manager 索引標籤驗證哪些專案已成功安裝。您也可以從 Installation Manager 索引標籤驗證欄位、畫面、狀態和工作流程的組態。

如需的詳細資訊Jira Cloud，請參閱 Atlassian 網站上的 [Jira Cloud 資源](#)。

建議

為您的 Jira 環境建立專用系統帳戶

Security Hub 與的整合Jira Cloud使用與 Jira 執行個體中特定使用者相關聯的 OAuth 連線。基於下列原因，建議為您的連線建立專用系統帳戶以用於 Security Hub OAuth 連線：

- 專用系統使用者可確保連線不會與具有 Jira 環境許可的員工相關聯，隨著時間而變更，這會影響 Security Hub 與您的 Jira 環境整合的能力。
- Security Hub 在 Jira 中建立的每個問題都會顯示 建立的，這是用來建立 OAuth 連線的使用者名稱。使用 OAuth 連線的系統帳戶將導致此系統帳戶顯示為票證建立者，協助提供問題清單是透過 Security Hub 整合建立，而不是由其他 Jira 使用者手動建立的可見性。

設定 Security Hub 與 之間的整合 Jira Cloud

對於您要傳送 Security Hub 問題清單的每個 Jira Cloud 專案，需要完成下列程序。

Note

當您建立 Jira Cloud 連接器時，系統會將您從目前的 重新導向 AWS 區域 至 "https://3rdp.oauth.console.api.aws"，因此您可以完成連接器註冊。之後，您會回到正在建立連接器 AWS 區域 的。

設定 的整合 Jira Cloud

1. 使用您的登入資料登入 AWS 您的帳戶，然後開啟位於 [https://console.aws.amazon.com/securityhub/v2/home](https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1) 的 Security Hub 主控台？region=us-east-1。
2. 從導覽窗格中，選擇管理，然後選擇整合。
3. 選擇新增 Jira Cloud。
4. 如需詳細資訊，請輸入整合的唯一描述性名稱，並決定是否要輸入整合的選用描述。
5. 針對加密，選擇您希望如何在 Security Hub 中加密整合憑證。
 - 使用 AWS 擁有的金鑰 - 使用此選項時，Security Hub 擁有的服務金鑰將用於加密 Security Hub 中的整合憑證資料。
 - 選擇不同的 KMS 金鑰（進階） - 使用此選項，您可以選擇您已建立 AWS KMS key 的，用於加密 Security Hub 中的整合憑證資料。如需有關如何建立 AWS KMS 金鑰的資訊，請參閱《AWS Key Management Service 開發人員指南》中的[建立 AWS KMS 金鑰](#)。如果您選擇使用自己的金鑰，則必須將政策陳述式新增至允許 Security Hub 存取金鑰的 KMS 金鑰。如需必要[AWS KMS 政策的詳細資訊](#)，請參閱 [Security Hub 票證整合的重要政策](#)。

 Note

一旦完成此組態，您就無法變更這些設定。不過，如果您選擇自訂金鑰，您可以隨時編輯自訂金鑰政策。

6. (選用) 對於標籤，請建立標籤並將其新增至您的整合。您最多可以新增 50 個標籤。
7. 針對授權，選擇建立連接器並授權。您選擇允許 來完成授權的快顯視窗隨即出現。完成授權後，會出現核取方塊，讓您知道授權成功。
8. 針對組態，輸入 Jira Cloud 專案 ID。
9. 選擇完成組態。完成組態後，您可以在已設定的整合索引標籤中檢視已設定的整合。

設定與 Jira 的整合後，您可以測試連線，以確認 Jira 環境和 Security Hub 中的所有項目都已正確設定。如需詳細資訊，請參閱[測試設定的票證整合](#)。

其他 Jira 整合詳細資訊

速率限制考量

Jira 會強制執行 API 速率限制，以維持服務穩定性，並確保其平台的公平使用。使用 AWS Security Hub 與 Jira 整合時，這些速率限制可能會影響 Security Hub 調查結果的處理，尤其是在產生大量調查結果的環境中。這可能會導致票證建立延遲，而且在問題清單磁碟區極高的情況下，有些問題清單可能根本不會處理為 Jira 票證。若要最佳化整合，請考慮在 Security Hub 中對自動化規則實作篩選條件，以排定最重要問題清單的票證優先順序、透過其管理員主控台監控 Jira API 使用情況，並根據 Jira 授權層的特定費率限制規劃工作流程。對於關鍵業務實作，請聯絡您的 Jira 管理員以檢閱您的速率限制配置。

如需 Jira API 速率限制的詳細資訊，請參閱 Atlassian 開發人員指南網站上的[速率限制](#)文件。

身分驗證和安全性

Jira API 身分驗證需要適當的 OAuth 2.0 組態才能安全存取。確保您的應用程式遵循 Atlassian 的安全最佳實務進行 API 整合。

資源：

- Jira Rest API v3： <https://developer.atlassian.com/cloud/jira/platform/rest/v3/intro/>
- 實作 OAuth 2.0 (3LO)： <https://developer.atlassian.com/cloud/oauth/getting-started/implementing-oauth-3lo/>

- 管理 Jira Cloud 應用程式： <https://support.atlassian.com/jira-cloud-administration/resources/>
- 管理 Jira 許可： <https://support.atlassian.com/jira-cloud-administration/docs/manage-project-permissions/>

建立 Jira Cloud 整合票證

建立與 的整合後 Jira Cloud，您可以為問題清單建立票證。

Note

問題清單一律會在其整個生命週期內與單一票證建立關聯。初始建立後對問題清單的所有後續更新都會傳送到相同的票證。如果與自動化規則相關聯的連接器已變更，則更新的連接器只會用於符合規則條件的新問題清單和傳入問題清單。

為問題清單建立票證

1. 使用您的登入資料登入 AWS 您的帳戶，然後開啟位於 <https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1> 的 Security Hub 主控台。
2. 在導覽窗格中的庫存下，選擇調查結果。
3. 選擇問題清單。在調查結果中，選擇建立票證。
4. 針對整合，開啟下拉式選單，然後選擇整合。此整合是您先前在設定 Jira Cloud 專案時建立的整合。選擇您要傳送問題清單的整合。
5. 選擇建立。

檢視 Jira Cloud 整合的票證

為問題清單建立票證後，您可以在 Jira Cloud 執行個體上開啟票證。

在 Jira Cloud 執行個體上檢視問題清單

1. 使用您的登入資料登入 AWS 您的帳戶，然後開啟位於 <https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1> 的 Security Hub 主控台。
2. 在導覽窗格中的庫存下，選擇調查結果。
3. 選擇您建立票證的調查結果。
4. 在調查結果中，選擇票證 ID 以在 Jira Cloud 執行個體上檢視票證或檢視 JSON。

的整合 ServiceNow

本主題說明如何存取 Security Hub 主控台來設定 的整合ServiceNow ITSM。在完成本主題中的任何程序之前，您必須先訂閱 ServiceNow ITSM，才能新增此整合。如需詳細資訊，請參閱 ServiceNow 網站上的[定價頁面](#)。

對於組織中的帳戶，只有委派管理員可以設定整合。委派管理員可以手動使用任何成員帳戶調查結果的建立票證功能。此外，委派管理員可以使用[自動化規則](#)，自動為與成員帳戶相關聯的任何問題清單建立票證。定義自動化規則時，委派管理員可以設定條件，其中包含所有成員帳戶或特定成員帳戶。如需設定委派管理員的資訊，請參閱[在 Security Hub 中設定委派管理員帳戶](#)。

對於不在組織中的帳戶，此功能的所有層面都可用。

先決條件 - 設定 ServiceNow 環境

您必須先完成下列先決條件，才能設定 的整合ServiceNow ITSM。否則，您在 ServiceNow ITSM和 Security Hub 之間的整合將無法運作。

1. 安裝適用於 IT Service Management (ITSM) 的 Security Hubfindings 整合

下列程序說明如何安裝 Security Hub 外掛程式。

1. 登入您的ServiceNow ITSM執行個體，然後開啟應用程式導覽器。
2. 導覽至 [ServiceNow 存放區](#)。
3. 搜尋適用於 IT Service Management (ITSM) 的 Security Hub 調查結果整合，然後選擇取得以安裝應用程式。

Note

在 Security Hub 應用程式的設定中，選擇當新的 Security Hub 問題清單傳送到您的 ServiceNow ITSM環境時要採取的動作。您可以選擇不執行任何操作、建立事件、建立問題或建立兩者（事件/問題）。

2. 設定傳入 OAuth 請求的用戶端登入資料授予類型

您必須為傳入 OAuth 請求設定此授予類型。如需詳細資訊，請參閱ServiceNow支援網頁中[支援傳入 OAuth 的用戶端憑證授予類型](#)。

3. 建立 OAuth 應用程式

如果您已建立 OAuth 應用程式，則可以略過此先決條件。如需有關建立 OAuth 應用程式的資訊，請參閱[設定 OAuth](#)。

先決條件 - 設定 AWS Secrets Manager

若要使用 Security Hub 與 ServiceNow 的整合，ServiceNow OAuth 應用程式的登入資料必須存放在 Secrets Manager 中。在 Secrets Manager 中存放您的登入資料可讓您控制和查看登入資料的使用情況，同時允許 Security Hub 使用登入資料與您的 ServiceNow 執行個體整合。若要將登入資料儲存在 Secrets Manager 中，您必須使用客戶受管 AWS KMS 金鑰來保護秘密。此 AWS KMS 金鑰可讓您在靜態儲存時保護秘密，也允許將政策連接至金鑰，讓 Security Hub 能夠存取保護秘密的金鑰。

使用下列步驟為您的 ServiceNow 登入資料設定 Secrets Manager。

步驟 1：將政策連接至您的 AWS KMS 金鑰

若要成功設定 ServiceNow 整合，您必須先授予 Security Hub 許可，才能使用與 Secrets Manager 中的 ServiceNow 登入資料相關聯的 AWS KMS 金鑰。

修改 Security Hub 的 AWS KMS 金鑰政策以存取您的 ServiceNow 登入資料

1. 在 <https://console.aws.amazon.com/kms> 開啟 AWS KMS 主控台。
2. 若要變更 AWS 區域，請使用頁面右上角的區域選擇器。
3. 選取現有的 AWS KMS 金鑰，或執行《AWS KMS 開發人員指南》中的[建立新金鑰](#)的步驟。
4. 在 Key policy (金鑰政策) 區段中，選擇 Edit (編輯)。
5. 如果顯示切換到政策檢視，請選擇它以顯示金鑰政策，然後選擇編輯。
6. 將下列政策區塊複製到您的 AWS KMS 金鑰政策，以授予 Security Hub 使用您的金鑰的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::your-account-id:root"
      },
      "Action": "kms:*",
```



```

    "Resource": "*"
  },
  {
    "Sid": "Allow Security Hub connector service to decrypt secrets",
    "Effect": "Allow",
    "Principal": {
      "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "kms:ViaService": "secretsmanager.your-region.amazonaws.com"
      },
      "StringLike": {
        "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:your-region:your-account-id:secret:ServiceNow*"
      }
    }
  }
]
}

```

7. 透過取代政策範例中的下列值來編輯政策：

- 將 *your-account-id* 取代為 AWS 您的帳戶 ID。
- *###* 取代為您的 AWS 區域（例如 us-east-1）。

8. 如果您在最終陳述式之前新增政策陳述式，請在新增此陳述式之前新增逗號。請確定 AWS KMS 金鑰政策的 JSON 語法有效。

9. 選擇儲存。

10. （選用）將金鑰 ARN 複製到記事本，以供後續步驟使用。

步驟 2：在 Secrets Manager 中建立秘密

在 Secrets Manager 中建立秘密，以存放您的 ServiceNow 登入資料。Security Hub 會在與您的 ServiceNow 環境互動時存取此秘密。

請依照 AWS Secrets Manager 《使用者指南》中的步驟[建立秘密](#)。建立秘密之後，請複製秘密 ARN，因為在建立 Security Hub 連接器時需要此操作。

建立秘密時，請務必設定下列項目：

秘密類型

其他類型的秘密

鍵/值對（純文字格式）

```
{
  "ClientId": "your-servicenow-client-id",
  "ClientSecret": "your-servicenow-client-secret"
}
```

Note

欄位名稱必須完全為 ClientId 和 ClientSecret（區分大小寫）。Security Hub 需要這些確切名稱才能擷取登入資料。

加密金鑰

使用您在步驟 1 中設定的 AWS KMS 金鑰

資源政策

請使用下列資源政策：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:your-region:your-account-id:secret:ServiceNow*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "your-account-id",
          "aws:SourceArn": "arn:aws:securityhub:your-region:your-account-id:*"
        }
      }
    }
  ]
}
```

```
}
```

現在已設定您的秘密，您可以使用 CreateConnectorV2 API 或 AWS 主控台建立 Security Hub 連接器。您需要提供：

- InstanceName：您的 ServiceNow 執行個體 URL（例如 `your-instance.service-now.com`）
- SecretArn：您在此程序中建立之秘密的 ARN

設定 的整合 ServiceNow ITSM

Security Hub 可以在 中自動建立事件或問題ServiceNow ITSM。

設定 的整合 ServiceNow ITSM

1. 使用您的登入資料登入 AWS 您的帳戶，然後開啟位於 [https://console.aws.amazon.com/securityhub/v2/home](https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1) 的 Security Hub 主控台？region=us-east-1。
2. 從導覽窗格中，選擇管理，然後選擇整合。
3. 在下ServiceNow ITSM，選擇新增整合。
4. 如需詳細資訊，請輸入整合的名稱，並決定是否要輸入整合的選用描述。
5. 針對加密，選擇您希望如何在 Security Hub 中加密整合憑證。
 - 使用 AWS 擁有的金鑰 - 使用此選項時，Security Hub 擁有的服務金鑰將用於加密 Security Hub 中的整合憑證資料。
 - 選擇不同的 KMS 金鑰（進階） - 使用此選項，您可以選擇您已建立 AWS KMS key 的，用於在 Security Hub 中加密整合憑證資料。如需有關如何建立 AWS KMS 金鑰的資訊，請參閱《AWS Key Management Service 開發人員指南》中的[建立 AWS KMS 金鑰](#)。如果您選擇使用自己的金鑰，則必須將政策陳述式新增至允許 Security Hub 存取金鑰的 KMS 金鑰。如需必要[AWS KMS 政策的詳細資訊](#)，請參閱 [Security Hub 票證整合的重要](#)政策。

Note

一旦完成此組態，您就無法變更這些設定。不過，如果您選擇自訂金鑰，您可以隨時編輯自訂金鑰政策。

6. 針對登入資料，輸入您的 ServiceNow ITSM URL，以及在先決條件區段中產生的 AWS Secrets Manager 秘密 ARN。

7. 對於標籤，決定是否要建立選用標籤並將其新增至您的整合。
8. 選擇新增整合作業。完成組態後，您可以在已設定的整合索引標籤中檢視已設定的整合。

設定與 ServiceNow 的整合後，您可以測試連線，以確認所有內容都已在您的 ServiceNow 環境和 Security Hub 中正確設定。如需詳細資訊，請參閱[測試設定的票證整合](#)。

建立ServiceNow ITSM整合票證

建立與 的整合後ServiceNow ITSM，您可以為問題清單建立票證。

Note

問題清單一律會在其整個生命週期內與單一票證建立關聯。初始建立後對問題清單的所有後續更新都會傳送到相同的票證。如果與自動化規則相關聯的連接器已變更，則更新的連接器只會用於符合規則條件的新問題清單和傳入問題清單。

為問題清單建立票證

1. 使用您的登入資料登入 AWS 您的帳戶，然後開啟位於 [https://console.aws.amazon.com/securityhub/v2/home](https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1) 的 Security Hub 主控台？region=us-east-1。
2. 在導覽窗格中的庫存下，選擇調查結果。
3. 選擇問題清單。在調查結果中，選擇建立票證。
4. 針對整合，開啟下拉式選單，然後選擇整合。
5. 選擇建立。

檢視ServiceNow ITSM整合的票證

為問題清單建立票證後，您可以在ServiceNow ITSM執行個體上開啟票證。

在ServiceNow ITSM執行個體上檢視問題清單

1. 使用您的登入資料登入 AWS 您的帳戶，然後開啟位於 [https://console.aws.amazon.com/securityhub/v2/home](https://console.aws.amazon.com/securityhub/v2/home?region=us-east-1) 的 Security Hub 主控台？region=us-east-1。
2. 在導覽窗格中的庫存下，選擇調查結果。
3. 選擇您建立票證的調查結果。
4. 在調查結果中，選擇票證 ID 來檢視ServiceNow ITSM執行個體上的票證或檢視 JSON。

Security Hub 票證整合的 KMS 金鑰政策

搭配 Security Hub 票證整合使用客戶受管 KMS 金鑰時，需要將其他政策新增至 KMS 金鑰，以允許 Security Hub 與金鑰互動。此外，需要新增政策，以允許將金鑰新增至 Security Hub 連接器許可的主體存取金鑰。

Security Hub 許可政策

下列政策概述 Security Hub 能夠存取和使用與 Jira 和 ServiceNow 連接器相關聯的 KMS 金鑰所需的許可。此政策需要新增至與 Security Hub 連接器相關聯的每個 KMS 金鑰。

政策包含下列許可：

- 允許 Security Hub 使用 金鑰來保護、暫時存取或重新整理用於與您的票證整合通訊的字符。透過檢查來源 ARN 和加密內容的條件區塊，許可僅限於與特定 Security Hub 連接器相關的操作。
- 允許 Security Hub 透過允許 DescribeKey 操作來讀取有關 KMS 金鑰的中繼資料。Security Hub 必須具備此許可，才能驗證金鑰的狀態和組態。存取僅限於透過來源 ARN 條件的特定 Security Hub 連接器。

```
{
  "Sid": "Allow Security Hub access to the customer managed key",
  "Effect": "Allow",
  "Principal": {
    "Service": "connector.securityhub.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt",
    "kms:ReEncrypt*"
  ],
  "Resource": "*",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:securityhub:Region:AccountId:connectorv2/*"
    },
    "StringLike": {
      "kms:EncryptionContext:aws:securityhub:connectorV2Arn":
        "arn:aws:securityhub:Region:AccountId:connectorv2/*",
      "kms:EncryptionContext:aws:securityhub:providerName": "CloudProviderName"
    }
  }
}
```

```

    }
  },
  {
    "Sid": "Allow Security Hub read access to the customer managed key",
    "Effect": "Allow",
    "Principal": {
      "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": [
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:securityhub:Region:AccountId:connectorv2/*"
      }
    }
  }
}

```

透過取代政策範例中的下列值來編輯政策：

- 將 *CloudProviderName* 取代為 JIRA_CLOUD或 SERVICENOW
- 將 *AccountId* 取代為您建立 Security Hub 連接器的帳戶 ID。
- 將 *##* 取代為您的 AWS 區域（例如 us-east-1）。

Security Hub 操作的 IAM 主體存取

將客戶受管 KMS 金鑰指派給 Security Hub 連接器的任何委託人都需要具有許可，才能為要新增至連接器的金鑰執行金鑰操作（描述、產生、解密、重新加密和列出別名）。這適用於 [CreateConnectorV2](#) 和 [CreateTicketV2](#) APIs。對於將與這些 APIs 互動的任何委託人，下列政策陳述式應包含在政策中。

```

{
  "Sid": "Allow permissions to access key through Security Hub",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::AccountId:role/RoleName"
  },
  "Action": [

```

```

        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.Region.amazonaws.com"
            ]
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:providerName": "CloudProviderName"
        }
    }
},
{
    "Sid": "Allow read permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/RoleName"
    },
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.Region.amazonaws.com"
            ]
        }
    }
}
}

```

透過取代政策範例中的下列值來編輯政策：

- 將 *RoleName* 取代為呼叫 Security Hub 的 IAM 角色名稱。
- 將 *CloudProviderName* 取代為 JIRA_CLOUD或 SERVICENOW。
- 將 *AccountId* 取代為您建立 Security Hub 連接器的帳戶 ID。
- 將 *##* 取代為您的 AWS 區域（例如 us-east-1）。

測試設定的票證整合

對於設定的 Jira 和 ServiceNow 整合，您可以測試連線，以確保 Security Hub 和 Jira 或 ServiceNow 環境中的所有組態都已完成。

測試票證功能會建立標題為 的票證 TESTING Test CreateTicketV2 Finding。測試票證會填入範例資料，例如帳戶 ID 和執行測試的帳戶區域、範例資源詳細資訊，以及範例 AWS 問題清單 JSON。

使用主控台測試整合

使用下列步驟來測試您的整合：

1. 在 Security Hub 導覽面板中，選擇整合。
2. 在已設定的整合索引標籤中，選擇您要測試的整合。
3. 在整合的概觀頁面中，選擇建立測試票證。
4. 如果測試成功，將會顯示成功訊息以及測試票證的連結。如果測試未成功，則會顯示測試的錯誤。根據錯誤訊息，解決 Security Hub 或 Jira 或 Service Now 環境中的組態問題。

Note

測試票證功能旨在協助驗證設定新連線或變更現有連線時的端對端功能。此功能將在每次使用 Jira 或 Service Now 環境中建立新的票證，且不適用於定期驗證您的連線。

使用 進行測試 AWS CLI

若要使用 測試整合 AWS CLI，請使用 `create-ticket-v2` 命令搭配 `--mode DRYRUN` 參數：

```
aws securityhub create-ticket-v2 \  
  --mode DRYRUN \  
  --region <your-region> \  
  --connector-id <your-connector-id> \  
  --finding-metadata-uid "TEST_FINDING"
```

範例

下列範例示範如何測試 整合：

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region us-east-1 \
  --connector-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
  --finding-metadata-uid "TEST_FINDING"
```

成功回應

成功的回應會傳回下列項目：

```
{
  "TicketId": "a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6",
  "TicketSrcUrl": "https://your-instance.service-now.com/nav_to.do?uri=x_aws_se_0_finding.do?sys_id=a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6"
}
```

回應TicketSrcUrl中的 提供直接連結，可在 Jira 或 ServiceNow 環境中檢視測試票證。

如果測試失敗，將會顯示錯誤訊息，指出需要解決的組態問題。

故障診斷 Jira 雲端整合錯誤

從 Security Hub 測試與 Jira Cloud 的整合時，可能會傳回下列錯誤訊息。這些錯誤訊息可讓您深入了解連接器的組態問題可能在哪裡，以及如何解決。

Jira Cloud 整合錯誤訊息

錯誤	錯誤訊息	可能的原因和解決方案
ConflictException	找不到 jira 專案	可能原因：連接器上的專案不正確，或憑證/許可問題導致我們無法存取專案。 可能的解決方案：將正確的專案新增至連接器，或使用正確的登入資料重新驗證至 Jira。

錯誤	錯誤訊息	可能的原因和解決方案
ConflictException	找不到 Security Hub 問題類型	可能原因：應用程式安裝問題或問題類型未與專案相關聯。 可能的解決方案：執行先決條件步驟，將 Jira 應用程式安裝到您的 Jira 環境，並將應用程式與專案建立關聯。

監控 Security Hub 中的用量和成本

用量頁面可協助您了解和管理在整個組織中執行 Security Hub 的成本。在此頁面上，您可以檢視目前的成本、查看預計的每月成本、依功能或帳戶探索用量，以及尋找最佳化支出的策略。

誰可以存取用量頁面

任何已啟用 Security Hub 的帳戶都可以使用用量頁面。若要存取它，請開啟 Security Hub 主控台，然後在左側導覽面板的設定下選擇用量。

體驗會根據您的帳戶類型而有所不同：

- 委派管理員或管理帳戶 – 您會看到完整的用量頁面，其中包含組織成本摘要、依功能的用量、依帳戶的用量，以及成本最佳化策略。
- 成員帳戶或獨立帳戶 – 您會看到帳戶成本摘要，僅供您帳戶使用。由於您正在檢視單一帳戶，因此無法使用依帳戶索引標籤。

組織和帳戶成本摘要

Note

組織成本摘要區段只能從委派管理員帳戶或管理帳戶顯示。成員帳戶和獨立帳戶會改為查看帳戶成本摘要。

當您從委派管理員或管理帳戶開啟用量頁面時，組織成本摘要區段會顯示目前帳單週期中組織 Security Hub 成本的高階概觀。本節包含下列項目：

- 上次重新整理的資料 – Security Hub 上次重新整理組織用量資料的日期。Security Hub 會定期重新整理此資料。如果您在造訪用量頁面時資料超過 24 小時，Security Hub 會自動觸發重新整理。重新整理會在幾個小時內完成，視您組織的大小而定。重新整理資料時，會出現提醒，其中包含即將提供資料的訊息。
- 目前成本 – 從目前帳單週期開始到上次重新整理資料的日期，您的組織因使用 Security Hub 而產生的總金額。
- 預計每月成本 (30 天) – 根據過去 7 天的用量估計每月成本，推斷為完整的 30 天計費週期。此預測包含付費和免費試用用量，讓您實際估算每月成本。預計成本不會計入您與之協商的任何折扣 (EDPs) AWS。如果您的預計成本似乎低於目前成本，這表示您的用量已減少，並且根據過去 7 天的用量，則 30 天的帳單將低於目前帳單週期中的帳單。

功能檢視

功能檢視會顯示整個組織的成本和用量，依安全功能組織。功能會組織成三個可擴展的群組。您可以展開或摺疊每個群組，以查看其中的個別用量類型。每個用量類型都會直接映射到 AWS Cost Explorer 中對應的用量類型。

Security Hub 基本計劃 – 監控您的 EC2 執行個體、ECR 容器映像、Lambda 函數、IAM 使用者和 IAM 角色。涵蓋風險與暴露分析、漏洞管理（採用 Amazon Inspector 技術）、安全狀態管理（採用 Security Hub CSPM 技術）和安全回應。所有這些功能都以單一資源價格包含在基本計劃中 — 您不需要另外啟用或支付 Amazon Inspector 或 AWS Security Hub CSPM 的費用，而且您不需要為基礎服務使用量支付雙倍費用。

威脅分析 – 包括 CloudTrail 管理事件和資料事件、網路活動和其他日誌。這些功能涵蓋採用 Amazon GuardDuty 技術的威脅偵測。

其他功能 – 包括 Lambda 函數程式碼掃描。這是選用的增強功能，採用 Amazon Inspector 技術來分析 Lambda 函數應用程式程式碼是否有安全漏洞。

如需每個功能定價的詳細資訊，請參閱 [Security Hub 定價](#)。

此檢視中的資料表包含每種用量類型的下列資料欄：

- 目前用量 – 從計費週期開始到資料上次重新整理日期為止，此用量類型的總用量，涵蓋所有帳戶和所有區域。
- 免費用量 – 目前免費試用中帳戶的此用量類型總用量。免費用量值以綠色顯示。
- 目前成本 – 從計費週期開始到資料上次重新整理日期為止，此用量類型的總成本，涵蓋所有帳戶和所有區域。

- 免費試用值 – 如果目前在免費試用中的帳戶不在試用中，您為此用量類型產生的成本。這可協助您了解免費試用的價值。
- 預計每月成本 (30 天) – 此用量類型的估計每月成本，從所有帳戶和所有區域的過去 7 天的用量推斷。這包括付費和免費試用用量，以提供預估的每月成本。

帳戶檢視

Note

帳戶檢視僅適用於委派管理員帳戶或管理帳戶。

選擇帳戶檢視，以檢視所有區域中個別成員帳戶組織的成本。此檢視可協助您識別哪些帳戶的成本最高。

下表列出具有下列資料欄的每個帳戶：

- 帳戶 – AWS 帳戶 ID，顯示為可點選連結。選擇帳戶會開啟詳細的明細面板。
- 目前成本 – 從計費週期開始到資料上次重新整理日期為止，此帳戶在所有區域中的總成本。
- 免費試用值 – 如果此帳戶不在免費試用中，將會產生的成本。
- 預計每月成本 (30 天) – 此帳戶的估計每月成本，從所有區域的過去 7 天用量推斷為完整的 30 天計費週期。預測包含付費和免費試用用量，以提供每月成本的代表性預估。預計成本不會計入您與 AWS (EDPs 協商) 的任何折扣。

如果 Security Hub 在過去 7 天內在該帳戶上啟用，則預測會根據啟用後的天數而定。7 天後，投影會使用過去 7 天的完整用量。用量頁面目前不會偵測帳戶何時停用 Security Hub。如果 Security Hub 最近已在一或多個帳戶上停用，這些帳戶將繼續出現在預測中，直到其用量過期為止。對投影進行這些變更後，請等待 7 天，以反映組織的更新狀態。

帳戶詳細資訊檢視

當您從清單中選擇帳戶時，頁面右側會開啟詳細資訊面板。此面板會顯示與功能檢視相同的功能層級明細，但會篩選至該特定帳戶。您可以查看該帳戶內所有區域中每個用量類型的目前用量、免費用量、目前成本、免費試用價值和預計每月成本。

成本最佳化策略

選擇用量頁面頂端的成本最佳化策略，以導覽至專用頁面，以可行的方式管理您的成本，同時維護您的安全涵蓋範圍。

每個策略都會顯示為獨立選項，您可以根據組織的需求來評估和套用。沒有安全權衡的選項會先列出。套用任何策略後，變更通常需要 24 到 48 小時才能反映在您的帳單中。

相關資源

- [Security Hub 定價](#)
- [AWS Cost Explorer 使用者指南](#)

停用 Security Hub

停用單一帳戶的 Security Hub

如果您的帳戶不是組織的一部分，您可以隨時在 Security Hub 主控台中停用 Security Hub，或使用 [DisableSecurityHubV2 API](#)。當您停用 Security Hub 時，它會停止從偵測引擎擷取問題清單，您也無法存取現有的問題清單、整合和組態。

當您在所有區域中停用您帳戶的 Security Hub 時，Security Hub 也會刪除您啟用服務時建立的服務連結 IAM Access Analyzer。如果自動刪除失敗，您可以呼叫 IAM Access Analyzer `DeleteServiceLinkedAnalyzer` API 操作來刪除分析器。只有在您帳戶的 Security Hub 完全停用之後，此操作才會成功。如果您在單一區域中停用 Security Hub，但在其他區域中保持啟用，則未使用的存取分析器會繼續執行，而問題清單會繼續複寫到剩餘的啟用區域。

停用 Security Hub

1. 使用您的登入資料登入 AWS 您的帳戶，然後開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從導覽窗格中，選擇一般。
3. 在 Security Hub 中，選擇停用。在快顯視窗中，輸入 **Disable**，然後選擇停用。

停用整個組織的 Security Hub

如果您是 AWS 組織的委派管理員，您有兩個選項可在成員帳戶之間停用 Security Hub。

選項 1：使用偵測引擎停用 Security Hub

您可以利用委派管理員帳戶中政策目錄中的 Security Hub（基本和其他功能）部署和政策，針對特定組織單位、帳戶或區域停用 Security Hub 以及 Amazon Inspector。

使用政策在成員帳戶之間停用 Security Hub 和 Amazon Inspector

1. 使用您的 AWS 帳戶搭配委派管理員登入資料來登入。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從導覽窗格中，選擇管理，然後選擇組態。
3. 從組態目錄中選擇 Security Hub（基本和其他功能）。
4. 在詳細資訊區段的設定 Security Hub 頁面上，輸入政策的名稱和描述（例如，「Security Hub Disabling Policy」）。
5. 在帳戶選取區段中，選取下列其中一個選項。如果您想要將停用套用至所有組織單位和帳戶，請選擇所有組織單位和帳戶。如果您想要將停用套用至特定組織單位和帳戶，請選擇特定組織單位和帳戶。如果您選擇此選項，請使用搜尋列或組織結構樹來指定目標組織單位和帳戶。
6. 在區域區段中，選擇停用所有區域以停用所有區域中的 Security Hub。選擇性地選擇是否自動停用新區域。選擇指定區域，以選擇要停用的特定區域。
7. （選用）如需進階設定，請參閱 中的指引 AWS Organizations。
8. （選用）針對資源標籤，將標籤新增為鍵/值對，以協助您輕鬆識別組態。
9. 選擇下一步。
10. 檢閱您的變更，然後選擇套用。您的目標帳戶是根據政策設定。政策的組態狀態會顯示在政策頁面頂端。

停用 Amazon GuardDuty 和 AWS Security Hub CSPM

對於 GuardDuty 和 Security Hub CSPM 功能，您必須從個別委派的管理員帳戶手動停用功能。GuardDuty 和 Security Hub CSPM 使用部署（一次性動作）而非政策，因此必須從各自的主控台手動執行停用。

選項 2：僅停用 Security Hub

如果您有現有的 Security Hub 政策，並且只想要停用 Security Hub，而不會影響 Amazon Inspector、GuardDuty 或 Security Hub CSPM，請遵循下列步驟。

僅跨成員帳戶停用 Security Hub

1. 使用您的 AWS 帳戶搭配委派管理員登入資料來登入。開啟位於 <https://console.aws.amazon.com/securityhub/v2/home> 的 Security Hub 主控台。
2. 從導覽窗格中，選擇管理，然後選擇組態。
3. 從設定的政策中選擇任何 Security Hub 政策。
4. 按一下編輯政策，然後在帳戶選取區段中，選取下列其中一個選項。如果您想要將停用套用至所有組織單位和帳戶，請選擇所有組織單位和帳戶。如果您想要將停用套用至特定組織單位和帳戶，請選擇特定組織單位和帳戶。如果您選擇此選項，請使用搜尋列或組織結構樹來指定目標組織單位和帳戶。
5. 在區域區段中，選擇停用所有區域以停用所有區域中的 Security Hub。選擇性地選擇是否自動停用新區域。選擇指定區域，以選擇要停用的特定區域。
6. （選用）如需進階設定，請參閱 AWS Organizations 的指引。
7. （選用）針對資源標籤，將標籤新增為鍵/值對，以協助您輕鬆識別組態。
8. 選擇下一步。
9. 檢閱您的變更，然後選擇套用。您的目標帳戶是根據政策設定。政策的組態狀態會顯示在組態頁面頂端。

對其他安全服務的影響

透過 Security Hub 政策停用 Security Hub 不會影響 Security Hub CSPM、GuardDuty 和 Amazon Inspector 組態。

如果您只需要跨成員帳戶停用 Amazon Inspector，您可以使用 Security Hub 組態目錄中的漏洞管理政策。導覽至 Security Hub 組態頁面，從 Amazon Inspector 選擇漏洞管理，然後依照與上述 Security Hub 停用程序類似的步驟建立停用政策。

Security Hub 中的 AWS 安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，該架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[共同責任模型](#) 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 – AWS 負責保護在 Cloud AWS 中執行 AWS 服務的基礎設施。AWS 也為您提供可安全使用的服務。在 [AWS 合規計畫](#) 中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用於 Security Hub 的合規計畫，請參閱 [AWS 合規計畫範圍內的服務](#)。

- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您的公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Security Hub 時套用共同責任模型。下列主題說明如何設定 Security Hub 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Security Hub 資源。

主題

- [AWS Security Hub 中的資料保護](#)
- [AWS Security Hub 的 Identity and Access Management](#)
- [AWS Security Hub 的合規驗證](#)
- [AWS Security Hub 中的彈性](#)
- [AWS Security Hub 中的基礎設施安全性](#)
- [AWS Security Hub 和介面 VPC 端點 \(AWS PrivateLink\)](#)

AWS Security Hub 中的資料保護

[共同責任模型](#)適用於 AWS Security Hub AWS 中的資料保護。如此模型所述，AWS 負責保護執行所有的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱[資料隱私權常見問答集](#)。如需歐洲資料保護的相關資訊，請參閱「[一般資料保護法規 \(GDPR\) 中心](#)」。

基於資料保護目的，我們建議您保護 AWS 帳戶登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《使用者指南》中的[使用 CloudTrail 追蹤](#)。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-3](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Security Hub 或使用 AWS 服務 主控台、API AWS CLI 或其他 AWS SDKs 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

Security Hub 是多租戶服務產品。為了協助保護您的資料，Security Hub 會加密靜態資料和元件服務之間傳輸中的資料。

選擇不使用您的資料以改善服務

Note

本文件頁面僅適用於 2025 年 12 月 2 日推出的增強型 AWS Security Hub。如果您是原始 AWS Security Hub（現為 AWS Security Hub CSPM）的客戶，則以下所述的資料用量將僅在您啟用增強型 AWS Security Hub 之後適用。

您可以選擇不使用您的資料（在 Security Hub 服務條款中定義為「Security Hub 內容」），以使用 AWS Organizations 選擇不使用政策來開發和改善 AWS Security Hub 和其他 AWS 安全服務。即使 Security Hub 目前未收集任何此類內容，您也可以選擇不接收。如需有關如何選擇退出的詳細資訊，請參閱《AWS Organizations 使用者指南》中的 [AI 服務選擇退出政策](#)。

Note

若要使用選擇退出政策，AWS 您的帳戶必須由 AWS Organizations 集中管理。如果您尚未為 AWS 帳戶建立組織，請參閱 AWS Organizations 《使用者指南》中的 [建立和管理組織](#)。

選擇退出具有以下影響：

- Security Hub 會在您選擇退出（如果有的話）之前，刪除其為了改善服務而收集和儲存的內容。
- 在您選擇退出後，Security Hub 將不再收集或存放此內容以用於改善服務。

下一節說明 Security Hub 如何處理您的內容以改善服務。

AWS Security Hub 資料用量

目前，AWS Security Hub 不會基於服務改進目的收集或存放任何 Security Hub 內容。不過，在未來，Security Hub 可能會收集和使用您在 Security Hub 和其他形式的 Security Hub 內容中彙總的第三

方安全調查結果 (Security Hub 為提供 Security Hub 功能而從您或上游服務收到的調查結果) , 以改善 Security Hub 和其他 AWS 安全服務功能。

您的信任、隱私權和內容的安全性是我們的最高優先順序。如果 Security Hub 在未來開始收集 Security Hub 內容以改善服務, 此頁面將更新以反映這些變更, 並提供收集哪些資料及其使用方式的詳細資訊。您可以使用上述 AWS Organizations 選擇不接收政策, 隨時選擇退出此 Security Hub 內容集合。如需 AWS 資料隱私權實務的詳細資訊, 請參閱[資料隱私權常見問答集](#)。

參考

如需其他 AWS 安全服務中的類似選擇退出程序, 請參閱:

- 《Amazon GuardDuty 使用者指南》中的[選擇不使用您的資料來改善服務](#)。
- 《Amazon Security Lake 使用者指南》中的[選擇不使用您的資料來改善服務](#)。

AWS Security Hub 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務, 可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 (登入) 和授權 (具有許可) 來使用 Security Hub 資源。IAM 是您可以免費使用 AWS 服務的。

主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [Security Hub 如何與 IAM 搭配使用](#)
- [的身分型政策範例 AWS Security Hub CSPM](#)
- [AWS Security Hub 的服務連結角色](#)
- [AWS Security Hub 的受管政策](#)
- [針對 AWS Security Hub 身分和存取進行故障診斷](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同:

- 服務使用者 — 若無法存取某些功能, 請向管理員申請所需許可 (請參閱 [針對 AWS Security Hub 身分和存取進行故障診斷](#))

- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 [Security Hub 如何與 IAM 搭配使用](#))
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 [的身分型政策範例 AWS Security Hub CSPM](#))

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的[如何登入您的 AWS 帳戶](#)。

對於程式設計存取，AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的[API 請求的AWS 第 4 版簽署程序](#)。

AWS 帳戶 根使用者

當您建立時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務和資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的[需要根使用者憑證的任務](#)。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務使用臨時憑證存取。

聯合身分是您企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務憑證存取 Directory Service。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[什麼是 IAM Identity Center ?](#)。

IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的[要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取](#)。

[IAM 群組](#)會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 使用者的使用案例](#)。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過[從使用者切換到 IAM 角色（主控台）](#)或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的快帳戶資源存取](#)。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS，會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的[JSON 政策概觀](#)。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的[在受管政策與內嵌政策之間選擇](#)。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中[指定主體](#)。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 實體許可界限](#)。
- 服務控制政策 (SCP) — 為 AWS Organizations 中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的 [服務控制政策](#)。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的 [資源控制政策 \(RCP\)](#)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的 [工作階段政策](#)。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多個政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的 [政策評估邏輯](#)。

Security Hub 如何與 IAM 搭配使用

在您使用 AWS Identity and Access Management (IAM) 管理 AWS Security Hub 的存取權之前，請先了解哪些 IAM 功能可與 Security Hub 搭配使用。

您可以搭配 AWS Security Hub 使用的 IAM 功能

IAM 功能	Security Hub 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	否
政策條件索引鍵	是
存取控制清單 (ACL)	否
屬性型存取控制 (ABAC) – 政策中的標籤	是
臨時憑證	是
轉送存取工作階段 (FAS)	是

IAM 功能	Security Hub 支援
服務角色	否
服務連結角色	是

如需 Security Hub 和其他 如何與大多數 IAM 功能 AWS 服務 搭配使用的高階檢視，請參閱 [《AWS 服務 IAM 使用者指南》](#) 中的 [與 IAM 搭配使用](#)。

Security Hub 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱 [《IAM 使用者指南》](#) 中的 [透過客戶管理政策定義自訂 IAM 許可](#)。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱 [《IAM 使用者指南》](#) 中的 [IAM JSON 政策元素參考](#)。

Security Hub 支援以身分為基礎的政策。如需詳細資訊，請參閱 [身分型政策範例 AWS Security Hub CSPM](#)。

Security Hub 的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中 [指定主體](#)。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱 [《IAM 使用者指南》](#) 中的 [IAM 中的快帳戶資源存取](#)。

Security Hub 不支援以資源為基礎的政策。您無法將 IAM 政策直接連接至 Security Hub 資源。

Security Hub 的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

Security Hub 中的政策動作在動作之前使用下列字首：

```
securityhub:
```

例如，若要授予使用者啟用 Security Hub 的許可，也就是對應至 Security Hub API EnableSecurityHubV2 操作的動作，請在其政策中包含 securityhub:EnableSecurityHubV2 動作。政策陳述式必須包含 Action 或 NotAction 元素。Security Hub 會定義自己的一組動作，描述您可以使用此服務執行的任務。

```
"Action": "securityhub:EnableSecurityHubV2"
```

若要在單一陳述式中指定多個動作，請用逗號分隔。例如：

```
"Action": [  
    "securityhub:EnableSecurityHubV2",  
    "securityhub:CreateAutomationRuleV2"
```

您也可以使用萬用字元 (*) 指定多個動作。例如，若要指定開頭是 Get 文字的所有動作，請包含以下動作：

```
"Action": "securityhub:Get*"
```

但是，根據最佳實務，您應該定義遵循「最低權限」原則的政策。換句話說，您應建立其中只包含執行特定任務所需許可的政策。

如需 Security Hub 動作的清單，請參閱《服務授權參考》中的 [AWS Security Hub 定義的動作](#)。如需指定 Security Hub 動作的政策範例，請參閱 [的身分型政策範例 AWS Security Hub CSPM](#)。

Security Hub 的政策資源

支援政策資源：否

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

```
"Resource": ""
```

Security Hub 定義下列資源類型：

- Hub (樞紐)
- 產品
- 尋找彙總工具，也稱為跨區域彙總工具
- 自動化規則

您可以使用 ARNs 在政策中指定這些類型的資源。

如需 Security Hub 資源類型和每個類型的 ARN 語法清單，請參閱《服務授權參考》中的 [AWS Security Hub 定義的資源](#)。若要了解您可以為每種資源類型指定哪些動作，請參閱《服務授權參考》中的 [AWS Security Hub 定義的動作](#)。如需指定資源的政策範例，請參閱 [的身分型政策範例 AWS Security Hub CSPM](#)。

Security Hub 的政策條件金鑰

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用[條件運算子](#)的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的[AWS 全域條件內容索引鍵](#)。

如需 Security Hub 條件金鑰的清單，請參閱《服務授權參考》中的 [AWS Security Hub 的條件金鑰](#)。若要了解您可搭配哪些動作和資源使用條件金鑰，請參閱 [AWS Security Hub 定義的動作](#)。如需使用條件索引鍵的政策範例，請參閱 [的身分型政策範例 AWS Security Hub CSPM](#)。

Security Hub 中的存取控制清單 (ACLs)

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Security Hub 不支援 ACLs，這表示您無法將 ACL 連接至 Security Hub 資源。

使用 Security Hub 的屬性型存取控制 (ABAC)

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的 [條件元素](#) 中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的 [使用 ABAC 授權定義許可](#)。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的 [使用屬性型存取控制 \(ABAC\)](#)。

您可以將標籤連接至 Security Hub 資源。您也可以政策的 Condition 元素中提供標籤資訊，以控制對資源的存取。

如需標記 Security Hub 資源的資訊，請參閱 [標記 Security Hub 資源](#)。如需根據標籤控制資源存取的身分型政策範例，請參閱 [的身分型政策範例 AWS Security Hub CSPM](#)。

搭配 Security Hub 使用臨時登入資料

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，並在您使用聯合或切換角色時自動建立。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 中的臨時安全憑證與可與 IAM 搭配運作的 AWS 服務](#)。

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫 [AssumeRole](#) 或 [GetFederationToken](#) 等 AWS STS API 操作來取得臨時安全登入資料。

Security Hub 支援使用臨時登入資料。

轉送 Security Hub 的存取工作階段

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫的委託人許可 AWS 服務，結合 AWS 服務請求向下游服務提出請求。如需提出 FAS 請求時的政策詳細資訊，請參閱 [轉發存取工作階段](#)。

例如，當您將 Security Hub 與整合 AWS 服務，AWS Organizations 以及在 Organizations 中為組織指定委派的 Security Hub 管理員帳戶時，Security Hub 會向下游發出 FAS 請求。

對於其他任務，Security Hub 會使用服務連結角色代表您執行動作。如需此角色的詳細資訊，請參閱 [AWS Security Hub 的服務連結角色](#)。

Security Hub 的服務角色

Security Hub 不會擔任或使用服務角色。若要代表您執行動作，Security Hub 會使用服務連結角色。如需此角色的詳細資訊，請參閱 [AWS Security Hub 的服務連結角色](#)。

Warning

變更服務角色的許可可能會在您使用 Security Hub 時產生操作問題。只有在 Security Hub 提供指引時，才能編輯服務角色。

Security Hub 的服務連結角色

支援服務連結角色：是

服務連結角色是連結至的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

Security Hub 使用服務連結角色代表您執行動作。如需此角色的詳細資訊，請參閱 [AWS Security Hub 的服務連結角色](#)。

的身分型政策範例 AWS Security Hub CSPM

根據預設，使用者和角色沒有建立或修改 Security Hub CSPM 資源的許可。他們也無法使用 AWS 管理主控台 AWS CLI 或 AWS API 執行任務。管理員必須建立 IAM 政策，授與使用者和角色在指定資源上執行特定 API 操作所需的許可。管理員接著必須將這些政策連接至需要這些許可的使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱 IAM 使用者指南中的 [在 JSON 索引標籤上建立政策](#)。

主題

- [政策最佳實務](#)
- [使用 Security Hub CSPM 主控台](#)
- [範例：允許使用者檢視他們自己的許可](#)

- [範例：允許使用者檢視問題清單](#)
- [範例：允許使用者建立和管理自動化規則](#)

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Security Hub 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#) 或 [任務職能的 AWS 受管政策](#)。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [透過 MFA 的安全 API 存取](#)。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 [IAM 安全最佳實務](#)。

使用 Security Hub CSPM 主控台

若要存取 AWS Security Hub CSPM 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 Security Hub CSPM 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保這些使用者和角色可以使用 Security Hub CSPM 主控台，請將下列 AWS 受管政策連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的[新增許可到使用者](#)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

範例：允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視連接到他們使用者身分的內嵌及受管政策。此政策包含在 主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",

```

```

        "iam:ListUserPolicies",
        "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
},
{
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

範例：允許使用者檢視問題清單

此範例示範如何建立 IAM 政策，允許使用者檢視 Security Hub CSPM 問題清單。

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindingsV2"
            ],
            "Resource": "*"
        }
    ]
}

```

範例：允許使用者建立和管理自動化規則

此範例示範如何建立 IAM 政策，允許使用者建立、檢視、更新和刪除 Security Hub CSPM 自動化規則。若要讓此 IAM 政策正常運作，使用者必須是 Security Hub CSPM 管理員。若要限制許可，例如，只允許使用者檢視自動化規則，您可以移除建立、更新和刪除許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAndUpdateAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:CreateAutomationRuleV2",
      ],
      "Resource": "*"
    },
    {
      "Sid": "ViewAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:ListAutomationRulesV2",
        "securityhub:GetAutomationRuleV2"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DeleteAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:DeleteAutomationRuleV2"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS Security Hub 的服務連結角色

AWS Security Hub 使用名為 `AWS Identity and Access Management (IAM)` [服務連結角色](#) `AWSServiceRoleForSecurityHubV2`。此服務連結角色是直接連結至 Security Hub 的 IAM 角色。

色。它由 Security Hub 預先定義，並包含 Security Hub 代表您呼叫其他 AWS 服務和監控 AWS 資源所需的所有許可。Security Hub 會在可使用 AWS 區域 Security Hub 的所有 中使用此服務連結角色。

服務連結角色可讓您更輕鬆地設定 Security Hub，因為您不必手動新增必要的許可。Security Hub 定義其服務連結角色的許可，除非另有定義，否則只有 Security Hub 可以擔任該角色。定義的許可包括信任政策和許可政策，您無法將該許可政策連接到任何其他 IAM 實體。

若要檢閱服務連結角色的詳細資訊，您可以使用 Security Hub 主控台。在導覽窗格中，選擇設定下的一般。然後，在服務許可區段中，選擇檢視服務許可。

只有在啟用 Security Hub 的所有區域中停用 Security Hub 之後，才能刪除 Security Hub 服務連結角色。這可保護您的 Security Hub 資源，因為您不會不小心移除存取這些資源的許可。

如需有關支援服務連結角色的其他服務的資訊，請參閱《[AWS IAM 使用者指南](#)》中的與 IAM 搭配使用的服務，並在服務連結角色欄中尋找具有是的服務。選擇有連結的是，以檢閱該服務的服務連結角色文件。

主題

- [Security Hub 的服務連結角色許可](#)
- [為 Security Hub 建立服務連結角色](#)
- [編輯 Security Hub 的服務連結角色](#)
- [刪除 Security Hub 的服務連結角色](#)

Security Hub 的服務連結角色許可

Security Hub 使用名為的服務連結角色AWSServiceRoleForSecurityHubV2。這是 AWS Security Hub 存取資源所需的服務連結角色。此服務連結角色可讓 Security Hub 執行任務，例如從其他接收問題清單，AWS 服務並設定必要的 AWS Config 基礎設施來執行控制項的安全檢查。AWSServiceRoleForSecurityHubV2 服務連結角色信任 securityhub.amazonaws.com 服務來擔任該角色。

AWSServiceRoleForSecurityHubV2 服務連結角色使用受管政策
[AWSSecurityHubServiceRolePolicy](#)。

您必須授予許可，以允許 IAM 身分（例如角色、群組或使用者）建立、編輯或刪除服務連結角色。若要成功建立AWSServiceRoleForSecurityHubV2服務連結角色，您用來存取 Security Hub 的 IAM 身分必須具有必要的許可。若要授予必要許可，請將下列政策連接至 IAM 身分。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

為 Security Hub 建立服務連結角色

AWSServiceRoleForSecurityHubV2 服務連結角色會在您第一次啟用 Security Hub 時自動建立，或在先前未啟用該角色的區域中啟用 Security Hub。您也可以使用 IAM 主控台、IAM CLI 或 IAM API 手動建立 AWSServiceRoleForSecurityHubV2 服務連結角色。如需有關手動建立角色的詳細資訊，請參閱《IAM 使用者指南》中的[建立服務連結角色](#)。

 Important

為 Security Hub 管理員帳戶建立的服務連結角色不適用於相關聯的 Security Hub 成員帳戶。

編輯 Security Hub 的服務連結角色

Security Hub 不允許您編輯 AWSServiceRoleForSecurityHubV2 服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的[編輯服務連結角色](#)。

刪除 Security Hub 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。這樣就不會有未積極監控或維護的未使用實體。

當您停用 Security Hub 時，Security Hub 不會自動為您刪除 `AWSServiceRoleForSecurityHubV2` 服務連結角色。如果您再次啟用 Security Hub，則服務可以再次開始使用現有的服務連結角色。如果您不再需要使用 Security Hub，您可以手動刪除服務連結角色。

Important

刪除 `AWSServiceRoleForSecurityHubV2` 服務連結角色之前，您必須先在啟用該角色的所有區域中停用 Security Hub。如需詳細資訊，請參閱 [停用 Security Hub](#)。如果您在嘗試刪除服務連結角色時未停用 Security Hub，刪除會失敗。

若要刪除 `AWSServiceRoleForSecurityHubV2` 服務連結角色，您可以使用 IAM 主控台、IAM CLI 或 IAM API。如需詳細資訊，請參閱《IAM 使用者指南》中的 [刪除服務連結角色](#)。

AWS Security Hub 的 受管政策

AWS 受管政策是由 AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的 [客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，更新會影響政策連接的所有主體身分（使用者、群組和角色）。AWS 服務當新的 啟動或新的 API 操作可供現有服務使用時，AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#)。

AWS 受管政策：AWSSecurityHubFullAccess

您可將 `AWSSecurityHubFullAccess` 政策連接到 IAM 身分。

此政策會授予管理許可，允許委託人完整存取所有 Security Hub 動作。此政策必須連接到委託人，才能為其帳戶手動啟用 Security Hub。例如，具有這些許可的主體可以檢視和更新調查結果的狀態。他們

也可以設定自訂洞見、啟用整合，以及啟用和停用標準和控制項。管理員帳戶的主體也可以管理成員帳戶。

許可詳細資訊

此政策包含以下許可：

- `securityhub` – 允許主體完整存取所有 Security Hub 動作。
- `guardduty` – 允許主體取得 Amazon GuardDuty 中帳戶狀態的相關資訊。
- `iam` – 允許主體為 Security Hub 建立服務連結角色。
- `inspector` – 允許主體取得 Amazon Inspector 中帳戶狀態的相關資訊。
- `pricing` – 允許主體取得 AWS 服務 和 產品的價目表。

若要檢閱此政策的許可，請參閱《AWS 受管政策參考指南[AWSSecurityHubFullAccess](#)》中的。

AWS 受管政策：AWSSecurityHubReadOnlyAccess

您可將 AWSSecurityHubReadOnlyAccess 政策連接到 IAM 身分。

此政策授予唯讀許可，允許使用者檢視 Security Hub 中的資訊。附加此政策的委託人無法在 Security Hub 中進行任何更新。例如，具有這些許可的主體可以檢視與其帳戶相關聯的問題清單，但無法變更問題清單的狀態。他們可以檢視洞見的結果，但無法建立或設定自訂洞見。他們無法設定控制項或產品整合。

許可詳細資訊

此政策包含以下許可：

- `securityhub` – 允許使用者執行傳回項目清單或項目詳細資訊的動作。這包括以 `Get`、`List` 或 開頭的 API 操作 `Describe`。

若要檢閱此政策的許可，請參閱《AWS 受管政策參考指南[AWSSecurityHubReadOnlyAccess](#)》中的。

AWS 受管政策：AWSSecurityHubOrganizationsAccess

您可將 AWSSecurityHubOrganizationsAccess 政策連接到 IAM 身分。

此政策授予管理許可，以啟用和管理 中組織的 Security Hub AWS Organizations。此政策的許可允許組織管理帳戶指定 Security Hub 的委派管理員帳戶。它們也允許委派的管理員帳戶將組織帳戶啟用為成員帳戶。

此政策僅提供 的許可 AWS Organizations。組織管理帳戶和委派管理員帳戶也需要相關聯動作的許可。您可以使用 `AWSecurityHubFullAccess` 受管政策授予這些許可。

許可詳細資訊

此政策包含以下許可：

- `organizations:ListAccounts` – 允許主體擷取屬於組織一部分的帳戶清單。
- `organizations:DescribeOrganization` – 允許主體擷取組織的相關資訊。
- `organizations:ListRoots` – 允許主體列出組織的根目錄。
- `organizations:ListDelegatedAdministrators` – 允許主體列出組織的委派管理員。
- `organizations:ListAWSServiceAccessForOrganization` – 允許主體列出 AWS 服務 組織使用的。
- `organizations:ListOrganizationalUnitsForParent` – 允許主體列出父 OU 的子組織單位 (OU)。
- `organizations:ListAccountsForParent` – 允許主體列出父 OU 的子帳戶。
- `organizations:ListParents` – 列出做為指定子 OUs 或帳戶直接父項的根或組織單位 (OU)。
- `organizations:DescribeAccount` – 允許主體擷取組織中帳戶的相關資訊。
- `organizations:DescribeOrganizationalUnit` – 允許主體擷取組織中 OU 的相關資訊。
- `organizations:ListPolicies` – 擷取組織中指定類型的所有政策清單。
- `organizations:ListPoliciesForTarget` – 列出直接連接到指定目標根目錄、組織單位 (OU) 或帳戶的政策。
- `organizations:ListTargetsForPolicy` – 列出指定政策連接的所有根目錄、組織單位 (OUs) 和帳戶。
- `organizations:EnableAWSServiceAccess` – 允許主體啟用與 Organizations 的整合。
- `organizations:RegisterDelegatedAdministrator` – 允許主體指定委派的管理員帳戶。
- `organizations:DeregisterDelegatedAdministrator` – 允許主體移除委派的管理員帳戶。
- `organizations:DescribePolicy` – 擷取政策的相關資訊。
- `organizations:DescribeEffectivePolicy` – 傳回指定政策類型和帳戶的有效政策內容。

- `organizations:CreatePolicy` – 建立可連接至根目錄、組織單位 (OU) 或個別 AWS 帳戶之指定類型的政策。
- `organizations:UpdatePolicy` – 使用新名稱、描述或內容更新現有政策。
- `organizations>DeletePolicy` – 從您的組織刪除指定的政策。
- `organizations:AttachPolicy` – 將政策連接至根帳戶、組織單位 (OU) 或個別帳戶。
- `organizations:DetachPolicy` – 從目標根目錄、組織單位 (OU) 或帳戶分離政策。
- `organizations:EnablePolicyType` – 在根目錄中啟用政策類型。
- `organizations:DisablePolicyType` – 在根目錄中停用組織政策類型。
- `organizations:TagResource` – 將一或多個標籤新增至指定的資源。
- `organizations:UntagResource` – 從指定的資源移除具有指定金鑰的任何標籤。
- `organizations:ListTagsForResource` – 列出連接至指定資源的標籤。

若要檢閱此政策的許可，請參閱《AWS 受管政策參考指南[AWS Security Hub Organizations Access](#)》中的。

AWS 受管政策：AWS Security Hub V2 Service Role Policy

此政策允許 Security Hub 代表您管理組織和的 AWS Config 規則和 Security Hub 資源。此政策會連接到服務連結角色，允許服務代表您執行動作。無法將此政策附接到 IAM 身分。如需詳細資訊，請參閱[the section called “服務連結角色”](#)。

許可詳細資訊

此政策包含以下許可：

- `access-analyzer` – 當客戶啟用或停用 Security Hub 時建立和刪除服務連結 IAM Access Analyzers、列出分析器以確認分析器狀態與啟用狀態一致，以及產生和擷取未使用的存取問題清單的政策建議。
- `cloudwatch` – 擷取指標資料以支援 Security Hub 資源的計量功能。
- `config` – 管理 Security Hub 資源的服務連結組態記錄器，包括對全域 Config 記錄器的支援。
- `ecr` – 擷取有關 Amazon Elastic Container Registry 映像和儲存庫的資訊，以支援計量功能。
- `iam` – 建立的服務連結角色 AWS Config、在客戶帳戶中建立 IAM Access Analyzer 服務連結角色、擷取帳戶資訊以支援計量功能，以及擷取現有的 IAM 政策，讓客戶可以檢視其目前政策和建議最低權限取代的比較。

- `lambda` – 擷取 AWS Lambda 函數資訊以支援計量功能。
- `organizations` – 擷取組織的帳戶和組織單位 (OU) 資訊。
- `securityhub` – 管理 Security Hub 組態。
- `tag` – 擷取資源標籤的相關資訊。

若要檢閱此政策的許可，請參閱《AWS 受管政策參考指南[AWSSecurityHubV2ServiceRolePolicy](#)》中的。

AWS 受管政策的 Security Hub 更新

下表提供有關自此服務開始追蹤 AWS 這些變更以來 Security Hub AWS 受管政策更新的詳細資訊。如需政策更新的自動提醒，請訂閱 [Security Hub 文件歷史記錄](#) 頁面上的 RSS 摘要。

變更	描述	Date
AWSSecurityHubV2ServiceRolePolicy – 更新的政策	Security Hub 已更新政策以新增 IAM Access Analyzer 許可。更新可讓 Security Hub 建立和管理服務受管分析器、列出分析器以確認分析器組態與啟用狀態一致、產生和擷取未使用的存取調查結果的政策建議，以及擷取建議顯示的 IAM 政策。	2026 年 5 月 10 日
AWSSecurityHubOrganizationsAccess – 更新的政策	Security Hub 已更新政策，新增描述資源政策以支援 Security Hub 功能的許可。Security Hub 處於預覽版本，可能會有所變更。	2025 年 11 月 12 日
AWSSecurityHubFullAccess – 更新的政策	Security Hub 已更新政策，新增有關管理 GuardDuty、Amazon Inspector 和帳戶管理的功能，以支援 Security	2025 年 11 月 17 日

變更	描述	Date
	Hub 功能。Security Hub 處於預覽版本，可能會有所變更。	
AWSSecurityHubV2ServiceRolePolicy – 更新的政策	Security Hub 已更新政策，為 Amazon Elastic Container Registry、Amazon CloudWatch AWS Lambda 和新增計量功能 AWS Identity and Access Management，以支援 Security Hub 功能。更新也新增了對全域 AWS Config 記錄器的支援。Security Hub 處於預覽版本，可能會有所變更。	2025 年 11 月 5 日
AWSSecurityHubOrganizationsAccess – 更新現有政策	Security Hub 已將新許可新增至政策。許可允許組織管理為組織啟用和管理 Security Hub 和 Security Hub CSPM。	2025 年 6 月 17 日
AWSSecurityHubFullAccess – 更新現有政策	Security Hub CSPM 新增了新的許可，允許主體為 Security Hub 建立服務連結角色。	2025 年 6 月 17 日
AWSSecurityHubV2ServiceRolePolicy – 新政策	Security Hub 新增了新的政策，以允許 Security Hub 代表客戶管理客戶組織和的 AWS Config 規則和 Security Hub 資源。Security Hub 處於預覽版本，可能會有所變更。	2025 年 6 月 17 日
AWSSecurityHubFullAccess – 更新現有政策	Security Hub CSPM 已更新政策，以取得 AWS 服務和產品的定價詳細資訊。	2024 年 4 月 24 日

變更	描述	Date
AWSSecurityHubReadOnlyAccess – 更新現有政策	Security Hub CSPM 透過新增Sid欄位來更新此受管政策。	2024 年 2 月 22 日
AWSSecurityHubFullAccess – 更新現有政策	Security Hub CSPM 已更新政策，因此可以判斷帳戶中是否啟用 Amazon GuardDuty 和 Amazon Inspector。這有助於客戶整合來自多個的安全相關資訊 AWS 服務。	2023 年 11 月 16 日
AWSSecurityHubOrganizationsAccess – 更新現有政策	Security Hub CSPM 已更新政策，授予其他許可，以允許對委派管理員功能進行 AWS Organizations 唯讀存取。這包括根目錄、組織單位 (OUs)、帳戶、組織結構和服務存取等詳細資訊。	2023 年 11 月 16 日
AWSSecurityHubOrganizationsAccess – 新政策	Security Hub CSPM 新增了一項新政策，授予 Security Hub CSPM 與 Organizations 整合所需的許可。	2021 年 3 月 15 日
Security Hub CSPM 已開始追蹤變更	Security Hub CSPM 開始追蹤其 AWS 受管政策的變更。	2021 年 3 月 15 日

針對 AWS Security Hub 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 AWS Security Hub 和 IAM 時可能遇到的常見問題。

主題

- [我無權在 Security Hub 中執行動作](#)
- [我未獲得執行 iam:PassRole 的授權](#)
- [我想要以程式設計方式存取 Security Hub](#)

- [我是管理員，想要允許其他人存取 Security Hub](#)
- [我想要允許以外的人員 AWS 帳戶 存取我的 Security Hub 資源](#)

我無權在 Security Hub 中執行動作

如果 AWS 管理主控台 通知您無權執行 動作，則必須聯絡您的管理員尋求協助。您的管理員是為您提供簽署憑證的人員。

當使用者mateojackson嘗試使用主控台檢視###的詳細資訊，但沒有securityhub:*GetWidget*許可時，會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
securityhub:GetWidget on resource: my-example-widget
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 *my-example-widget* 動作存取 securityhub:*GetWidget* 資源。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 iam:PassRole動作，您的政策必須更新，以允許您將角色傳遞至 Security Hub。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM marymajor 使用者嘗試使用主控台在 Security Hub 中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要以程式設計方式存取 Security Hub

如果使用者想要與 AWS 外部互動，則需要程式設計存取 AWS 管理主控台。授予程式設計存取權的方式取決於正在存取的使用者類型 AWS。

若要授予使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	根據
IAM	(建議) 使用主控台登入資料做為臨時登入資料，以簽署對 AWS CLI、AWS SDKs 程式設計請求。AWS APIs	請依照您要使用的介面所提供的指示操作。 - 如需 AWS CLI，請參閱 AWS Command Line Interface 《使用者指南》中的登入以進行 AWS 本機開發。 - AWS SDKs 請參閱 AWS SDKs 和工具參考指南中的登入以進行 AWS 本機開發。
人力資源身分 (IAM Identity Center 中管理的使用者)	使用暫時登入資料簽署對 AWS CLI、AWS SDKs 程式設計請求。AWS APIs	請依照您要使用的介面所提供的指示操作。 - 如需 AWS CLI，請參閱 AWS Command Line Interface 《使用者指南》中的設定 AWS CLI 要使用 AWS IAM Identity Center的。 - AWS SDKs、工具和 AWS APIs，請參閱 AWS SDK 和工具參考指南中的 SDKs IAM Identity Center 身分驗證。
IAM	使用暫時登入資料簽署對 AWS CLI、AWS SDKs 程式設計請求。AWS APIs	遵循《IAM 使用者指南》中將臨時登入資料與 AWS 資源搭配使用的指示。
IAM	(不建議使用) 使用長期憑證簽署對 AWS CLI、AWS SDKs 程式設計請求。AWS APIs	請依照您要使用的介面所提供的指示操作。 如需 AWS CLI，請參閱 AWS Command Line Interface

哪個使用者需要程式設計存取權？	到	根據
		《使用者指南》中的使用 IAM 使用者憑證進行身分驗證。 • AWS SDKs和工具，請參閱 AWS SDKs和工具參考指南中的使用長期憑證進行身分驗證。 • 對於 AWS APIs，請參閱《IAM 使用者指南》中的管理 IAM 使用者的存取金鑰。

我是管理員，想要允許其他人存取 Security Hub

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 中的使用者和群組 AWS IAM Identity Center：

建立權限合集。請按照《AWS IAM Identity Center 使用者指南》中的[建立權限合集](#)說明進行操作。

- 透過身分提供者在 IAM 中管理的使用者：

建立聯合身分的角色。遵循《IAM 使用者指南》的[為第三方身分提供者 \(聯合\) 建立角色](#)中的指示。

- IAM 使用者：
 - 建立您的使用者可擔任的角色。請按照《IAM 使用者指南》的[為 IAM 使用者建立角色](#)中的指示。
 - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循《IAM 使用者指南》的[新增許可到使用者 \(主控台\)](#)中的指示。

我想要允許 以外的人員 AWS 帳戶 存取我的 Security Hub 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Security Hub 是否支援這些功能，請參閱 [Security Hub 如何與 IAM 搭配使用](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《IAM 使用者指南》中的 [在您擁有 AWS 帳戶 的另一個 中提供存取權給](#) IAM 使用者。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的 [將存取權提供給第三方 AWS 帳戶 擁有](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的 [將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 [IAM 中的跨帳戶資源存取](#)。

AWS Security Hub 的合規驗證

若要了解 AWS 服務 是否在特定合規計劃範圍內，請參閱[AWS 服務 合規計劃範圍內](#)然後選擇您感興趣的合規計劃。如需一般資訊，請參閱[AWS 合規計劃](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱[下載報告 in AWS Artifact](#)

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 [AWS 安全文件](#)。

AWS Security Hub 中的彈性

AWS 全球基礎設施是以 AWS 區域 和可用區域為基礎建置。區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

AWS Security Hub 中的基礎設施安全性

作為受管服務，AWS Security Hub 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全的最佳實務設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的 [基礎設施保護](#)。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 Security Hub。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。

- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

AWS Security Hub 和介面 VPC 端點 (AWS PrivateLink)

您可以建立介面 VPC 端點，在 VPC 和 AWS Security Hub 之間建立私有連線。介面端點採用 [AWS PrivateLink](#) 技術，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連接或 AWS Direct Connect 連接的情況下私下存取 Security Hub APIs。VPC 中的執行個體不需要公有 IP 地址，即可與 Security Hub APIs 通訊。VPC 和 Security Hub 之間的流量不會離開 Amazon 網路。

每個介面端點都是由您子網路中的一或多個[彈性網路介面](#)表示。如需詳細資訊，請參閱 [《Amazon Virtual Private Cloud 指南》](#) 中的 [AWS 服務 使用介面 VPC 端點存取](#)。Amazon Virtual Private Cloud

Security Hub VPC 端點的考量事項

設定 Security Hub 的介面 VPC 端點之前，請務必檢閱 [Amazon Virtual Private Cloud 指南](#) 中的先決條件和其他資訊。

Security Hub 支援從您的 VPC 呼叫其所有 API 動作。

建立 Security Hub 的介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 為 Security Hub 服務建立 VPC 端點。如需詳細資訊，請參閱 [《Amazon Virtual Private Cloud 指南》](#) 中的 [建立 VPC 端點](#)。

使用下列服務名稱建立 Security Hub 的 VPC 端點：

`com.amazonaws.region.securityhub`

其中 *region* 是適用的區域代碼 AWS 區域。

如果您為端點啟用私有 DNS，則可以使用區域的預設 DNS 名稱向 Security Hub 提出 API 請求，例如，美國東部 `securityhub.us-east-1.amazonaws.com`（維吉尼亞北部）區域。

為 Security Hub 建立 VPC 端點政策

您可以將端點政策連接至控制 Security Hub 存取的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《Amazon Virtual Private Cloud 指南》中的[使用端點政策控制對 VPC 端點的存取](#)。

範例：Security Hub 動作的 VPC 端點政策

以下是 Security Hub 的端點政策範例。連接到端點時，此政策會授予所有資源上所有委託人的所列 Security Hub 動作的存取權。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "securityhub:getFindings",
        "securityhub:getEnabledStandards",
        "securityhub:getInsights"
      ],
      "Resource": "*"
    }
  ]
}
```

共用子網路

無法在與您共用的子網路中建立、描述、修改或刪除 VPC 端點。不過，可以在與您共用的子網路中使用 VPC 端點。如需 VPC 共用的相關資訊，請參閱《Amazon Virtual Private Cloud 指南》中的[與其他帳戶共用 VPC 子網路](#)。

使用 CloudTrail 記錄 Security Hub API 呼叫

已與服務整合 AWS CloudTrail，此服務提供由使用者、角色或 Security Hub 中的 AWS 服務所採取之動作的記錄。CloudTrail 會將 Security Hub 的 API 呼叫擷取為事件。擷取的呼叫包括來自 Security Hub 主控台的呼叫，以及對 Security Hub API 操作的程式碼呼叫。如果您建立線索，您可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Security Hub 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台內的 Event history (事件歷史記錄) 檢視最新事件。您可以使用 CloudTrail 收集的資訊，判斷向 Security Hub 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，包括如何設定及啟用，請參閱 [《AWS CloudTrail 使用者指南》](#)。

CloudTrail 中的 Security Hub 資訊

當您建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當 Security Hub 中發生支援的事件活動時，該活動會與事件歷史記錄中的其他 AWS 服務事件一起記錄在 CloudTrail 事件中。您可以檢視、搜尋和下載 帳戶的最新事件。如需詳細資訊，請參閱[使用 CloudTrail 事件歷史記錄檢視事件](#)。

若要不持續記錄您帳戶中的事件，包括 Security Hub 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，在主控台建立線索時，該線索會套用到所有 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [接收多個區域的 CloudTrail 日誌檔案](#)和[接收多個帳戶的 CloudTrail 日誌檔案](#)

Security Hub 支援將所有 Security Hub API 動作記錄為 CloudTrail 日誌中的事件。若要檢視 Security Hub 操作的清單，請參閱[Security Hub API 參考](#)。

將下列動作的活動記錄到 CloudTrail 時，`responseElements` 會設為 null。這可確保敏感資訊不包含在 CloudTrail 日誌中。

- `GetFindingsV2`

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求
- 提出該請求時，是否使用了特定角色或聯合身分使用者的臨時安全憑證
- 請求是否由其他 AWS 服務提出

如需詳細資訊，請參閱[CloudTrail userIdentity 元素](#)。

範例：Security Hub 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時

間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例顯示的是展示 CreateAutomationRuleV2 動作的 CloudTrail 日誌項目。在此範例中，TestAutomationRule 會建立名為 的自動化規則。Severity 和 Account ID 屬性指定為條件。當規則相符時，Severity 會更新為高。如需自動化規則的詳細資訊，請參閱 [Security Hub 中的自動化規則](#)。

```
{
  "eventVersion": "1.09",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI23456789EXAMPLE:Admin",
    "arn": "arn:aws:sts::555555555555:assumed-role/Admin",
    "accountId": "555555555555",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI23456789EXAMPLE",
        "arn": "aarn:aws:iam::555555555555:role/Admin",
        "accountId": "555555555555",
        "userName": "Admin"
      },
      "attributes": {
        "creationDate": "2025-11-15T18:49:13Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2025-11-15T18:51:17Z",
  "eventSource": "securityhub.amazonaws.com",
  "eventName": "CreateAutomationRuleV2",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "205.251.233.50",
  "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
  "requestParameters": {
    "Description": "Test Automation Rule",
    "Actions": [
      {
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "SeverityId": 4
        }
      }
    ]
  }
}
```

```

        }
      }
    ],
    "RuleStatus": "ENABLED",
    "Criteria": {
      "OcsfFindingCriteria": {
        "CompositeFilters": [
          {
            "Operator": "OR",
            "StringFilters": [
              {
                "FieldName": "severity",
                "Filter": {
                  "Value": "Medium",
                  "Comparison": "EQUALS"
                }
              }
            ]
          },
          {
            "Operator": "OR",
            "StringFilters": [
              {
                "FieldName": "cloud.account.uid",
                "Filter": {
                  "Value": "111122223333",
                  "Comparison": "EQUALS"
                }
              }
            ]
          }
        ]
      },
      "CompositeOperator": "AND"
    }
  },
  "ClientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
  "RuleOrder": 61,
  "RuleName": "TestAutomationRule",
  "Tags": {}
},
"responseElements": {
  "RuleArn": "arn:aws:securityhub:us-west-2:555555555555:automation-rulev2/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "RuleId": "c8bc6f90-29e9-4eb7-919f-b145e44eb8ec"
}

```



```
},  
"requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",  
"eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",  
"readOnly": false,  
"eventType": "AwsApiCall",  
"managementEvent": true,  
"recipientAccountId": "555555555555",  
"eventCategory": "Management"  
}
```

AWS Security Hub CSPM 簡介

AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) 可讓您全面檢視中的安全狀態，AWS 並協助您根據安全產業標準和最佳實務評估 AWS 環境。

AWS Security Hub CSPM 會跨 AWS 帳戶和支援的第三方產品收集安全資料 AWS 服務，並協助您分析安全趨勢並識別最高優先順序的安全問題。

為了協助您管理組織的安全狀態，Security Hub CSPM 支援多個安全標準。其中包括 制定 AWS 的基礎安全最佳實務 (FSBP) 標準 AWS，以及外部合規架構，例如網際網路安全中心 (CIS)、支付卡產業資料安全標準 (PCI DSS) 和國家標準技術研究所 (NIST)。每個標準都包含數個安全控制，每個都代表安全最佳實務。Security Hub CSPM 會針對安全控制執行檢查，並產生控制調查結果，協助您根據安全最佳實務評估合規性。

除了產生控制調查結果之外，Security Hub CSPM 也會接收其他 的調查結果 AWS 服務，例如 Amazon GuardDuty、Amazon Inspector 和 Amazon Macie，以及支援的第三方產品。這可讓您將單一窗格放入各種與安全相關的問題中。您也可以將 Security Hub CSPM 調查結果傳送至其他 AWS 服務和支援的第三方產品。

Security Hub CSPM 提供自動化功能，可協助您分類和修復安全問題。例如，您可以使用自動化規則，在安全檢查失敗時自動更新關鍵問題清單。您也可以利用與 Amazon EventBridge 的整合來觸發對特定調查結果的自動回應。

主題

- [Security Hub CSPM 的優點](#)
- [存取 Security Hub CSPM](#)
- [相關服務](#)
- [Security Hub CSPM 免費試用和定價](#)
- [Security Hub CSPM 中的概念和術語](#)
- [啟用 Security Hub CSPM](#)
- [在 Security Hub CSPM 中管理管理員和成員帳戶](#)
- [了解 Security Hub CSPM 中的跨區域彙總](#)
- [了解 Security Hub CSPM 中的安全標準](#)
- [了解 Security Hub CSPM 中的安全控制](#)
- [了解 Security Hub CSPM 中的整合](#)

- [在 Security Hub CSPM 中建立和更新問題清單](#)
- [在 Security Hub CSPM 中檢視洞見](#)
- [自動修改 Security Hub CSPM 中的調查結果並對其採取行動](#)
- [在 Security Hub CSPM 中使用儀表板](#)
- [Security Hub CSPM 的區域限制](#)
- [使用 CloudFormation 建立 Security Hub CSPM 資源](#)
- [使用 Amazon SNS 訂閱 Security Hub CSPM 公告](#)
- [停用 Security Hub CSPM](#)
- [中的安全性 AWS Security Hub CSPM](#)
- [使用 CloudTrail 記錄 Security Hub API 呼叫](#)

Security Hub CSPM 的優點

以下是 Security Hub CSPM 協助您監控整個 AWS 環境合規性和安全性狀態的一些重要方式。

可讓您更輕易地收集和排列問題清單的優先順序

Security Hub CSPM 可減少從整合和 AWS 合作夥伴產品收集 AWS 服務 和排定跨帳戶安全調查結果優先順序的精力。Security Hub CSPM 會使用標準調查結果格式 AWS (ASFF) 來處理調查結果資料。這樣就不需要以多種格式管理來自不同來源的問題清單。Security Hub CSPM 也會跨提供者關聯問題清單，以協助您排定最重要的問題清單。

根據最佳實務和標準自動進行安全檢查

Security Hub CSPM 會根據 AWS 最佳實務和業界標準，自動執行持續的帳戶層級組態和安全檢查。Security Hub CSPM 使用這些檢查的結果來計算安全分數，並識別需要注意的特定帳戶和資源。

合併帳戶與提供者問題清單的檢視

Security Hub CSPM 會整合您跨帳戶和提供者產品的安全性調查結果，並在 Security Hub CSPM 主控台上顯示結果。您也可以透過 Security Hub CSPM API AWS CLI 或 SDKs 擷取問題清單。透過對目前安全狀態的全面檢視，您可以發現趨勢、識別潛在問題，並採取必要的修補步驟。

能夠自動化問題清單更新和修復

您可以建立自動化規則，以根據您的定義條件修改或隱藏問題清單。Security Hub CSPM 也支援與 Amazon EventBridge 整合。若要自動修復特定問題清單，您可以定義產生問題清單時要採取的自訂動作。例如，您可以設定自訂動作，將問題清單傳送到售票系統或自動化修補系統。

存取 Security Hub CSPM

Security Hub CSPM 適用於大多數 AWS 區域。如需目前可使用 Security Hub CSPM 的區域清單，請參閱《》中的 [AWS Security Hub CSPM 端點和配額](#) AWS 一般參考。如需有關管理 AWS 區域 的資訊 AWS 帳戶，請參閱《AWS 帳戶管理 參考指南》中的 [指定 AWS 區域 您的帳戶可以使用哪些](#)。

在每個區域中，您可以透過下列任何方式存取和使用 Security Hub CSPM：

Security Hub CSPM 主控台

AWS 管理主控台 是以瀏覽器為基礎的界面，可用來建立和管理 AWS 資源。作為該主控台的一部分，Security Hub CSPM 主控台可讓您存取 Security Hub CSPM 帳戶、資料和資源。您可以使用 Security Hub CSPM 主控台來執行 Security Hub CSPM 任務：檢視問題清單、建立自動化規則、建立彙總區域等。

Security Hub CSPM API

Security Hub CSPM API 可讓您以程式設計方式存取 Security Hub CSPM 帳戶、資料和資源。使用 API，您可以將 HTTPS 請求直接傳送到 Security Hub CSPM。如需 API 的相關資訊，請參閱 [AWS Security Hub API 參考](#)。

AWS CLI

使用 AWS CLI，您可以在系統的命令列執行命令，以執行 Security Hub CSPM 任務。在某些情況下，使用命令列比使用主控台更快、更方便。如果您想要建置執行任務的指令碼，命令列也很有用。如需安裝和使用的詳細資訊 AWS CLI，請參閱 [AWS Command Line Interface 《使用者指南》](#)。

AWS SDKs

AWS 提供 SDKs，其中包含適用於各種程式設計語言和平台的程式庫和範本程式碼，例如 Java、Go、Python、C++ 和 .NET。SDKs 以您偏好的語言提供對 Security Hub CSPM 和其他 AWS 服務的便利、程式設計存取。它們也會處理諸如密碼編譯簽署請求、管理錯誤和自動重試請求等任務。如需有關安裝和使用 AWS SDKs 的資訊，請參閱 [要建置的工具 AWS](#)。

Important

Security Hub CSPM 只會偵測和合併啟用 Security Hub CSPM 後產生的問題清單。它不會追溯偵測和合併在您啟用 Security Hub CSPM 之前產生的安全調查結果。

Security Hub CSPM 只會在您帳戶中啟用 Security Hub CSPM 的區域中接收和處理問題清單。

若要完全符合 CIS AWS Foundations Benchmark 安全檢查，您必須在所有支援 AWS 的區域啟用 Security Hub CSPM。

相關服務

若要進一步保護您的 AWS 環境，請考慮使用其他 AWS 服務 搭配 Security Hub CSPM。有些 AWS 服務 會將問題清單傳送至 Security Hub CSPM，而 Security Hub CSPM 會將問題清單標準化為標準格式。有些 AWS 服務 也可以從 Security Hub CSPM 接收問題清單。

如需傳送或接收 Security Hub CSPM 調查結果 AWS 服務 的其他 清單，請參閱 [AWS 服務 與 Security Hub CSPM 整合](#)。

Security Hub CSPM 使用來自 的服務連結規則 AWS Config 來執行大多數控制項的安全檢查。控制項是指特定 AWS 服務 和資源。如需 Security Hub CSPM 控制項的清單，請參閱 [Security Hub CSPM 的控制項參考](#)。您必須在 AWS Config Security Hub CSPM 的 中啟用 AWS Config 並記錄資源，以產生大多數的控制問題清單。如需詳細資訊，請參閱[啟用和設定 之前的考量事項 AWS Config](#)。

Security Hub CSPM 免費試用和定價

當您 AWS 帳戶 第一次在 中啟用 Security Hub CSPM 時，該帳戶會自動註冊 30 天的 Security Hub CSPM 免費試用。

當您在免費試用期間使用 Security Hub CSPM 時，您需要支付使用 Security Hub CSPM 互動的其他服務的費用，例如 AWS Config 項目。對於僅由 Security Hub CSPM 安全標準啟用的 AWS Config 規則，您不需要付費。

在免費試用結束之前，您無需支付使用 Security Hub CSPM 的費用。

檢視用量詳細資訊

Security Hub CSPM 提供用量資訊，包括您帳戶處理的安全性檢查和調查結果數量。用量詳細資訊也包含免費試用的剩餘時間。此資訊可協助您了解免費試用結束後的 Security Hub CSPM 用量。免費試用結束後，也會提供用量資訊。

顯示用量資訊（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。

2. 在導覽窗格中，選擇設定下的用量。

用量資訊僅適用於目前帳戶和目前區域。在彙總區域中，用量資訊不包含連結的區域。如需連結區域的詳細資訊，請參閱 [the section called “彙總的資料類型”](#)。

若要檢視您帳戶的成本詳細資訊，請使用 [AWS 帳單主控台](#)。

定價詳情

如需 Security Hub CSPM 如何針對擷取的問題清單和安全檢查收費的詳細資訊，請參閱 [Security Hub CSPM 定價](#)。

Security Hub CSPM 中的概念和術語

在 AWS Security Hub CSPM 中，我們以常見的 AWS 概念和術語為基礎，並使用這些額外的術語。

帳戶

包含 AWS 資源的標準 Amazon Web Services (AWS) 帳戶。您可以使用 AWS 帳戶登入，並啟用 Security Hub CSPM。

帳戶可以邀請其他帳戶啟用 Security Hub CSPM，並在 Security Hub CSPM 中與該帳戶建立關聯。接受成員邀請為選擇性。如果接受邀請，帳戶會成為管理員帳戶，而新增的帳戶是成員帳戶。管理員帳戶可以檢視其成員帳戶中的問題清單。

如果您已註冊 AWS Organizations，則組織會為組織指定 Security Hub CSPM 管理員帳戶。Security Hub CSPM 管理員帳戶可以將其他組織帳戶啟用為成員帳戶。

帳戶不能同時是管理員帳戶和成員帳戶。帳戶只能有一個管理員帳戶。

如需詳細資訊，請參閱 [在 Security Hub CSPM 中管理管理員和成員帳戶](#)。

管理員帳戶

Security Hub CSPM 中的帳戶，有權檢視相關聯成員帳戶的問題清單。

帳戶會以下列其中一種方式成為管理員帳戶：

- 帳戶會邀請其他帳戶在 Security Hub CSPM 中與其建立關聯。當這些帳戶接受邀請時，他們將成為成員帳戶，邀請帳戶將成為其管理員帳戶。

- 帳戶由組織管理帳戶指定為 Security Hub CSPM 管理員帳戶。Security Hub CSPM 管理員帳戶可以將任何組織帳戶啟用為成員帳戶，也可以邀請其他帳戶成為成員帳戶。

帳戶只能有一個管理員帳戶。帳戶不能同時是管理員帳戶和成員帳戶。

彙總區域

設定彙總區域可讓您在 AWS 區域 單一玻璃窗格中檢視來自多個的安全調查結果。

彙總區域是您檢視和管理問題清單的區域。調查結果會從連結的區域彙總到彙總區域。問題清單的更新會跨區域複寫。

在彙總區域中，安全標準、洞見和調查結果頁面包含來自所有連結區域的資料。

如需詳細資訊，請參閱[the section called “跨區域彙總資料”](#)。

存檔的問題清單

記錄狀態 (RecordState) 為 的調查結果ARCHIVED。封存問題清單表示問題清單提供者認為問題清單不再相關。記錄狀態與工作流程狀態不同，工作流程狀態會追蹤調查結果的調查狀態。

問題清單提供者可以使用 Security Hub CSPM API [BatchImportFindings](#)的操作來封存他們建立的問題清單。Security Hub CSPM 會自動封存符合特定條件的控制調查結果。如需詳細資訊，請參閱[產生、更新和封存控制問題清單](#)。

在 Security Hub CSPM 主控台上，預設篩選條件設定會從問題清單和資料表中排除封存的問題清單。您可以更新設定以包含封存的問題清單。如果您使用 Security Hub CSPM API [GetFindings](#)的操作來擷取問題清單，則該操作會同時擷取封存和作用中的問題清單。若要排除封存的問題清單，您可以篩選結果。例如：

```
"RecordState": [
  {
    "Comparison": "EQUALS",
    "Value": "ARCHIVED"
  }
],
```

AWS 安全調查結果格式 (ASFF)

Security Hub CSPM 彙總或產生之問題清單內容的標準化格式。AWS 安全調查結果格式可讓您使用 Security Hub CSPM 檢視和分析 AWS 由安全服務、第三方解決方案或 Security Hub CSPM 本身從執行安全檢查所產生的調查結果。如需詳細資訊，請參閱[AWS 安全調查結果格式 \(ASFF\)](#)。

控制項

為資訊系統或組織規定的一種保護或應對措施，旨在保護其資訊的機密性、完整性和可用性，並符合一組定義的安全需求。安全標準與控制項集合相關聯。

安全控制一詞是指跨標準具有單一控制項 ID 和標題的控制項。標準控制項一詞是指具有標準特定控制項 IDs 和標題的控制項。目前，Security Hub CSPM 僅支援中國區域和 的標準控制項 AWS GovCloud (US) Regions。所有其他 區域都支援安全控制。

自訂動作

用於將所選問題清單傳送至 EventBridge 的 Security Hub CSPM 機制。自訂動作是在 Security Hub CSPM 中建立。然後，它會連結到 EventBridge 規則。規則會定義一個要在接收到與自訂動作 ID 建立關聯的問題清單時，所要採取的特定動作。例如，您可以使用自訂動作來將特定問題清單，或是一小組問題清單傳送至回應或修補工作流程。如需詳細資訊，請參閱[the section called “建立自訂動作”](#)。

委派管理員帳戶（組織）

在 中 AWS Organizations，服務的委派管理員帳戶可以管理組織的服務使用。

在 Security Hub CSPM 中，Security Hub CSPM 管理員帳戶也是 Security Hub CSPM 的委派管理員帳戶。當組織管理帳戶首次指定 Security Hub CSPM 管理員帳戶時，Security Hub CSPM 會呼叫 Organizations 將該帳戶設為委派管理員帳戶。

組織管理帳戶接著必須選擇委派管理員帳戶作為所有區域中的 Security Hub CSPM 管理員帳戶。

問題清單

安全檢查或安全性相關偵測的可觀察記錄。Security Hub CSPM 會在完成控制項的安全檢查後產生和更新問題清單。這些稱為控制調查結果。問題清單也可以來自與其他 AWS 服務 和第三方產品的整合。

如需詳細資訊，請參閱[the section called “調查結果”](#)。

跨區域彙總

問題清單、洞見、控制合規狀態和安全分數從連結區域彙總到彙總區域。然後，您可以從彙總區域檢視所有資料，並從彙總區域更新調查結果和洞見。

如需詳細資訊，請參閱[the section called “跨區域彙總資料”](#)。

尋找擷取

從其他 AWS 服務和第三方合作夥伴提供者將問題清單匯入 Security Hub CSPM。

調查結果擷取事件包括新調查結果和現有調查結果的更新。

Insight

彙總陳述式和選用篩選條件定義的相關問題清單集合。洞見可識別需要注意和介入的安全區域。Security Hub CSPM 提供數個您無法修改的受管（預設）洞見。您也可以建立自訂 Security Hub CSPM 洞見，以追蹤您 AWS 環境和用量特有的安全問題。如需詳細資訊，請參閱[the section called “洞見”](#)。

連結的區域

當您啟用跨區域彙總時，連結的區域是將問題清單、洞見、控制合規狀態和安全分數彙總至彙總區域的區域。

在連結的區域中，調查結果和洞見頁面僅包含該區域的調查結果。

如需詳細資訊，請參閱[the section called “跨區域彙總資料”](#)。

成員帳戶

已授予管理員帳戶檢視其問題清單並對其採取動作之許可的帳戶。

帳戶會以下列其中一種方式成為成員帳戶：

- 帳戶接受來自另一個帳戶的邀請。
- 對於組織帳戶，Security Hub CSPM 管理員帳戶會將帳戶啟用為成員帳戶。

相關要求

映射到控制的一組產業或法規要求。

規則

用於評定是否有遵守控制的一組自動化條件。規則受到評估時，可能會通過或失敗。如果評估無法判斷規則通過或失敗，則規則會處於警告狀態。如果無法評估規則，則規則會處於不可用狀態。

安全檢查

針對單一資源對規則的特定point-in-time評估，導致 PASSED、WARNING、FAILED 或 NOT_AVAILABLE 狀態。執行安全檢查會產生問題清單。

Security Hub CSPM 管理員帳戶

管理組織 Security Hub CSPM 成員資格的組織帳戶。

組織管理帳戶會指定每個區域中的 Security Hub CSPM 管理員帳戶。組織管理帳戶必須在所有區域中選擇相同的 Security Hub CSPM 管理員帳戶。

Security Hub CSPM 管理員帳戶也是 Organizations 中 Security Hub CSPM 的委派管理員帳戶。

Security Hub CSPM 管理員帳戶可以將任何組織帳戶啟用為成員帳戶。Security Hub CSPM 管理員帳戶也可以邀請其他帳戶成為成員帳戶。

安全標準

針對指定特性主題發佈的陳述式，通常可測量且為控制項形式，必須予以滿足或加以存檔以確保合規性。安全標準可以是以法規框架、最佳實務或內部公司政策為基礎。控制項可能與 Security Hub CSPM 中的一或多個支援的標準相關聯。若要進一步了解 Security Hub CSPM 中的安全標準，請參閱 [了解 Security Hub CSPM 中的安全標準](#)。

嚴重性

指派給 Security Hub CSPM 控制項的嚴重性可識別控制項的重要性。控制項的嚴重性可以是「關鍵」、「高」、「中」、「低」或「資訊」。指派給控制調查結果的嚴重性等於控制本身的嚴重性。若要了解 Security Hub CSPM 如何將嚴重性指派給控制項，請參閱 [控制問題清單的嚴重性等級](#)。

工作流程狀態

調查問題清單的狀態。這是使用 Workflow.Status 屬性進行追蹤。

最初的工作流程狀態為 NEW。如果您通知資源擁有者對搜尋結果採取動作，您可以將工作流程狀態設定為 NOTIFIED。如果搜尋結果不是問題，且不需要任何動作，請將工作流程狀態設定為 SUPPRESSED。檢閱並修正尋找項目後，請將工作流程狀態設定為 RESOLVED。

依預設，大多數的搜尋結果清單只包含工作流程狀態為 NEW 或 NOTIFIED 的搜尋結果。控制的問題清單也會包含在 RESOLVED 的問題清單中。

對於 [GetFindings](#) 操作，您可以包含工作流程狀態的篩選條件。

```
"WorkflowStatus": [
  {
    "Comparison": "EQUALS",
    "Value": "RESOLVED"
  }
],
```

Security Hub CSPM 主控台提供設定問題清單工作流程狀態的選項。客戶 (或 SIEM、票證、事件管理或 SOAR 工具代表客戶更新來自問題清單提供者的問題清單) 也可以用 [BatchUpdateFindings](#) 來更新工作流程狀態。

啟用 Security Hub CSPM

有兩種方式可整合 AWS Organizations 或 手動啟用 AWS Security Hub CSPM。

強烈建議在多帳戶和多區域環境中與 Organizations 整合。如果您有獨立帳戶，則必須手動設定 Security Hub CSPM。

驗證必要的許可

註冊 Amazon Web Services (AWS) 之後，您必須啟用 Security Hub CSPM 才能使用其功能。若要啟用 Security Hub CSPM，您必須先設定允許您存取 Security Hub CSPM 主控台和 API 操作的許可。您或您的 AWS 管理員可以使用 AWS Identity and Access Management (IAM) 將名為 `AWSSecurityHubFullAccess` 的 AWS 受管政策連接到您的 IAM 身分，以執行此操作。

若要透過 Organizations 整合啟用和管理 Security Hub CSPM，您也應該連接名為 `AWSSecurityHubOrganizationsAccess` 的 AWS 受管政策。

如需詳細資訊，請參閱[AWS Security Hub 的 受管政策](#)。

啟用 Security Hub CSPM 與 Organizations 整合

若要開始搭配 Security Hub CSPM 使用 AWS Organizations，組織的 AWS Organizations 管理帳戶會將帳戶指定為組織的委派 Security Hub CSPM 管理員帳戶。Security Hub CSPM 會在目前區域中的委派管理員帳戶中自動啟用。

選擇您偏好的方法，然後依照步驟指定委派管理員。

Security Hub CSPM console

在加入時指定委派的 Security Hub CSPM 管理員

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 選擇移至 Security Hub CSPM。系統會提示您登入 Organizations 管理帳戶。
3. 在指定委派管理員頁面上的委派管理員帳戶區段中，指定委派管理員帳戶。我們建議您選擇已為其他 AWS 安全與合規服務設定的相同委派管理員。

4. 選擇設定委派管理員。

Security Hub CSPM API

從 Organizations 管理帳戶叫用 [EnableOrganizationAdminAccount](#) API。提供 Security Hub CSPM 委派管理員帳戶的 AWS 帳戶 ID。

AWS CLI

從 Organizations 管理帳戶執行 [enable-organization-admin-account](#) 命令。提供 Security Hub CSPM 委派管理員帳戶的 AWS 帳戶 ID。

範例命令：

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

如需與 Organizations 整合的詳細資訊，請參閱 [將 Security Hub CSPM 與 整合 AWS Organizations](#)。

中央組態

當您整合 Security Hub CSPM 和 Organizations 時，您可以選擇使用稱為[中央組態](#)的功能，為您的組織設定和管理 Security Hub CSPM。我們強烈建議使用中央組態，因為它可讓管理員自訂組織的安全涵蓋範圍。在適當情況下，委派管理員可以允許成員帳戶設定自己的安全涵蓋範圍設定。

中央組態可讓委派管理員跨帳戶、OUs 和 設定 Security Hub CSPM AWS 區域。委派管理員透過建立組態政策來設定 Security Hub CSPM。在組態政策中，您可以指定下列設定：

- Security Hub CSPM 是否啟用或停用
- 啟用和停用哪些安全標準
- 啟用和停用哪些安全控制
- 是否自訂特定控制項的參數

身為委派管理員，您可以為整個組織建立單一組態政策，或為各種帳戶和 OUs 建立不同的組態政策。例如，測試帳戶和生產帳戶可以使用不同的組態政策。

使用組態政策的成員帳戶和 OUs 是集中管理的，只能由委派管理員設定。委派管理員可以將特定成員帳戶和 OUs 指定為自我管理，讓成員能夠 Region-by-Region 自己的設定。

如果您不使用中央組態，則必須在每個帳戶和區域中分別設定 Security Hub CSPM。這稱為[本機組態](#)。在本機組態下，委派管理員可以在目前區域中的新組織帳戶中自動啟用 Security Hub CSPM 和一組有限的安全標準。本機組態不適用於現有的組織帳戶或目前區域以外的區域。本機組態也不支援使用組態政策。

手動啟用 Security Hub CSPM

如果您有獨立帳戶或未與整合，則必須手動啟用 Security Hub CSPM AWS Organizations。獨立帳戶無法與整合 AWS Organizations，且必須使用手動啟用。

當您手動啟用 Security Hub CSPM 時，您可以指定 Security Hub CSPM 管理員帳戶，並邀請其他帳戶成為成員帳戶。當潛在成員帳戶接受邀請時，會建立管理員成員關係。

選擇您偏好的方法，並依照步驟啟用 Security Hub CSPM。當您從主控台啟用 Security Hub CSPM 時，您也可以選擇啟用支援的安全標準。

Security Hub CSPM console

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 當您第一次開啟 Security Hub CSPM 主控台時，請選擇移至 Security Hub CSPM。
3. 在歡迎頁面上，安全標準區段列出 Security Hub CSPM 支援的安全標準。

選取標準的核取方塊以啟用它，然後清除核取方塊以停用它。

您可以隨時啟用或停用標準，或是其個別的控制項。如需管理安全標準的資訊，請參閱[了解 Security Hub CSPM 中的安全標準](#)。

4. 選擇 Enable Security Hub (啟用 Security Hub)。

Security Hub CSPM API

叫用 [EnableSecurityHub](#) API。當您從 API 啟用 Security Hub CSPM 時，它會自動啟用下列預設安全標準：

- AWS 基礎安全最佳實務
- Center for Internet Security (CIS) AWS Foundations Benchmark 1.2.0 版

如果您不希望啟用這些標準，請將 `EnableDefaultStandards` 設為 `false`。

您也可以使用 Tags 參數將標籤值指派給中樞資源。

AWS CLI

執行 [enable-security-hub](#) 命令。若要啟用預設標準，請包含 `--enable-default-standards`。若要不啟用預設標準，請包含 `--no-enable-default-standards`。預設安全標準如下：

- AWS 基礎安全最佳實務
- Center for Internet Security (CIS) AWS Foundations Benchmark 1.2.0 版

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-standards | --no-enable-default-standards]
```

範例

```
aws securityhub enable-security-hub --enable-default-standards --tags '{"Department": "Security"}'
```

多帳戶啟用指令碼

Note

我們建議您使用中央組態，在多個帳戶和區域中啟用和設定 Security Hub CSPM，而不是此指令碼。

[GitHub 中的 Security Hub CSPM 多帳戶啟用指令碼](#)可讓您跨帳戶和區域啟用 Security Hub CSPM。指令碼也會自動化傳送邀請至成員帳戶和啟用的程序 AWS Config。

指令碼會自動啟用所有區域中所有資源 AWS Config 的資源記錄，包括全域資源。它不會將全域資源的記錄限制為單一區域。為了節省成本，我們建議僅在單一區域中記錄全域資源。如果您使用中央組態或跨區域彙總，這應該是您的主區域。如需詳細資訊，請參閱[在中記錄資源 AWS Config](#)。

有一個對應的指令碼可跨帳戶和區域停用 Security Hub CSPM。

後續步驟：姿勢管理和整合

啟用 Security Hub CSPM 之後，我們建議啟用安全標準和控制項來監控您的安全狀態。啟用控制項之後，Security Hub CSPM 會開始執行安全檢查並產生控制項調查結果，協助您偵測 AWS 環境中的錯誤組態。若要接收控制調查結果，您必須啟用和設定 AWS Config Security Hub CSPM。如需詳細資訊，請參閱[啟用和設定 AWS Config Security Hub CSPM](#)。

啟用 Security Hub CSPM 之後，您也可以利用 Security Hub CSPM AWS 服務 與其他和第三方解決方案之間的整合，在 Security Hub CSPM 中查看其問題清單。Security Hub CSPM 會彙總來自不同來源的問題清單，並以一致的格式擷取問題清單。如需詳細資訊，請參閱[了解 Security Hub CSPM 中的整合](#)。

啟用和設定 AWS Config Security Hub CSPM

AWS Security Hub CSPM 使用 AWS Config 規則來執行安全檢查並產生大多數控制項的問題清單。AWS Config 提供 中 AWS 資源組態的詳細檢視 AWS 帳戶。它使用規則來為您的資源和組態記錄器建立基準組態，以偵測特定資源是否違反規則的條件。

有些規則稱為 AWS Config 受管規則，由 預先定義和開發 AWS Config。其他規則是 Security Hub CSPM 開發的自訂 AWS Config 規則。Security Hub CSPM 用於控制項的 AWS Config 規則稱為服務連結規則。服務連結規則允許 AWS 服務 例如 Security Hub CSPM 在您的帳戶中建立 AWS Config 規則。

若要在 Security Hub CSPM 中接收控制項問題清單，您必須 AWS Config 為您的帳戶啟用 。您也必須為啟用控制項評估的資源類型開啟資源記錄。然後，Security Hub CSPM 可以為控制項建立適當的 AWS Config 規則，並開始執行安全檢查並產生控制項的問題清單。

主題

- [啟用和設定 之前的考量事項 AWS Config](#)
- [在 中記錄資源 AWS Config](#)
- [啟用和設定的方法 AWS Config](#)
- [了解 Config.1 控制項](#)
- [產生服務連結規則](#)
- [成本考量](#)

啟用和設定 之前的考量事項 AWS Config

若要在 Security Hub CSPM 中接收控制問題清單，AWS Config 必須在啟用 Security Hub CSPM 的每個 AWS 區域 中為您的帳戶啟用。如果您將 Security Hub CSPM 用於多帳戶環境，AWS Config 則必須在每個區域中為管理員帳戶和所有成員帳戶啟用。

我們強烈建議您在啟用任何 Security Hub CSPM 標準和控制項 AWS Config 之前，先開啟 中的資源記錄。這可協助您確保控制問題清單的準確性。

若要在 中開啟資源記錄 AWS Config，您必須有足夠的許可，才能在連接到組態記錄器的 AWS Identity and Access Management (IAM) 角色中記錄資源。此外，請確保沒有任何 IAM 政策或 AWS Organizations 政策 AWS Config 會阻止 擁有記錄 資源的許可。Security Hub CSPM 控制項會直接評估資源組態，且不考慮 AWS Organizations 政策。如需錄製的詳細資訊 AWS Config，請參閱《AWS Config 開發人員指南》中的[使用組態記錄器](#)。

如果您在 Security Hub CSPM 中啟用標準，但尚未啟用 AWS Config，Security Hub CSPM 會嘗試根據下列排程建立服務連結 AWS Config 規則：

- 在您啟用標準的那一天。
- 啟用標準的隔天。
- 啟用標準後 3 天。
- 啟用標準後 7 天，之後每 7 天持續一次。

如果您使用中央組態，Security Hub CSPM 也會在每次您將啟用一或多個標準與帳戶、組織單位 (OUs) 或根目錄的組態政策建立關聯時，嘗試建立服務連結 AWS Config 規則。

在 中記錄資源 AWS Config

啟用 時 AWS Config，您必須指定您希望 AWS Config 組態記錄器記錄 AWS 的資源。透過服務連結規則，組態記錄器可讓 Security Hub CSPM 偵測資源組態的變更。

若要讓 Security Hub CSPM 產生準確的控制調查結果，您必須開啟 中的 AWS Config 記錄，以取得對應於已啟用控制項的資源類型。它主要是啟用的控制項，具有需要資源記錄的變更觸發排程類型。有些具有定期排程類型的控制項也需要資源記錄。如需這些控制項及其對應資源的清單，請參閱 [控制問題清單所需的 AWS Config 資源](#)。

Warning

如果您未 AWS Config 正確設定 Security Hub CSPM 控制項的記錄，可能會導致不正確的控制調查結果，尤其是在下列執行個體中：

- 您永遠不會記錄特定控制項的資源，或在建立該類型的資源之前停用資源的錄製。在這些情況下，您會收到問題控制項的問題WARNING清單，即使您在停用錄製之後，可能已建立控制項範圍內的資源。此WARNING調查結果是預設調查結果，不會實際評估資源的組態狀態。
- 您可以停用特定控制項評估之資源的錄製。在此情況下，即使控制項未評估新的或更新的資源，Security Hub CSPM 仍會保留停用錄製之前產生的控制項調查結果。Security Hub CSPM 也會將調查結果的合規狀態變更為 WARNING。這些保留的問題清單可能無法準確反映資源的目前組態狀態。

根據預設，會 AWS Config 記錄它在執行 AWS 區域 所在的中探索的所有支援的區域資源。若要接收所有 Security Hub CSPM 控制調查結果，您還必須設定 AWS Config 來記錄全域資源。為了節省成本，我們建議僅在單一區域中記錄全域資源。如果您使用中央組態或跨區域彙總，則此區域應該是您的主區域。

在中 AWS Config，您可以選擇持續記錄和每日記錄資源狀態的變更。如果您選擇每日錄製，則會在資源狀態發生變更時，在每個 24 小時期間結束時 AWS Config 傳送資源組態資料。如果沒有變更，則不會交付任何資料。這可能會延遲產生由變更觸發之控制項的 Security Hub CSPM 調查結果，直到 24 小時期間完成為止。

如需 AWS Config 錄製的詳細資訊，請參閱《AWS Config 開發人員指南》中的[錄製 AWS 資源](#)。

啟用和設定的方法 AWS Config

您可以透過下列任何方式啟用 AWS Config 和開啟資源記錄：

- AWS Config 主控台 – 您可以使用 AWS Config 主控台 AWS Config 為帳戶啟用。如需說明，請參閱《AWS Config 開發人員指南》中的[AWS Config 使用 主控台設定](#)。
- AWS CLI 或 SDKs – 您可以使用 AWS Command Line Interface () AWS Config 為帳戶啟用AWS CLI。如需說明，請參閱《AWS Config 開發人員指南》中的[AWS Config 使用 設定 AWS CLI](#)。AWS 軟體開發套件 SDKs) 也適用於多種程式設計語言。
- CloudFormation 範本 – 若要 AWS Config 為許多帳戶啟用，建議使用名為啟用 AWS Config的 AWS CloudFormation 範本。若要存取此範本，請參閱AWS CloudFormation 《使用者指南》中的[AWS CloudFormation StackSet 範本範例](#)。

根據預設，此範本會排除 IAM 全域資源的記錄。確保您只開啟一個 AWS 區域中的 IAM 全域資源記錄，以節省記錄成本。如果您已啟用跨區域彙總，這應該是您的 [Security Hub CSPM 主區域](#)。否則，可以是 Security Hub CSPM 在支援記錄 IAM 全域資源的任何可用區域。我們建議執行一個 StackSet，以記錄主要區域或其他所選區域中的所有資源，包括 IAM 全域資源。然後，執行第二個 StackSet 來記錄其他區域中 IAM 全域資源以外的所有資源。

- GitHub 指令碼 – Security Hub CSPM 提供 [GitHub 指令碼](#)，AWS Config 可為跨區域的多個帳戶啟用 Security Hub CSPM 和。如果您尚未與整合 AWS Organizations，或者您有一些不屬於組織的成員帳戶，則此指令碼很有用。

如需詳細資訊，請參閱安全部落格上的下列AWS 部落格文章：[AWS Config 最佳化 AWS Security Hub CSPM 以有效管理您的雲端安全狀態](#)。

了解 Config.1 控制項

在 Security Hub CSPM 中，如果 AWS Config 停用，[Config.1](#) 控制項會在您的帳戶中產生FAILED問題清單。如果 AWS Config 已啟用但資源錄製未開啟，它也會在您的帳戶中產生FAILED問題清單。

如果 AWS Config 已啟用且資源記錄已開啟，但已啟用控制檢查的資源類型未開啟資源記錄，Security Hub CSPM 會為 Config.1 控制項產生FAILED問題清單。除了此FAILED調查結果之外，Security Hub CSPM 還會為已啟用的控制項和控制項檢查的資源類型產生WARNING調查結果。例如，如果您啟用[KMS.5](#) 控制項且未開啟資源錄製 AWS KMS keys，Security Hub CSPM 會產生 Config.1 控制項的問題FAILED清單。Security Hub CSPM 也會產生 KMS.5 控制項和 KMS 金鑰WARNING的問題清單。

若要接收 Config.1 控制項的問題PASSED清單，請開啟對應至已啟用控制項之所有資源類型的資源記錄。同時停用組織不需要的控制項。這有助於確保您在安全控制檢查中沒有組態差距。它還有助於確保您收到有關設定錯誤資源的準確調查結果。

如果您是組織的委派 Security Hub CSPM 管理員，則必須為您的帳戶和成員帳戶正確設定 AWS Config 記錄。如果您使用跨區域彙總，則必須在主要區域和所有連結區域中正確設定 AWS Config 記錄。全域資源不需要記錄在連結的區域中。

產生服務連結規則

對於每個使用服務連結 AWS Config 規則的控制項，Security Hub CSPM 會在您的 AWS 環境中建立所需規則的執行個體。

這些服務連結規則專屬於 Security Hub CSPM。即使相同規則的其他執行個體已存在，Security Hub CSPM 也會建立這些服務連結規則。服務連結規則會在原始規則名稱securityhub之前新增，並在

規則名稱之後新增唯一識別符。例如，對於 AWS Config 受管規則 `vpc-flow-logs-enabled`，服務連結規則名稱可能是 `securityhub-vpc-flow-logs-enabled-12345`。

AWS Config 受管規則的數量有配額，可用於評估 controls. AWS Config rules，Security Hub CSPM 建立的規則不會計入這些配額。即使您已達到帳戶中受管規則的 AWS Config 配額，也可以啟用安全標準。若要進一步了解 AWS Config 規則的配額，請參閱《AWS Config 開發人員指南》中的 [的服務限制 AWS Config](#)。

成本考量

Security Hub CSPM 可以透過更新 AWS Config 組態項目來影響您的 `AWS::Config::ResourceCompliance` 組態記錄器成本。每次與 AWS Config 規則相關聯的 Security Hub CSPM 控制項變更合規狀態、啟用或停用，或具有參數更新時，都可以進行更新。如果您只將 AWS Config 組態記錄器用於 Security Hub CSPM，而且不將此組態項目用於其他用途，我們建議您關閉其中的錄製 AWS Config。這可以降低您的 AWS Config 成本。您不需要記錄安全檢查 `AWS::Config::ResourceCompliance`，即可在 Security Hub CSPM 中運作。

如需與資源記錄相關的成本資訊，請參閱 [AWS Security Hub CSPM 定價](#) 和 [AWS Config 定價](#)。

了解 Security Hub CSPM 中的本機組態

本機組態是 AWS 組織在 Security Hub CSPM 中設定的預設方式。如果您不選擇加入並啟用中央組態，您的組織預設會使用本機組態。

在本機組態下，委派的 Security Hub CSPM 管理員帳戶對組態設定的控制有限。委派管理員可以強制執行的唯一設定是在新的組織帳戶中自動啟用 Security Hub CSPM 和預設安全標準。這些設定僅適用於您指定委派管理員帳戶的區域。預設安全標準為 AWS 基礎安全最佳實務 (FSBP) 和網際網路安全中心 (CIS) AWS 基準 1.2.0 版。本機組態設定不適用於現有的組織帳戶或指定委派管理員帳戶所在區域以外的區域。

除了在單一區域的新組織帳戶中啟用 Security Hub CSPM 和預設標準之外，您還必須在每個區域和帳戶中分別設定其他 Security Hub CSPM 設定，包括標準和控制項。由於這可能是重複的程序，如果下列一或多個項目適用於您，建議您針對多帳戶環境使用中央組態：

- 您想要針對組織的各個部分進行不同的組態設定（例如，針對不同團隊啟用不同的標準或控制項）。
- 您在多個區域中操作，並希望減少在這些區域中設定服務的時間和複雜性。
- 您希望新帳戶在加入組織時使用特定的組態設定。

- 您希望組織帳戶從父帳戶或根繼承特定組態設定。

如需中央組態的資訊，請參閱 [了解 Security Hub CSPM 中的中央組態](#)。

了解 Security Hub CSPM 中的中央組態

中央組態是一項 AWS Security Hub CSPM 功能，可協助您跨多個和設定和管理 Security Hub CSPM AWS 帳戶 AWS 區域。若要使用中央組態，您必須先整合 Security Hub CSPM 和 AWS Organizations。您可以透過建立組織並指定組織的委派 Security Hub CSPM 管理員帳戶來整合服務。

從委派的 Security Hub CSPM 管理員帳戶，您可以為組織的帳戶和跨區域的組織單位 (OUs) 啟用 Security Hub CSPM。您也可以跨區域啟用、設定和停用帳戶和 OUs 的個別安全標準和安全控制。您只需幾個步驟即可從一個主要區域設定這些設定，稱為主要區域。

當您使用中央組態時，委派管理員可以選擇要設定哪些帳戶和 OUs。如果委派管理員將成員帳戶或 OU 指定為自我管理，則該成員可以在每個區域中分別設定自己的設定。如果委派管理員將成員帳戶或 OU 指定為集中管理，則只有委派管理員才能跨區域設定成員帳戶或 OU。您可以將組織中的所有帳戶和 OUs 指定為集中管理、所有自我管理或兩者的組合。

若要設定集中受管帳戶，委派管理員會使用 Security Hub CSPM 組態政策。組態政策可讓委派管理員指定啟用或停用 Security Hub CSPM，以及啟用或停用哪些標準和控制項。它們也可以用來自訂特定控制項的參數。

組態政策會在主要區域和所有連結區域中生效。委派管理員會先指定組織的主區域和連結的區域，再開始使用中央組態。指定連結的區域是選用的。委派管理員可以為整個組織建立單一組態政策，或建立多個組態政策來設定不同帳戶和 OUs 的變數設定。

Tip

如果您不使用中央組態，則必須在每個帳戶和區域中分別設定 Security Hub CSPM。這稱為本機組態。在本機組態下，委派管理員可以在目前區域中的新組織帳戶中自動啟用 Security Hub CSPM 和一組有限的安全標準。本機組態不適用於現有的組織帳戶或目前區域以外的區域。本機組態也不支援使用組態政策。

本節提供中央組態的概觀。

使用中央組態的優點

中央組態的優點包括下列項目：

簡化 Security Hub CSPM 服務和功能的組態

當您使用中央組態時，Security Hub CSPM 會引導您完成為組織設定安全最佳實務的程序。它也會自動將產生的組態政策部署到指定的帳戶和 OUs。如果您有現有的 Security Hub CSPM 設定，例如自動啟用新的安全控制，您可以使用這些設定做為組態政策的起點。此外，Security Hub CSPM 主控台上的組態頁面會顯示組態政策的即時摘要，以及哪些帳戶和 OUs 使用每個政策。

跨帳戶和區域設定

您可以使用中央組態，跨多個帳戶和區域設定 Security Hub CSPM。這有助於確保組織的每個部分維持一致的組態和足夠的安全涵蓋範圍。

適應不同帳戶和 OUs 中的不同組態

使用中央組態，您可以選擇以不同的方式設定組織的帳戶和 OUs。例如，您的測試帳戶和生產帳戶可能需要不同的組態。您也可以建立組態政策，涵蓋加入組織的新帳戶。

防止組態偏離

當使用者變更與委派管理員選擇衝突的服務或功能時，會發生組態偏離。中央組態可防止此偏離。當您將帳戶或 OU 指定為集中管理時，只能由組織的委派管理員設定。如果您偏好特定帳戶或 OU 來設定自己的設定，您可以將其指定為自我管理。

何時使用中央組態？

中央組態最適合包含多個 Security Hub CSPM 帳戶 AWS 的環境。它旨在協助您集中管理多個帳戶的 Security Hub CSPM。

您可以使用中央組態來設定 Security Hub CSPM 服務、安全標準和安全控制。您也可以使用它來自訂特定控制項的參數。如需安全標準的詳細資訊，請參閱 [了解 Security Hub CSPM 中的安全標準](#)。如需安全控制的詳細資訊，請參閱 [了解 Security Hub CSPM 中的安全控制](#)。

中央組態術語和概念

了解下列關鍵術語和概念可協助您使用 Security Hub CSPM 中央組態。

中央組態

Security Hub CSPM 功能可協助組織的委派 Security Hub CSPM 管理員帳戶設定跨多個帳戶和區域的 Security Hub CSPM 服務、安全標準和安全控制。若要設定這些設定，委派管理員會為其組織中的集中受管帳戶建立和管理 Security Hub CSPM 組態政策。自我管理帳戶可以在每個區域中分別設定自己的設定。若要使用中央組態，您必須整合 Security Hub CSPM 和 AWS Organizations。

主區域

委派管理員透過建立和管理組態政策，AWS 區域 從中集中設定 Security Hub CSPM 的。組態政策會在主要區域和所有連結區域中生效。

主要區域也做為 Security Hub CSPM 彙總區域，接收來自連結區域的調查結果、洞見和其他資料。

在 2019 年 3 月 20 日或之後 AWS 引進的區域稱為選擇加入區域。選擇加入區域不能是主要區域，但可以是連結的區域。如需選擇加入區域的清單，請參閱《AWS 帳戶管理參考指南》中的[啟用和停用區域的考量事項](#)。

連結的區域

可從主要區域 AWS 區域 設定。組態政策由主要區域中的委派管理員建立。這些政策會在主要區域和所有連結區域中生效。指定連結的區域是選用的。

連結的區域也會將問題清單、洞見和其他資料傳送至主要區域。

在 2019 年 3 月 20 日或之後 AWS 引進的區域稱為選擇加入區域。您必須先為帳戶啟用此類區域，才能套用組態政策。Organizations 管理帳戶可以為成員帳戶啟用選擇加入區域。如需詳細資訊，請參閱《[帳戶管理參考指南](#)》中的[指定 AWS 區域 您的帳戶可以使用哪些](#)。AWS

目標

AWS 帳戶、組織單位 (OU) 或組織根目錄。

Security Hub CSPM 組態政策

委派管理員可為集中受管目標設定的 Security Hub CSPM 設定集合。其中包含：

- 是否啟用或停用 Security Hub CSPM。
- 是否啟用一或多個[安全標準](#)。
- 要跨啟用的標準啟用哪些[安全控制](#)。委派管理員可以透過提供應啟用的特定控制項清單來執行此操作，而 Security Hub CSPM 會停用所有其他控制項（包括發行時的新控制項）。或者，委派管理員可以提供應停用的特定控制項清單，而 Security Hub CSPM 會啟用所有其他控制項（包括發行時的新控制項）。
- 或者，[自訂已啟用標準之所選控制項的參數](#)。

組態政策在與至少一個帳戶、組織單位 (OU) 或根關聯之後，會在主區域和所有連結區域中生效。

在 Security Hub CSPM 主控台上，委派管理員可以選擇 Security Hub CSPM 建議的組態政策或建立自訂組態政策。使用 Security Hub CSPM API 和 AWS CLI，委派管理員只能建立自訂組態政策。委派管理員最多可以建立 20 個自訂組態政策。

在建議的組態政策中，Security Hub CSPM、AWS 基礎安全最佳實務 (FSBP) 標準，以及所有現有和新的 FSBP 控制項都會啟用。接受參數的控制項會使用預設值。建議的組態政策適用於整個組織。

若要將不同的設定套用至組織，或將不同的組態政策套用至不同的帳戶和 OUs，請建立自訂組態政策。

本機組態

整合 Security Hub CSPM 和 之後，組織的預設組態類型 AWS Organizations。透過本機組態，委派管理員可以選擇在目前區域中的新組織帳戶中自動啟用 Security Hub CSPM 和 [預設安全標準](#)。如果委派管理員自動啟用預設標準，則屬於這些標準的所有控制項也會自動啟用，其中包含新組織帳戶的預設參數。這些設定不適用於現有帳戶，因此在帳戶加入組織之後，組態漂移是可能的。停用屬於預設標準一部分的特定控制項，以及設定其他標準和控制項，都必須在每個帳戶和區域中分別完成。

本機組態不支援使用組態政策。若要使用組態政策，您必須切換到中央組態。

手動帳戶管理

如果您未將 Security Hub CSPM 與 整合，AWS Organizations 或擁有獨立帳戶，則必須在每個區域中分別指定每個帳戶的設定。手動帳戶管理不支援使用組態政策。

中央組態 APIs

只有 Security Hub CSPM 委派 Security Hub CSPM 管理員可以在主區域中使用 Security Hub CSPM 操作來管理集中管理帳戶的組態政策。這些操作包括：

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

帳戶特定的 APIs

Security Hub CSPM 操作，可用於account-by-account啟用或停用 Security Hub CSPM、標準和控制項。這些操作作用於每個個別區域。

自我管理帳戶可以使用帳戶特定的操作來設定自己的設定。在主要區域和連結區域中，集中管理的帳戶無法使用下列帳戶特定操作。在這些區域中，只有委派管理員可以透過中央組態操作和組態政策來設定集中受管帳戶。

- BatchDisableStandards
- BatchEnableStandards
- BatchUpdateStandardsControlAssociations
- DisableSecurityHub
- EnableSecurityHub
- UpdateStandardsControl

若要檢查帳戶狀態，集中管理帳戶的擁有者可以使用 Security Hub CSPM API 的任何 Get 或 Describe 操作。

如果您使用本機組態或手動帳戶管理，而不是中央組態，則可以使用這些帳戶特定的操作。

自我管理帳戶也可以使用 *Invitations 和 *Members 操作。不過，我們建議自我管理帳戶不要使用這些操作。如果成員帳戶自己的成員與委派管理員屬於不同的組織，則政策關聯可能會失敗。

組織單位 (OU)

在 AWS Organizations 和 Security Hub CSPM 中，群組的容器 AWS 帳戶。組織單位 (OU) 也可以包含其他 OUs，可讓您建立類似上下倒置樹狀結構的階層，其中 OU 的父系 OU 位於 OUs 的頂端和分支，以樹狀樹葉的帳戶結尾。OU 可以只有一個父系，而且每個組織帳戶可以是只有一個 OU 的成員。

您可以在 AWS Organizations 或 中管理 OUs AWS Control Tower。如需詳細資訊，請參閱AWS Organizations 《使用者指南》中的[管理組織單位](#)，或《AWS Control Tower 使用者指南》中的[使用 管理組織和帳戶 AWS Control Tower](#)。

委派管理員可以將組態政策與特定帳戶或 OUs 或根關聯，以涵蓋組織中的所有帳戶和 OUs。

集中管理

只有委派管理員可以使用組態政策跨區域設定的目標。

委派管理員帳戶指定目標是否集中管理。委派管理員也可以將目標的狀態從集中受管變更為自我管理，或反之亦然。

自我管理

管理自己的 Security Hub CSPM 設定的目標。自我管理目標使用帳戶特定的操作，在每個區域中分別設定 Security Hub CSPM。這與集中受管目標相反，這些目標只能由跨區域的委派管理員透過組態政策進行設定。

委派管理員帳戶會指定目標是否為自我管理。委派管理員可以將自我管理行為套用至目標。或者，帳戶或 OU 可以從父系繼承自我管理的行為。

委派管理員帳戶本身可以是自我管理帳戶。委派管理員帳戶可以將目標的狀態從自我管理變更為集中管理，或反之亦然。

組態政策關聯

組態政策與帳戶、組織單位 (OU) 或根帳戶之間的連結。當政策關聯存在時，帳戶、OU 或根會使用組態政策定義的設定。下列任一情況下都會存在關聯：

- 當委派管理員直接將組態政策套用至帳戶、OU 或根帳戶時
- 當帳戶或 OU 從父 OU 或根繼承組態政策時

在套用或繼承不同的組態之前，都會存在關聯。

套用的組態政策

一種組態政策關聯的類型，其中委派的管理員會將組態政策直接套用至目標帳戶、OUs 或根帳戶。目標的設定方式是設定組態政策，只有委派的管理員可以變更其組態。如果套用至根帳戶，則組態政策會影響組織中所有帳戶和 OUs，這些帳戶和 OU 不會透過應用程式使用不同的組態，或繼承來自最近的父系。

委派管理員也可以將自我管理組態套用至特定帳戶、OUs 或根目錄。

繼承的組態政策

一種組態政策關聯類型，其中帳戶或 OU 採用最接近父系 OU 或根目錄的組態。如果組態政策未直接套用至帳戶或 OU，則會繼承最接近父項的組態。政策的所有元素都會繼承。換句話說，帳戶或 OU 無法選擇僅選擇性地繼承政策的一部分。如果最近的父系是自我管理的，子帳戶或 OU 會繼承父系的自我管理行為。

繼承無法覆寫套用的組態。也就是說，如果組態政策或自我管理組態直接套用至帳戶或 OU，則會使用該組態，而不會繼承父系的組態。

根目錄

在 AWS Organizations 和 Security Hub CSPM 中，組織中最上層的父節點。如果委派管理員將組態政策套用於根目錄，則政策會與組織中的所有帳戶和 OUs 相關聯，除非他們透過應用程式或繼承使用不同的政策，或被指定為自我管理。如果管理員將根指定為自我管理，則組織中的所有帳戶和 OUs 都會自我管理，除非他們透過應用程式或繼承使用組態政策。如果根是自我管理的，且目前沒有組態政策，則組織中的所有新帳戶都會保留其目前的設定。

加入組織的新帳戶屬於根帳戶，直到指派給特定 OU 為止。如果新帳戶未指派給 OU，則會繼承根組態，除非委派管理員將其指定為自我管理帳戶。

在 Security Hub CSPM 中啟用中央組態

委派的 AWS Security Hub CSPM 管理員帳戶可以使用中央組態，為多個帳戶和組織單位 (OUs) 設定 Security Hub CSPM、標準和控制 AWS 區域。

如需中央組態優點及其運作方式的背景資訊，請參閱 [了解 Security Hub CSPM 中的中央組態](#)。

本節說明中央組態的先決條件，以及如何開始使用它。

中央組態的先決條件

您必須先將 Security Hub CSPM 與整合 AWS Organizations 並指定主要區域，才能開始使用中央組態。如果您使用 Security Hub CSPM 主控台，這些先決條件會包含在中央組態的選擇加入工作流程中。

與 Organizations 整合

您必須整合 Security Hub CSPM 和 Organizations，才能使用中央組態。

若要整合這些服務，請先在 Organizations 中建立組織。然後，從 Organizations 管理帳戶指定 Security Hub CSPM 委派管理員帳戶。如需說明，請參閱[將 Security Hub CSPM 與整合 AWS Organizations](#)。

請確定您在預定的主區域中指定委派管理員。當您開始使用中央組態時，也會在所有連結區域中自動設定相同的委派管理員。Organizations 管理帳戶無法設定為委派管理員帳戶。

Important

當您使用中央組態時，無法使用 Security Hub CSPM 主控台或 Security Hub CSPM APIs 來變更或移除委派的管理員帳戶。如果 Organizations 管理帳戶使用 AWS Organizations APIs 來變更或移除 Security Hub CSPM 委派管理員，Security Hub CSPM 會自動停止中央組態。您的

組態政策也會取消關聯並刪除。成員帳戶會保留他們在委派管理員變更或移除之前所擁有的組態。

指定主要區域

您必須指定主要區域才能使用中央組態。主要區域是委派管理員從中設定組織的區域。

Note

主要區域不能是 AWS 已指定為選擇加入區域的區域。預設會停用選擇加入區域。如需選擇加入區域的清單，請參閱《AWS 帳戶管理參考指南》中的[啟用和停用區域的考量](#)事項。

或者，您可以指定一個或多個可從主要區域設定的連結區域。

委派管理員只能從主要區域建立和管理組態政策。組態政策會在主要區域和所有連結區域中生效。您無法建立僅適用於這些區域子集的組態政策，而不是其他區域。例外情況是涉及全域資源的控制項。如果您使用中央組態，Security Hub CSPM 會自動停用涉及主要區域以外所有區域中全域資源的控制項。如需詳細資訊，請參閱[使用全域資源的控制項](#)。

主要區域也是您的 Security Hub CSPM 彙總區域，可接收來自連結區域的調查結果、洞見和其他資料。

如果您已設定跨區域彙總的彙總區域，則這是中央組態的預設主區域。您可以在開始使用中央組態之前變更主要區域，方法是刪除目前的問題清單彙總工具，並在所需的主要區域中建立新的問題清單彙總工具。問題清單彙整工具是一種 Security Hub CSPM 資源，可指定主要區域和連結的區域。

若要指定主要區域，請參閱[設定彙總區域的步驟](#)。如果您已有主要區域，您可以叫用 [GetFindingAggregator](#) API 以查看其詳細資訊，包括目前與其連結的區域。

啟用中央組態的說明

選擇您偏好的方法，然後依照步驟為您的組織啟用中央組態。

Security Hub CSPM console

啟用中央組態（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。

2. 在導覽窗格中，選擇設定和組態。然後，選擇開始中央組態。

如果您要加入 Security Hub CSPM，請選擇移至 Security Hub CSPM。

3. 在指定委派管理員頁面上，選取委派管理員帳戶或輸入其帳戶 ID。如果適用，我們建議您選擇已為其他 AWS 安全與合規服務設定的相同委派管理員。選擇設定委派管理員。
4. 在集中組織頁面上的區域區段中，選取您的主要區域。您必須登入主區域才能繼續。如果您已設定跨區域彙總的彙總區域，則會顯示為主要區域。若要變更主要區域，請選擇編輯區域設定。然後，您可以選取您偏好的主區域並返回此工作流程。
5. 選取至少一個區域以連結至主要區域。或者，選擇是否要將未來的支援區域自動連結至主要區域。您在此處選取的區域將由委派管理員從主要區域設定。組態政策會在您的主要區域和所有連結區域中生效。
6. 選擇確認並繼續。
7. 您現在可以使用中央組態。繼續遵循主控台提示建立您的第一個組態政策。如果您尚未準備好建立組態政策，請選擇我尚未準備好進行設定。您可以稍後在導覽窗格中選擇設定和組態來建立政策。如需建立組態政策的說明，請參閱 [建立和關聯組態政策](#)。

Security Hub CSPM API

啟用中央組態 (API)

1. 使用委派管理員帳戶的登入資料，從主要區域叫用 [UpdateOrganizationConfiguration](#) API。
2. 將 AutoEnable 欄位設定為 false。
3. 將 OrganizationConfiguration 物件中的 ConfigurationType 欄位設定為 CENTRAL。此動作具有下列影響：
 - 在所有連結區域中，將呼叫帳戶指定為 Security Hub CSPM 委派管理員。
 - 在所有連結區域的委派管理員帳戶中啟用 Security Hub CSPM。
 - 針對使用 Security Hub CSPM 且屬於組織的新帳戶和現有帳戶，將呼叫帳戶指定為 Security Hub CSPM 委派管理員。這發生在主要區域和所有連結的區域。呼叫帳戶只有在與已啟用 Security Hub CSPM 的組態政策相關聯時，才會設定為新組織帳戶的委派管理員。呼叫帳戶只有在已啟用 Security Hub CSPM 時，才會設定為現有組織帳戶的委派管理員。
 - 在所有連結 false 的區域中 [AutoEnable](#) 設定為 `AutoEnable`，並在主要區域和所有連結的區域中 [AutoEnableStandards](#) 設定為 NONE。當您使用中央組態時，這些參數與主區域和連結區域無關，但您可以透過使用組態政策，在組織帳戶中自動啟用 Security Hub CSPM 和預設安全標準。

4. 您現在可以使用中央組態。委派管理員可以建立組態政策，在您的組織中設定 Security Hub CSPM。如需建立組態政策的說明，請參閱 [建立和關聯組態政策](#)。

範例 API 請求：

```
{
  "AutoEnable": false,
  "OrganizationConfiguration": {
    "ConfigurationType": "CENTRAL"
  }
}
```

AWS CLI

啟用中央組態 (AWS CLI)

1. 使用委派管理員帳戶的登入資料，從主要區域執行 [update-organization-configuration](#) 命令。
2. 納入 no-auto-enable 參數。
3. 將 organization-configuration 物件中的 ConfigurationType 欄位設定為 CENTRAL。此動作具有下列影響：
 - 在所有連結區域中，將呼叫帳戶指定為 Security Hub CSPM 委派管理員。
 - 在所有連結區域的委派管理員帳戶中啟用 Security Hub CSPM。
 - 針對使用 Security Hub CSPM 且屬於組織的新帳戶和現有帳戶，將呼叫帳戶指定為 Security Hub CSPM 委派管理員。這發生在主要區域和所有連結的區域。呼叫帳戶只有在與已啟用 Security Hub 的組態政策相關聯時，才會設定為新組織帳戶的委派管理員。呼叫帳戶只有在已啟用 Security Hub CSPM 時，才會設定為現有組織帳戶的委派管理員。
 - 在所有連結 [no-auto-enable](#) 區域中將自動啟用選項設定為 `no-auto-enable`，並在主要區域和所有連結 NONE 區域中 [auto-enable-standards](#) 將設定為 `no-auto-enable-standards`。當您使用中央組態時，這些參數與主區域和連結區域無關，但您可以透過使用組態政策，在組織帳戶中自動啟用 Security Hub CSPM 和預設安全標準。
4. 您現在可以使用中央組態。委派管理員可以建立組態政策，在您的組織中設定 Security Hub CSPM。如需建立組態政策的說明，請參閱 [建立和關聯組態政策](#)。

範例命令：

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}
```

集中管理與自我管理的目標

當您啟用中央組態時，委派的 AWS Security Hub CSPM 管理員可以將每個組織帳戶、組織單位 (OU) 和根指定為集中管理或自我管理。目標的管理類型決定如何指定其 Security Hub CSPM 設定。

如需中央組態優點及其運作方式的背景資訊，請參閱 [了解 Security Hub CSPM 中的中央組態](#)。

本節說明集中管理和自我管理指定之間的差異，以及如何選擇帳戶、OU 或根的管理類型。

自我管理

自我管理帳戶、OU 或根的擁有者必須在每個帳戶中分別設定其設定 AWS 區域。委派管理員無法建立自我管理目標的組態政策。

集中管理

只有委派的 Security Hub CSPM 管理員可以設定集中受管帳戶、OUs 或主要區域和連結區域的根目錄的設定。組態政策可以與集中管理的帳戶和 OUs 建立關聯。

委派管理員可以在自我管理和集中管理之間切換目標的狀態。根據預設，當您透過 Security Hub CSPM API 啟動中央組態時，所有帳戶和 OU 都會自我管理。在主控台中，管理類型取決於您的第一個組態政策。與您第一個政策相關聯的帳戶和 OUs 會集中管理。根據預設，其他帳戶和 OUs 會自我管理。

如果您將組態政策與先前自我管理的帳戶建立關聯，政策設定會覆寫自我管理的指定。帳戶會成為集中管理，並採用組態政策中反映的設定。

如果您將集中受管帳戶變更為自我管理帳戶，則先前透過組態政策套用至帳戶的設定會保持不變。例如，中央受管帳戶最初可以與啟用 Security Hub CSPM、啟用 AWS 基礎安全最佳實務和停用 CloudTrail.1。如果您接著將帳戶指定為自我管理，則所有設定保持不變。不過，帳戶擁有者可以獨立變更未來帳戶的設定。

子帳戶和 OUs 可以從自我管理的父系繼承自我管理行為，就像子帳戶和 OUs 可以從集中管理的父系繼承組態政策一樣。如需詳細資訊，請參閱 [透過應用程式和繼承的政策關聯](#)。

自我管理帳戶或 OU 無法從父節點或根繼承組態政策。例如，如果您希望組織中的所有帳戶和 OUs 從根繼承組態政策，您必須將自我管理節點的管理類型變更為集中管理。

在自我管理帳戶中設定設定的選項

自我管理帳戶必須在每個區域中分別設定自己的設定。

自我管理帳戶的擁有者可以在每個區域中調用 Security Hub CSPM API 的下列操作來設定其設定：

- `EnableSecurityHub` 和 `DisableSecurityHub` 啟用或停用 Security Hub CSPM 服務（如果自我管理帳戶具有委派的 Security Hub CSPM 管理員，則管理員必須先[取消帳戶關聯](#)，帳戶擁有者才能停用 Security Hub CSPM）。
- `BatchEnableStandards` 和 `BatchDisableStandards` 來啟用或停用標準
- `BatchUpdateStandardsControlAssociations` 或 `UpdateStandardsControl` 以啟用或停用控制項

自我管理帳戶也可以使用 `*Invitations` 和 `*Members` 操作。不過，我們建議自我管理帳戶不要使用這些操作。如果成員帳戶自己的成員與委派管理員屬於不同的組織，則政策關聯可能會失敗。

如需 Security Hub CSPM API 動作的說明，請參閱 [AWS Security Hub CSPM API 參考](#)。

自我管理帳戶也可以使用 Security Hub CSPM 主控台或 AWS CLI 在每個區域中設定其設定。

自我管理帳戶無法叫用與 Security Hub CSPM 組態政策和政策關聯相關的任何 APIs。只有委派管理員可以叫用中央組態 APIs 並使用組態政策來設定集中受管帳戶。

選擇目標的管理類型

選擇您偏好的方法，並依照步驟在 AWS Security Hub CSPM 中將帳戶或 OU 指定為集中管理或自我管理。

Security Hub CSPM console

選擇帳戶或 OU 的管理類型

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用主要區域中委派 Security Hub CSPM 管理員帳戶的登入資料登入。

2. 選擇 Configuration (組態)。

3. 在組織索引標籤上，選取目標帳戶或 OU。選擇編輯。
4. 在定義組態頁面上，針對管理類型，如果您希望委派管理員設定目標帳戶或 OU，請選擇集中管理。然後，如果您想要將現有的組態政策與目標建立關聯，請選擇套用特定政策。如果您希望目標繼承其最近父系的組態，請選擇從我的組織繼承。如果您希望帳戶或 OU 設定自己的設定，請選擇自我管理。
5. 選擇下一步。檢閱您的變更，然後選擇儲存。

Security Hub CSPM API

選擇帳戶或 OU 的管理類型

1. 從主區域中的 Security Hub CSPM 委派管理員帳戶叫用 [StartConfigurationPolicyAssociation](#) API。
2. 對於 ConfigurationPolicyIdentifier 欄位，SELF_MANAGED_SECURITY_HUB如果您希望帳戶或 OU 控制自己的設定，請提供。如果您希望委派管理員控制帳戶或 OU 的設定，請提供相關組態政策的 Amazon Resource Name (ARN) 或 ID。
3. 針對 Target 欄位，提供您要變更其管理類型之目標的 AWS 帳戶 ID、OU ID 或根 ID。這會將自我管理行為或指定的組態政策與目標建立關聯。目標的子帳戶可能會繼承自我管理的行為或組態政策。

指定自我管理帳戶的範例 API 請求：

```
{
  "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
  "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

選擇帳戶或 OU 的管理類型

1. 從主區域中的 Security Hub CSPM 委派管理員帳戶執行 [start-configuration-policy-association](#) 命令。
2. 對於 configuration-policy-identifier 欄位，SELF_MANAGED_SECURITY_HUB如果您希望帳戶或 OU 控制自己的設定，請提供。如果您希望委派管理員控制帳戶或 OU 的設定，請提供相關組態政策的 Amazon Resource Name (ARN) 或 ID。

- 針對 target 欄位，提供您要變更其管理類型之目標的 AWS 帳戶 ID、OU ID 或根 ID。這會將自我管理行為或指定的組態政策與目標建立關聯。目標的子帳戶可能會繼承自我管理的行為或組態政策。

指定自我管理帳戶的範例命令：

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

組態政策如何在 Security Hub CSPM 中運作

委派的 AWS Security Hub CSPM 管理員可以建立組態政策，以設定組織的 Security Hub CSPM、安全標準和安全控制。建立組態政策後，委派管理員可以將其與特定帳戶、組織單位 (OUs) 或根帳戶建立關聯。政策接著會在指定的帳戶、OUs 或根帳戶中生效。

如需中央組態優點及其運作方式的背景資訊，請參閱 [了解 Security Hub CSPM 中的中央組態](#)。

本節提供組態政策的詳細概觀。

政策考量事項

在 Security Hub CSPM 中建立組態政策之前，請考慮下列詳細資訊。

- 組態政策必須建立關聯才能生效 – 建立組態政策之後，您可以將其與一或多個帳戶、組織單位 (OUs) 或根帳戶建立關聯。組態政策可以透過直接應用程式或從父 OUs 繼承來與帳戶或 OU 建立關聯。
- 帳戶或 OU 只能與一個組態政策相關聯 – 為了防止設定衝突，帳戶或 OU 在任何指定時間只能與一個組態政策相關聯。或者，帳戶或 OU 可以自我管理。
- 組態政策已完成 – 組態政策提供設定的完整規格。例如，子帳戶無法接受來自某個政策的某些控制項設定，以及來自另一個政策的其他控制項設定。當您將政策與子帳戶建立關聯時，請確保政策指定您希望子帳戶使用的所有設定。
- 無法還原組態政策 – 將組態政策與帳戶或 OUs 建立關聯後，就無法還原組態政策。例如，如果您將停用 CloudWatch 控制項的組態政策與特定帳戶建立關聯，然後取消該政策的關聯，則會繼續在該帳戶中停用 CloudWatch 控制項。若要再次啟用 CloudWatch 控制項，您可以將帳戶與啟用控制項的新政策建立關聯。或者，您可以將帳戶變更為自我管理，並啟用帳戶中的每個 CloudWatch 控制項。

- 組態政策在您的主要區域和所有連結區域中生效 – 組態政策會影響主要區域和所有連結區域中的所有關聯帳戶。您無法建立僅在其中部分區域而非其他區域生效的組態政策。例外狀況是[使用全域資源的控制項](#)。Security Hub CSPM 會自動停用涉及主要區域以外所有區域中全域資源的控制項。

在 2019 年 3 月 20 日或之後 AWS 引進的區域稱為選擇加入區域。您必須先為帳戶啟用此類區域，組態政策才會在該處生效。Organizations 管理帳戶可以為成員帳戶啟用選擇加入區域。如需啟用選擇加入區域的指示，請參閱 [《帳戶管理參考指南》中的指定 AWS 區域 您的帳戶可以使用哪些](#)。

AWS

如果您的政策設定的主區域或一或多個連結區域中無法使用的控制項，Security Hub CSPM 會略過無法使用區域中的控制項組態，但在可使用控制項的區域中套用組態。您缺少主區域或任何連結區域中無法使用之控制項的涵蓋範圍。

- 組態政策是 資源 – 組態政策具有 Amazon Resource Name (ARN) 和通用唯一識別符 (UUID)。ARN 使用以下格式：`arn:partition:securityhub:region:delegated administrator account ID:configuration-policy/configuration policy UUID`。自我管理組態沒有 ARN 或 UUID。自我管理組態的識別符為 SELF_MANAGED_SECURITY_HUB。

組態政策的類型

每個組態政策都會指定下列設定：

- 啟用或停用 Security Hub CSPM。
- 啟用一或多個[安全標準](#)。
- 指出跨已啟用的標準啟用哪些[安全控制](#)。您可以透過提供應啟用的特定控制項清單來執行此操作，Security Hub CSPM 會停用所有其他控制項，包括發行時的新控制項。或者，您可以提供應該停用的特定控制項清單，而 Security Hub CSPM 會啟用所有其他控制項，包括發行時的新控制項。
- 或者，[自訂跨已啟用標準啟用之選取控制項的參數](#)。

中央組態政策不包含 AWS Config 記錄器設定。您必須分別啟用 AWS Config 和開啟必要資源的記錄，Security Hub CSPM 才能產生控制問題清單。如需詳細資訊，請參閱[啟用和設定 之前的考量事項 AWS Config](#)。

如果您使用中央組態，Security Hub CSPM 會自動停用涉及主要區域以外所有區域中全域資源的控制項。在可用的所有區域中啟用組態政策時，您選擇啟用的其他控制項。若要將這些控制項的問題清單限制為僅一個區域，您可以更新 AWS Config 記錄器設定，並關閉主要區域以外的所有區域中的全域資源記錄。

如果主區域中不支援涉及全域資源的已啟用控制項，Security Hub CSPM 會嘗試在支援控制項的一個連結區域中啟用控制項。使用中央組態時，您缺乏無法在主要區域或任何連結區域中使用的控制項涵蓋範圍。

如需涉及全域資源的控制項清單，請參閱 [使用全域資源的控制項](#)。

建議的組態政策

第一次在 Security Hub CSPM 主控台中建立組態政策時，您可以選擇 Security Hub CSPM 建議的政策。

建議的政策可啟用 Security Hub CSPM、AWS 基礎安全最佳實務 (FSBP) 標準，以及所有現有和新的 FSBP 控制項。接受參數的控制項會使用預設值。建議的政策適用於根（所有帳戶和 OUs，包括新帳戶和現有帳戶）。為您的組織建立建議的政策之後，您可以從委派的管理員帳戶修改該政策。例如，您可以啟用其他標準或控制項，或停用特定的 FSBP 控制項。如需修改組態政策的說明，請參閱 [更新組態政策](#)。

自訂組態政策

委派管理員可以建立最多 20 個自訂組態政策，而不是建議的政策。您可以將單一自訂政策與整個組織建立關聯，或將不同的自訂政策與不同的帳戶和 OUs 建立關聯。對於自訂組態政策，您可以指定所需的設定。例如，您可以建立自訂政策，以啟用 FSBP、網際網路安全中心 (CIS) AWS Foundations Benchmark v1.4.0，以及這些標準中的所有控制項，但 Amazon Redshift 控制項除外。您在自訂組態政策中使用的精細程度取決於整個組織的預期安全涵蓋範圍。

Note

您無法將停用 Security Hub CSPM 的組態政策與委派管理員帳戶建立關聯。這類政策可以與其他帳戶建立關聯，但會略過與委派管理員的關聯。委派的管理員帳戶會保留其目前的組態。

建立自訂組態政策後，您可以更新組態政策以反映建議的組態，以切換至建議的組態政策。不過，在建立第一個政策之後，您看不到在 Security Hub CSPM 主控台中建立建議組態政策的選項。

透過應用程式和繼承的政策關聯

當您第一次選擇加入中央組態時，您的組織沒有關聯，並採取與選擇加入之前相同的行為。委派管理員接著可以在組態政策或自我管理行為與帳戶、OUs 或根帳戶之間建立關聯。關聯可以透過應用程式或繼承來建立。

從委派管理員帳戶，您可以直接將組態政策套用至帳戶、OU 或根帳戶。或者，委派管理員可以直接將自我管理的指定套用至帳戶、OU 或根帳戶。

如果沒有直接應用程式，帳戶或 OU 會繼承具有組態政策或自我管理行為的最近父系設定。如果最接近的父項與組態政策相關聯，子項會繼承該政策，並且只能由主要區域的委派管理員進行設定。如果最接近的父系是自我管理的，子系會繼承自我管理的行為，並能夠在每個行為中指定自己的設定 AWS 區域。

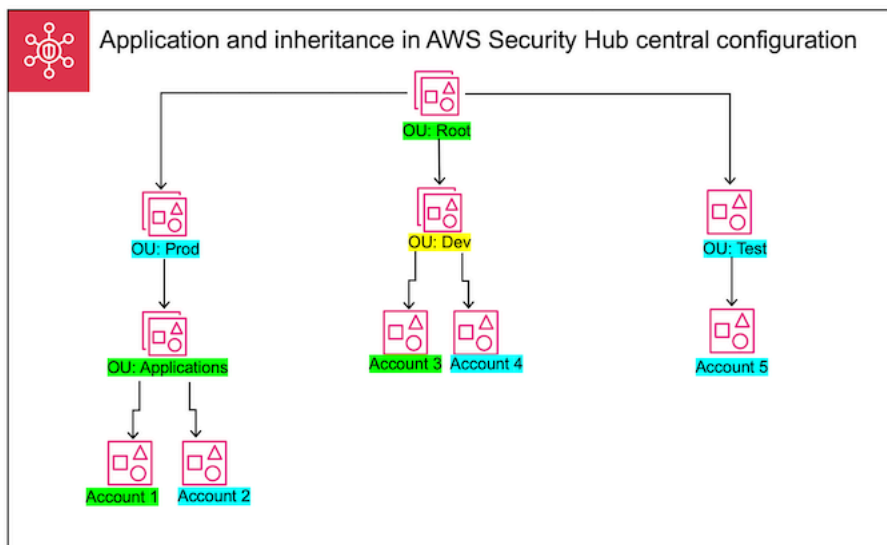
應用程式優先於繼承。換言之，繼承不會覆寫委派管理員直接套用至帳戶或 OU 的組態政策或自我管理指定。

如果您直接將組態政策套用至自我管理帳戶，政策會覆寫自我管理的指定。帳戶會成為集中管理，並採用組態政策中反映的設定。

我們建議將組態政策直接套用至根目錄。如果您將政策套用到根帳戶，則加入組織的新帳戶會自動繼承根政策，除非您將它們與不同的政策建立關聯或將其指定為自我管理。

在指定時間，透過應用程式或繼承，只能有一個組態政策與帳戶或 OU 相關聯。這是為了防止設定衝突而設計。

下圖說明政策應用程式和繼承如何在中央組態中運作。



在此範例中，以綠色反白顯示的節點具有已套用的組態政策。以藍色反白顯示的節點沒有套用到它的組態政策。以黃色反白顯示的節點已指定為自我管理。每個帳戶和 OU 使用以下組態：

- OU : Root (綠色) – 此 OU 使用套用到它的組態政策。
- OU : Prod (藍色) – 此 OU 繼承來自 OU : Root 的組態政策。

- OU：應用程式（綠色）– 此 OU 使用已套用到它的組態政策。
- 帳戶 1（綠色）– 此帳戶使用套用到它的組態政策。
- 帳戶 2（藍色）– 此帳戶繼承來自 OU：Applications 的組態政策。
- OU：Dev（黃色）– 此 OU 是自我管理的。
- 帳戶 3（綠色）– 此帳戶使用套用到它的組態政策。
- 帳戶 4（藍色）– 此帳戶繼承自 OU：Dev 的自我管理行為。
- OU：Test（藍色）– 此帳戶繼承來自 OU：Root 的組態政策。
- 帳戶 5（藍色）– 此帳戶繼承 OU：Root 的組態政策，因為其直接父系 OU：Test 未與組態政策相關聯。

測試組態政策

為了確保您了解組態政策的運作方式，建議您建立一個政策，並將其與測試帳戶或 OU 建立關聯。

測試組態政策

1. 建立自訂組態政策，並確認 Security Hub CSPM 啟用、標準和控制項的指定設定正確無誤。如需說明，請參閱[建立和關聯組態政策](#)。
2. 將組態政策套用至沒有任何子帳戶或 OU 的測試帳戶或 OUs。
3. 確認測試帳戶或 OU 以您主要區域和所有連結區域中的預期方式使用組態政策。您也可以驗證組織中的所有其他帳戶和 OUs 保持自我管理，並且可以在每個區域中變更自己的設定。

在單一帳戶或 OU 中測試組態政策之後，您可以將其與其他帳戶和 OUs 建立關聯。

建立和關聯組態政策

委派的 AWS Security Hub CSPM 管理員帳戶可以建立組態政策，指定如何在指定的帳戶和組織單位 (OUs) 中設定 Security Hub CSPM、標準和控制項。只有在委派管理員將其與至少一個帳戶或組織單位 (OUs) 或根關聯之後，組態政策才會生效。委派管理員也可以將自我管理組態與帳戶、OUs 或根建立關聯。

如果這是您第一次建立組態政策，我們建議您先檢閱 [組態政策如何在 Security Hub CSPM 中運作](#)。

選擇您偏好的存取方法，並依照步驟建立和關聯組態政策或自我管理組態。使用 Security Hub CSPM 主控台時，您可以同時將組態與多個帳戶或 OUs 建立關聯。使用 Security Hub CSPM API 或 AWS CLI，您在每個請求中只能將組態與一個帳戶或 OU 建立關聯。

Note

如果您使用中央組態，Security Hub CSPM 會自動停用涉及主要區域以外所有區域中全域資源的控制項。您選擇在可用的所有區域中啟用組態政策時啟用的其他控制項。若要將這些控制項的問題清單限制為僅一個區域，您可以更新 AWS Config 記錄器設定，並關閉主要區域以外的所有區域中的全域資源記錄。

如果主區域不支援涉及全域資源的已啟用控制項，Security Hub CSPM 會嘗試在支援控制項的一個連結區域中啟用控制項。使用中央組態時，您無法涵蓋主要區域或任何連結區域中無法使用的控制項。

如需涉及全域資源的控制項清單，請參閱 [使用全域資源的控制項](#)。

Security Hub CSPM console

建立和關聯組態政策

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用主要區域中委派 Security Hub CSPM 管理員帳戶的登入資料登入。

2. 在導覽窗格中，選擇組態和政策索引標籤。然後，選擇建立政策。
3. 在設定組織頁面上，如果這是您第一次建立組態政策，您會在組態類型下看到三個選項。如果您已建立至少一個組態政策，則只會看到自訂政策選項。
 - 選擇在整個組織中使用 AWS 建議的 Security Hub CSPM 組態，以使用我們的建議政策。建議的政策會在所有組織帳戶中啟用 Security Hub CSPM、啟用 AWS 基礎安全最佳實務 (FSBP) 標準，以及啟用所有新的和現有的 FSBP 控制項。控制項使用預設參數值。
 - 選擇我尚未準備好進行設定，以便稍後建立組態政策。
 - 選擇自訂政策以建立自訂組態政策。指定是否啟用或停用 Security Hub CSPM、要啟用哪些標準，以及要跨這些標準啟用哪些控制項。或者，為支援 [自訂參數的一或多個已啟用控制項指定自訂參數值](#)。
4. 在帳戶區段中，選擇您要套用組態政策的目標帳戶、OUs 或根帳戶。
 - 如果您想要將組態政策套用至根帳戶，請選擇所有帳戶。這包括組織中未套用或繼承其他政策的所有帳戶和 OUs。

- 如果您想要將組態政策套用至特定帳戶或 OUs 請選擇特定帳戶。輸入帳戶 IDs，或從組織結構中選取帳戶和 OUs。建立政策時，您最多可以將政策套用至 15 個目標（帳戶、OUs 或根目錄）。若要指定較大的數字，請在建立後編輯您的政策，並將其套用至其他目標。
 - 選擇委派管理員，僅將組態政策套用至目前的委派管理員帳戶。
5. 選擇下一步。
 6. 在檢閱和套用頁面上，檢閱您的組態政策詳細資訊。然後，選擇建立政策並套用。在您的主要區域和連結區域中，此動作會覆寫與此組態政策相關聯之帳戶的現有組態設定。帳戶可能會透過應用程式或從父節點繼承，與組態政策相關聯。套用目標的子帳戶和 OUs 將自動繼承此組態政策，除非明確排除、自我管理或使用不同的組態政策。

Security Hub CSPM API

建立和關聯組態政策

1. 從主區域中的 Security Hub CSPM 委派管理員帳戶叫用 [CreateConfigurationPolicy](#) API。
2. 針對 Name，提供組態政策的唯一名稱。或者，對於 Description，提供組態政策的描述。
3. 針對 ServiceEnabled 欄位，指定您希望在此組態政策中啟用或停用 Security Hub CSPM。
4. 針對 EnabledStandardIdentifiers 欄位，指定您要在此組態政策中啟用哪些 Security Hub CSPM 標準。
5. 針對 SecurityControlsConfiguration 物件，指定您要在此組態政策中啟用或停用哪些控制項。選擇 EnabledSecurityControlIdentifiers 表示已啟用指定的控制項。屬於已啟用標準（包括新發佈的控制項）的其他控制項已停用。選擇 DisabledSecurityControlIdentifiers 表示已停用指定的控制項。啟用屬於已啟用標準（包括新發佈的控制項）的其他控制項。
6. 或者，對於 SecurityControlCustomParameters 欄位，指定您要自訂參數的已啟用控制項。CUSTOM 為 ValueType 欄位提供，並為 Value 欄位提供自訂參數值。此值必須是正確的資料類型，且在 Security Hub CSPM 指定的有效範圍內。僅選取控制項支援自訂參數值。如需詳細資訊，請參閱[了解 Security Hub CSPM 中的控制參數](#)。
7. 若要將組態政策套用至帳戶或 OUs，請從主區域中的 Security Hub CSPM 委派管理員帳戶叫用 [StartConfigurationPolicyAssociation](#) API。
8. 針對 ConfigurationPolicyIdentifier 欄位，提供政策的 Amazon Resource Name (ARN) 或通用唯一識別碼 (UUID)。CreateConfigurationPolicy API 會傳回 ARN 和 UUID。對於自我管理組態，ConfigurationPolicyIdentifier 欄位等於 SELF_MANAGED_SECURITY_HUB。

- 針對 Target 欄位，提供您要套用此組態政策的 OU、帳戶或根 ID。每個 API 請求只能提供一個目標。所選目標的子帳戶和 OUs 將自動繼承此組態政策，除非它們是自我管理或使用不同的組態政策。

建立組態政策的 API 請求範例：

```
{
  "Name": "SampleConfigurationPolicy",
  "Description": "Configuration policy for production accounts",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
        "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
      ],
      "SecurityControlsConfiguration": {
        "DisabledSecurityControlIdentifiers": [
          "CloudTrail.2"
        ],
        "SecurityControlCustomParameters": [
          {
            "SecurityControlId": "ACM.1",
            "Parameters": {
              "daysToExpiration": {
                "ValueType": "CUSTOM",
                "Value": {
                  "Integer": 15
                }
              }
            }
          }
        ]
      }
    }
  }
}
```

建立組態政策關聯的 API 請求範例：


```
{
  "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

建立和關聯組態政策

1. 從主區域中的 Security Hub CSPM 委派管理員帳戶執行 [create-configuration-policy](#) 命令。
2. 針對 name，提供組態政策的唯一名稱。或者，對於 description，提供組態政策的描述。
3. 針對 ServiceEnabled 欄位，指定您希望在此組態政策中啟用或停用 Security Hub CSPM。
4. 針對 EnabledStandardIdentifiers 欄位，指定您要在此組態政策中啟用哪些 Security Hub CSPM 標準。
5. 針對 SecurityControlsConfiguration 欄位，指定您要在此組態政策中啟用或停用哪些控制項。選擇 EnabledSecurityControlIdentifiers 表示已啟用指定的控制項。屬於已啟用標準（包括新發佈的控制項）的其他控制項已停用。選擇 DisabledSecurityControlIdentifiers 表示已停用指定的控制項。會啟用適用於已啟用標準（包括新發佈的控制項）的其他控制項。
6. 或者，對於 SecurityControlCustomParameters 欄位，指定您要自訂參數的已啟用控制項。CUSTOM 為 ValueType 欄位提供，並為 Value 欄位提供自訂參數值。此值必須是正確的資料類型，且在 Security Hub CSPM 指定的有效範圍內。僅選取控制項支援自訂參數值。如需詳細資訊，請參閱[了解 Security Hub CSPM 中的控制參數](#)。
7. 若要將組態政策套用至帳戶或 OUs，請從主區域中的 Security Hub CSPM 委派管理員帳戶執行 [start-configuration-policy-association](#) 命令。
8. 針對 configuration-policy-identifier 欄位，提供組態政策的 Amazon Resource Name (ARN) 或 ID。此 ARN 和 ID 由 create-configuration-policy 命令傳回。
9. 針對 target 欄位，提供您要套用此組態政策的 OU、帳戶或根 ID。每次執行命令時只能提供一個目標。所選目標的子項將自動繼承此組態政策，除非它們是自我管理或使用不同的組態政策。

建立組態政策的範例命令：

```
aws securityhub --region us-east-1 create-configuration-policy \
```

```
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
  "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "arn:aws:securityhub::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
  "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}]}}}'
```

建立組態政策關聯的範例命令：

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

StartConfigurationPolicyAssociation API 會傳回名為 `AssociationStatus` 的欄位。此欄位會告訴您政策關聯是待定還是處於成功或失敗狀態。狀態最多可能需要 24 小時才能從 `PENDING` 變更為 `SUCCESS` 或 `FAILURE`。如需關聯狀態的詳細資訊，請參閱 [檢閱組態政策的關聯狀態](#)。

檢閱組態政策的狀態和詳細資訊

委派的 AWS Security Hub CSPM 管理員可以檢視組織的組態政策及其詳細資訊。這包括與政策相關聯的帳戶和組織單位 (OUs)。

如需中央組態優點及其運作方式的背景資訊，請參閱 [了解 Security Hub CSPM 中的中央組態](#)。

選擇您偏好的方法，然後依照步驟檢視您的組態政策。

Security Hub CSPM console

檢視組態政策（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用主要區域中委派 Security Hub CSPM 管理員帳戶的憑證登入。

2. 在導覽窗格中，選擇設定和組態。

3. 選擇政策索引標籤以取得組態政策的概觀。
4. 選取組態政策，然後選擇檢視詳細資訊以查看其相關其他詳細資訊，包括與其相關聯的帳戶和 OUs。

Security Hub CSPM API

若要檢視所有組態政策的摘要清單，請使用 Security Hub CSPM API [ListConfigurationPolicies](#) 的操作。如果您使用 AWS CLI，請執行 [list-configuration-policies](#) 命令。委派的管理員帳戶應該叫用主區域中的操作。

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutLYJHwPn9xnG4hqS0hvw3o2JqjI23QDxdf
```

若要檢視特定組態政策的詳細資訊，請使用 [GetConfigurationPolicy](#) 操作。如果您使用 AWS CLI，請執行 [get-configuration-policy](#)。委派的管理員帳戶應該叫用主區域中的操作。提供您要查看其詳細資訊之組態政策的 Amazon Resource Name (ARN) 或 ID。

```
$ aws securityhub get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

若要檢視所有組態政策及其帳戶關聯的摘要清單，請使用 [ListConfigurationPolicyAssociations](#) 操作。如果您使用 AWS CLI，請執行 [list-configuration-policy-associations](#) 命令。委派的管理員帳戶應該叫用主區域中的操作。或者，您可以提供分頁參數，或依特定政策 ID、關聯類型或關聯狀態篩選結果。

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

若要檢視特定帳戶的關聯，請使用 [GetConfigurationPolicyAssociation](#) 操作。如果您使用 AWS CLI，請執行 [get-configuration-policy-association](#) 命令。委派的管理員帳戶應該叫用主區域中的操作。針對 target，請提供帳戶號碼、OU ID 或根 ID。

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

檢閱組態政策的關聯狀態

下列中央組態 API 操作會傳回名為 的欄位 `AssociationStatus`：

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

當基礎組態是組態政策和自我管理行為時，此欄位都會傳回。

的值 `AssociationStatus` 會告訴您政策關聯是擱置中，還是處於特定帳戶的成功或失敗狀態。狀態最多可能需要 24 小時才能從 變更為 `PENDINGSUCCESS` 或 `FAILED`。狀態 `SUCCESS` 表示組態政策中指定的所有設定都與帳戶相關聯。狀態 `FAILED` 表示組態政策中指定的一或多個設定無法與帳戶建立關聯。儘管 `FAILED` 狀態為，仍可根據政策部分設定帳戶。例如，您可能嘗試將帳戶與啟用 Security Hub CSPM 的組態政策建立關聯，啟用 AWS 基礎安全最佳實務，並停用 CloudTrail.1。最初的兩個設定可能會成功，但 CloudTrail.1 設定可能會失敗。在此範例中，`FAILED` 即使部分設定已正確設定，關聯狀態仍為。

父 OU 或根的關聯狀態取決於其子系的狀態。如果所有子系的關聯狀態為 `SUCCESS`，則父系的關聯狀態為 `SUCCESS`。如果一或多個子系的關聯狀態為 `FAILED`，則父系的關聯狀態為 `FAILED`。

的值 `AssociationStatus` 取決於所有相關區域中政策的關聯狀態。如果關聯在主要區域和所有連結區域中成功，則 的值 `AssociationStatus` 為 `SUCCESS`。如果其中一或多個區域中的關聯失敗，則 的值 `AssociationStatus` 為 `FAILED`。

下列行為也會影響 的值 `AssociationStatus`：

- 如果目標是父系 OU 或根，`FAILED` 則只有在所有子系都有 `SUCCESS` 或 `FAILED` 狀態時，目標才會有 `AssociationStatus SUCCESS` 或。如果在您第一次將父系與組態建立關聯之後，子帳戶或 OU 的關聯狀態變更（例如，新增或移除連結區域時），除非您再次叫用 `StartConfigurationPolicyAssociation` API，否則變更不會更新父系的關聯狀態。
- 如果目標是帳戶，則 `FAILED` 只有在 關聯的結果為 `AssociationStatus SUCCESS` 或在 `FAILED` 主區域和所有連結區域中時，該目標才會有 `SUCCESS` 或。如果目標帳戶的關聯狀態在您第一次將其與組態建立關聯後變更（例如，新增或移除連結區域時），則會更新其關聯狀態。不過，除非您再次叫用 `StartConfigurationPolicyAssociation` API，否則變更不會更新父系的關聯狀態。

如果您新增連結的區域，Security Hub CSPM 會複寫新區域中處於 PENDING、SUCCESS 或 FAILED 狀態的現有關係。

即使關係狀態為 SUCCESS，作為政策一部分的標準啟用狀態也可以轉換為不完整的狀態。在這種情況下，Security Hub CSPM 無法產生標準控制項的問題清單。如需詳細資訊，請參閱[檢查標準的狀態](#)。

對關係失敗進行故障診斷

在 AWS Security Hub CSPM 中，組態政策關係可能會失敗，原因如下。

- Organizations 管理帳戶不是成員 – 如果您想要將組態政策與 Organizations 管理帳戶建立關係，則該帳戶必須已啟用 AWS Security Hub CSPM。這會使管理帳戶成為組織中的成員帳戶。
- AWS Config 未啟用或正確設定 – 若要在組態政策中啟用標準，AWS Config 必須啟用並設定來記錄相關資源。
- 必須從委派管理員帳戶建立關係 – 只有在您登入委派 Security Hub CSPM 管理員帳戶時，才能將政策與目標帳戶和 OUs 建立關係。
- 必須從主要區域建立關係 – 只有在您登入主要區域時，才能將政策與目標帳戶和 OUs 建立關係。
- 未啟用選擇加入區域 – 如果已連結區域中的成員帳戶或 OU 是尚未啟用委派管理員的選擇加入區域，則政策關係會失敗。您可以在從委派的管理員帳戶啟用區域後重試。
- 成員帳戶暫停 – 如果您嘗試將政策與暫停成員帳戶建立關係，政策關係會失敗。

更新組態政策

建立組態政策後，委派的 AWS Security Hub CSPM 管理員帳戶可以更新政策詳細資訊和政策關係。更新政策詳細資訊時，與組態政策相關聯的帳戶會自動開始使用更新的政策。

如需中央組態優點及其運作方式的背景資訊，請參閱[了解 Security Hub CSPM 中的中央組態](#)。

委派管理員可以更新下列政策設定：

- 啟用或停用 Security Hub CSPM。
- 啟用一或多個[安全標準](#)。
- 指出跨已啟用的標準啟用哪些[安全控制](#)。您可以透過提供應啟用的特定控制項清單來執行此操作，Security Hub CSPM 會停用所有其他控制項，包括發行時的新控制項。或者，您可以提供應停用的特定控制項清單，而 Security Hub CSPM 會啟用所有其他控制項，包括發行時的新控制項。
- 或者，[自訂跨已啟用標準啟用之選取控制項的參數](#)。

選擇您偏好的方法，然後依照步驟更新組態政策。

Note

如果您使用中央組態，Security Hub CSPM 會自動停用涉及主要區域以外所有區域中全域資源的控制項。在可用的所有區域中啟用組態政策時，您選擇啟用的其他控制項。若要將這些控制項的問題清單限制為僅一個區域，您可以更新 AWS Config 記錄器設定，並關閉主要區域以外所有區域中的全域資源記錄。

如果主區域不支援涉及全域資源的已啟用控制項，Security Hub CSPM 會嘗試在支援控制項的一個連結區域中啟用控制項。使用中央組態，您缺乏主區域或任何連結區域中無法使用之控制項的涵蓋範圍。

如需涉及全域資源的控制項清單，請參閱 [使用全域資源的控制項](#)。

Console

更新組態政策

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用主要區域中委派 Security Hub CSPM 管理員帳戶的憑證登入。

2. 在導覽窗格中，選擇設定和組態。
3. 選擇 Policies (政策) 標籤。
4. 選取您要編輯的組態政策，然後選擇編輯。如有需要，請編輯政策設定。如果您想要保持政策設定不變，請將本節保持原狀。
5. 選擇下一步。如有需要，請編輯政策關聯。如果您想要讓政策關聯保持不變，請將本節保持不變。更新時，您可以將政策與最多 15 個目標（帳戶、OUs 或根帳戶）建立關聯或取消關聯。
6. 選擇下一步。
7. 檢閱您的變更，然後選擇儲存並套用。在您的主要區域和連結區域中，此動作會覆寫與此組態政策相關聯之帳戶的現有組態設定。帳戶可以透過應用程式或從父節點繼承，與組態政策相關聯。

API

更新組態政策

1. 若要更新組態政策中的設定，請從主區域中的 Security Hub CSPM 委派管理員帳戶叫用 [UpdateConfigurationPolicy](#) API。
2. 提供您要更新的組態政策的 Amazon Resource Name (ARN) 或 ID。
3. 提供下欄位的更新值 ConfigurationPolicy。您也可以選擇性地提供更新的原因。
4. 若要為此組態政策新增關聯，請從主區域中的 Security Hub CSPM 委派管理員帳戶叫用 [StartConfigurationPolicyAssociation](#) API。若要移除一或多個目前的關聯，請從主區域中的 Security Hub CSPM 委派管理員帳戶叫用 [StartConfigurationPolicyDisassociation](#) API。
5. 針對 ConfigurationPolicyIdentifier 欄位，提供您要更新其關聯的組態政策 ARN 或 ID。
6. 針對 Target 欄位，提供您要關聯或取消關聯的帳戶、OUs 或根 ID。此動作會覆寫指定 OUs 或帳戶的先前政策關聯。

Note

當您叫用 UpdateConfigurationPolicy API 時，Security Hub CSPM 會為 EnabledStandardIdentifiers、DisabledSecurityControlIdentifiers、EnabledSecurityControlIdentifiers 和 SecurityControlCustomParameters 欄位執行完整清單取代。每次叫用此 API 時，請提供您要啟用的完整標準清單，以及您要啟用或停用和自訂參數的完整控制項清單。

更新組態政策的 API 請求範例：

```
{
  "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Description": "Updated configuration policy",
  "UpdatedReason": "Disabling CloudWatch.1",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
        "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0",
```



```

        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
    ],
    "SecurityControlsConfiguration": {
        "DisabledSecurityControlIdentifiers": [
            "CloudTrail.2",
            "CloudWatch.1"
        ],
        "SecurityControlCustomParameters": [
            {
                "SecurityControlId": "ACM.1",
                "Parameters": {
                    "daysToExpiration": {
                        "ValueType": "CUSTOM",
                        "Value": {
                            "Integer": 15
                        }
                    }
                }
            }
        ]
    }
}

```

AWS CLI

更新組態政策

1. 若要更新組態政策中的設定，請從主區域中的 Security Hub CSPM 委派管理員帳戶執行 [update-configuration-policy](#) 命令。
2. 提供您要更新的組態政策的 Amazon Resource Name (ARN) 或 ID。
3. 提供 下欄位的更新值 configuration-policy。您也可以選擇性地提供更新的原因。
4. 若要為此組態政策新增關聯，請從主區域中的 Security Hub CSPM 委派管理員帳戶執行 [start-configuration-policy-association](#) 命令。若要移除一或多個目前關聯，請從主區域中的 Security Hub CSPM 委派管理員帳戶執行 [start-configuration-policy-disassociation](#) 命令。
5. 針對 configuration-policy-identifier 欄位，提供您要更新其關聯的組態政策 ARN 或 ID。

- 針對 target 欄位，提供您要關聯或取消關聯的帳戶、OUs 或根 ID。此動作會覆寫指定 OUs 或帳戶的先前政策關聯。

Note

當您執行 update-configuration-policy 命令時，Security Hub CSPM 會為 EnabledStandardIdentifiers、DisabledSecurityControlIdentifiers、EnabledSecurityControlIdentifiers 和 SecurityControlCustomParameters 欄位執行完整清單取代。每次執行此命令時，請提供您要啟用的完整標準清單，以及您要啟用或停用和自訂參數的完整控制項清單。

更新組態政策的範例命令：

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0", "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration": {"DisabledSecurityControlIdentifiers": ["CloudTrail.2", "CloudWatch.1"], "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters": {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}]}}}'
```

StartConfigurationPolicyAssociation API 會傳回名為 的欄位 AssociationStatus。此欄位會告訴您政策關聯是待定還是處於成功或失敗狀態。狀態最多可能需要 24 小時才能從 變更為 PENDINGSUCCESS 或 FAILURE。如需關聯狀態的詳細資訊，請參閱 [檢閱組態政策的關聯狀態](#)。

刪除組態政策

建立組態政策後，委派的 AWS Security Hub CSPM 管理員可以將其刪除。或者，委派管理員可以保留政策，但將其與特定帳戶或組織單位 (OUs) 或根帳戶取消關聯。如需取消政策關聯的指示，請參閱 [取消組態與其目標的關聯](#)。

如需中央組態優點及其運作方式的背景資訊，請參閱 [了解 Security Hub CSPM 中的中央組態](#)。

本節說明如何刪除組態政策。

當您刪除組態政策時，您的組織不會再有該政策。目標帳戶、OUs 和組織根目錄無法再使用組態政策。與已刪除組態政策相關聯的目標會繼承最接近父項的組態政策，或在最接近的父項為自我管理時成為自我管理的目標。如果您希望目標使用不同的組態，您可以將目標與新的組態政策建立關聯。如需詳細資訊，請參閱 [建立和關聯組態政策](#)。

我們建議您建立至少一個組態政策並與您的組織建立關聯，以提供足夠的安全涵蓋範圍。

您必須先取消政策與目前套用的任何帳戶、OUs 或根的關聯，才能刪除組態政策。

選擇您偏好的方法，然後依照步驟刪除組態政策。

Console

刪除組態政策

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用主要區域中委派 Security Hub CSPM 管理員帳戶的登入資料登入。

2. 在導覽窗格中，選擇設定和組態。
3. 選擇 Policies (政策) 標籤。選取您要刪除的組態政策，然後選擇刪除。如果組態政策仍然與任何帳戶或 OUs 相關聯，系統會提示您先取消政策與這些目標的關聯，然後才能將其刪除。
4. 檢閱確認訊息。輸入 **confirm**，然後選擇刪除。

API

刪除組態政策

從主區域中的 Security Hub CSPM 委派管理員帳戶叫用 [DeleteConfigurationPolicy](#) API。

提供您要刪除之組態政策的 Amazon Resource Name (ARN) 或 ID。如果您收到 `ConflictException` 錯誤，則組態政策仍然適用於組織中的帳戶或 OUs。若要解決錯誤，請先取消組態政策與這些帳戶或 OUs 關聯，再嘗試將其刪除。

刪除組態政策的 API 請求範例：

```
{
```

```
"Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

刪除組態政策

從主區域中的 Security Hub CSPM 委派管理員帳戶執行 [delete-configuration-policy](#) 命令。

提供您要刪除之組態政策的 Amazon Resource Name (ARN) 或 ID。如果您收到 `ConflictException` 錯誤，則組態政策仍然適用於組織中的帳戶或 OUs。若要解決錯誤，請先取消組態政策與這些帳戶或 OUs 關聯，再嘗試將其刪除。

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

取消組態與其目標的關聯

從委派的 AWS Security Hub CSPM 管理員帳戶，您可以取消組態政策或自我管理組態與帳戶、OU 或根的關聯。取消關聯會保留政策以供日後使用，但會從特定帳戶、OUs 或根帳戶移除現有的關聯。您只能取消直接套用組態的關聯，而不能取消繼承組態的關聯。若要變更繼承的組態，您可以將組態政策或自我管理行為套用至受影響的帳戶或 OU。您也可以將包含所需修改的新組態政策套用至最近的父系。

取消關聯不會刪除組態政策。政策會保留在您的帳戶中，因此您可以將其與組織中的其他目標建立關聯。如需刪除組態政策的指示，請參閱 [刪除組態政策](#)。當取消關聯完成時，受影響的目標會繼承最接近父項的組態政策或自我管理行為。如果沒有可繼承的組態，目標會在取消關聯之前保留其設定，但會成為自我管理。

選擇您偏好的方法，並依照步驟取消帳戶、OU 或根與其目前組態的關聯。

Console

取消帳戶或 OU 與其目前組態的關聯

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。

使用主要區域中委派 Security Hub CSPM 管理員帳戶的登入資料登入。

2. 在導覽窗格中，選擇設定和組態。
3. 在組織索引標籤上，選取要與目前組態取消關聯的帳戶、OU 或根目錄。選擇編輯。
4. 在定義組態頁面上，針對管理，如果您希望委派管理員能夠將政策直接套用至目標，請選擇套用的政策。如果您希望目標繼承其最近父系的組態，請選擇繼承。在這些情況下，委派管理員會控制目標的設定。如果您希望帳戶或 OU 控制自己的設定，請選擇自我管理。
5. 檢閱您的變更後，選擇下一步並套用。如果這些組態與您目前的選擇衝突，此動作會覆寫範圍內任何帳戶或 OUs 的現有組態。

API

取消帳戶或 OU 與其目前組態的關聯

1. 從主區域中的 Security Hub CSPM 委派管理員帳戶叫用 [StartConfigurationPolicyDisassociation](#) API。
2. 針對 ConfigurationPolicyIdentifier，提供您要取消關聯的組態政策的 Amazon Resource Name (ARN) 或 ID。SELF_MANAGED_SECURITY_HUB 提供此欄位以取消自我管理行為的關聯。
3. 針對 Target，提供您要與此組態政策取消關聯的帳戶、OUs 或根帳戶。

取消組態政策關聯的 API 請求範例：

```
{
  "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

取消帳戶或 OU 與其目前組態的關聯

1. 從主區域中的 Security Hub CSPM 委派管理員帳戶執行 [start-configuration-policy-disassociation](#) 命令。

2. 針對 `configuration-policy-identifier`，提供您要取消關聯的組態政策的 Amazon Resource Name (ARN) 或 ID。SELF_MANAGED_SECURITY_HUB 提供此欄位以取消自我管理行為的關聯。
3. 針對 `target`，提供您要與此組態政策取消關聯的帳戶、OUs 或根帳戶。

取消組態政策關聯的命令範例：

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

在內容中設定標準或控制項

當您在 AWS Security Hub CSPM 中使用 [中央組態](#) 時，委派的 Security Hub CSPM 管理員可以建立組態政策，以指定如何為組織設定 Security Hub CSPM、安全標準和安全控制。委派管理員可以將政策與特定帳戶和組織單位 (OU) 建立關聯。這些政策在您的主要區域和所有連結區域中生效。委派管理員可以視需要更新組態政策。

在 Security Hub CSPM 主控台上，委派管理員可以透過兩種方式更新組態政策：從組態頁面或現有工作流程的內容。後者可能很有幫助，因為當您檢視安全調查結果時，您可以探索哪些標準和控制項與您的環境最相關，並同時進行設定。

內容內組態僅適用於 Security Hub CSPM 主控台。委派管理員必須以程式設計方式叫用 Security Hub CSPM API [UpdateConfigurationPolicy](#) 的操作，以變更組織中設定特定標準或控制項的方式。

請依照下列步驟，在內容中設定 Security Hub CSPM 標準或控制項。

在內容中設定標準或控制項（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用主要區域中委派 Security Hub CSPM 管理員帳戶的憑證登入。

2. 在導覽窗格中，選擇下列其中一個選項：

- 若要設定標準，請選擇安全標準，然後選擇特定標準。
- 若要設定控制項，請選擇控制項，然後選擇特定控制項。

3. 主控台會列出您現有的 Security Hub CSPM 組態政策，以及每個政策中所選標準或控制項的狀態。選擇選項以啟用或停用每個現有組態政策中的標準或控制項。對於控制項，您也可以選擇自訂[控制項參數](#)。您無法在內容內組態期間建立新的政策。若要建立新的政策，您必須前往組態頁面，選擇政策索引標籤，然後選擇建立政策。
4. 進行變更後，請選擇下一步。
5. 檢閱您的變更，然後選擇套用。更新會影響與已變更組態政策相關聯的所有帳戶和 OUs。更新也會在主要區域和所有連結區域中生效。

在 Security Hub CSPM 中停用中央組態

當您在 AWS Security Hub CSPM 中停用中央組態時，委派管理員將無法跨多個組織單位 (OUs) 和設定 Security Hub CSPM AWS 帳戶、安全標準和安全控制 AWS 區域。相反地，您必須為每個區域中的每個帳戶分別設定大多數設定。

Important

在停用中央組態之前，您必須先[取消帳戶和 OUs 與其目前組態的關聯](#)，無論是組態政策還是自我管理行為。

您必須先[刪除現有的組態政策](#)，才能停用中央組態。

當您停用中央組態時，會發生下列變更：

- 委派管理員無法再為組織建立組態政策。
- 已套用或繼承組態政策的帳戶會保留其目前的設定，但會自我管理。
- 您的組織會切換到本機組態。在本機組態下，大多數 Security Hub CSPM 設定都必須在每個組織帳戶和區域中分別設定。委派管理員可以選擇自動啟用 Security Hub CSPM、[預設安全標準](#)，以及屬於新組織帳戶中預設標準一部分的所有控制項。預設標準為 AWS 基礎安全最佳實務 (FSBP) 和網際網路安全中心 (CIS) AWS Foundations Benchmark 1.2.0 版。這些設定只會在目前區域中生效，並且只會影響新的組織帳戶。委派管理員無法變更預設的標準。本機組態不支援在 OU 層級使用組態政策或組態。

當您停止使用中央組態時，委派管理員帳戶的身分會保持不變。您的主要區域和連結區域也保持不變（您的主要區域現在稱為彙總區域，可用於尋找彙總）。

選擇您偏好的方法，然後依照步驟停用中央組態並切換到本機組態。

Security Hub CSPM console

停用中央組態 (主控台)

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用主要區域中委派 Security Hub CSPM 管理員帳戶的憑證登入。

2. 在導覽窗格中，選擇設定和組態。
3. 在概觀區段中，選擇編輯。
4. 在編輯組織組態方塊中，選擇本機組態。如果您還沒有，系統會提示您取消關聯並刪除目前的組態政策，然後才能停止中央組態。指定為自我管理的帳戶或 OUs 必須與其自我管理組態取消關聯。您可以在主控台中執行此操作，方法是[將每個自我管理帳戶或 OU 的管理類型變更](#)為集中管理和從我的組織繼承。
5. 或者，選取新組織帳戶的本機組態設定。
6. 選擇確認。

Security Hub CSPM API

停用中央組態 (API)

1. 叫用 [UpdateOrganizationConfiguration](#) API。
2. 將 OrganizationConfiguration 物件中的 ConfigurationType 欄位設定為 LOCAL。如果您有現有的組態政策或政策關聯，API 會傳回錯誤。若要取消關聯組態政策，請叫用 StartConfigurationPolicyDisassociation API。若要刪除組態政策，請叫用 DeleteConfigurationPolicy API。
3. 如果您想要在新的組織帳戶中自動啟用 Security Hub CSPM，請將 AutoEnable 欄位設定為 true。根據預設，此欄位的值為 false，且 Security Hub CSPM 不會在新的組織帳戶中自動啟用。或者，如果您想要在新的組織帳戶中自動啟用預設安全標準，請將 AutoEnableStandards 欄位設定為 DEFAULT。這是預設值。如果您不想在新的組織帳戶中自動啟用預設安全標準，請將 AutoEnableStandards 欄位設定為 NONE。

範例 API 請求：

```
{
  "AutoEnable": true,
  "OrganizationConfiguration": {
```



```
    "ConfigurationType" : "LOCAL"  
  }  
}
```

AWS CLI

停用中央組態 (AWS CLI)

1. 執行 [update-organization-configuration](#) 命令。
2. 將 organization-configuration 物件中的 ConfigurationType 欄位設定為 LOCAL。如果您有現有的組態政策或政策關聯，命令會傳回錯誤。若要取消與組態政策的關聯，請執行 start-configuration-policy-disassociation 命令。若要刪除組態政策，請執行 delete-configuration-policy 命令。
3. 如果您想要在新的組織帳戶中自動啟用 Security Hub CSPM，請包含 auto-enable 參數。根據預設，此參數的值為 no-auto-enable，且 Security Hub CSPM 不會在新組織帳戶中自動啟用。或者，如果您想要在新的組織帳戶中自動啟用預設安全標準，請將 auto-enable-standards 欄位設定為 DEFAULT。這是預設值。如果您不想在新的組織帳戶中自動啟用預設安全標準，請將 auto-enable-standards 欄位設定為 NONE。

```
aws securityhub --region us-east-1 update-organization-configuration \  
--auto-enable \  
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

在 Security Hub CSPM 中管理管理員和成員帳戶

如果您的 AWS 環境有多個帳戶，您可以將使用 AWS Security Hub CSPM 的帳戶視為成員帳戶，並將其與單一管理員帳戶建立關聯。管理員可以監控您的整體安全狀態，並對成員帳戶採取[允許的動作](#)。管理員也可以大規模執行各種帳戶管理和管理任務，例如監控預估用量成本和評估帳戶配額。

您可以透過兩種方式將 Security Hub CSPM 與管理員建立關聯，AWS Organizations 或在 Security Hub CSPM 中手動傳送和接受成員邀請。

使用 管理帳戶 AWS Organizations

AWS Organizations 是一種全域帳戶管理服務，可讓 AWS 管理員合併和管理多個 AWS 帳戶。它提供帳戶管理和合併帳單功能，旨在支援預算、安全和合規需求。它免費提供，並與多個整合 AWS 服

務，包括 AWS Security Hub CSPM、Amazon Macie 和 Amazon GuardDuty。如需詳細資訊，請參閱 [「AWS Organizations 使用者指南」](#)。

當您整合 Security Hub CSPM 和 時 AWS Organizations，Organizations 管理帳戶會指定 Security Hub CSPM 委派管理員。Security Hub CSPM 會在 AWS 區域 指定的 中的委派管理員帳戶中自動啟用。

指定委派管理員之後，建議您使用[中央組態](#)來管理 Security Hub CSPM 中的帳戶。這是自訂 Security Hub CSPM 並確保為您的組織提供足夠安全涵蓋範圍的最有效方法。

中央組態可讓委派管理員跨多個組織帳戶和區域自訂 Security Hub CSPM，而不是 Region-by-Region 設定。您可以為整個組織建立組態政策，或為不同的帳戶和 OUs 建立不同的組態政策。這些政策指定在關聯帳戶中啟用或停用 Security Hub CSPM，以及啟用了哪些安全標準和控制項。

委派管理員可以將帳戶指定為集中管理或自我管理。集中受管帳戶只能由委派管理員設定。自我管理帳戶可以指定自己的設定。

如果您不選擇加入中央組態，委派管理員具有更有限的能力來設定 Security Hub CSPM，稱為本機組態。在本機組態下，委派管理員可以在目前區域中的新組織帳戶中自動啟用 Security Hub CSPM 和[預設安全標準](#)。不過，現有帳戶不會使用這些設定，因此組態偏離可能會在帳戶加入組織之後發生。

除了這些新帳戶設定之外，本機組態是帳戶特定和區域特定。每個組織帳戶都必須在每個區域中分別設定 Security Hub CSPM 服務、標準和控制項。本機組態也不支援使用組態政策。

透過邀請手動管理帳戶

如果您有獨立帳戶或未與 Organizations 整合，則必須在 Security Hub CSPM 中透過邀請手動管理成員帳戶。獨立帳戶無法與 Organizations 整合，因此需要手動管理它。如果您未來新增其他帳戶，建議您與 整合 AWS Organizations 並使用中央組態。

當您使用手動帳戶管理時，您可以將帳戶指定為 Security Hub CSPM 管理員。管理員帳戶可以檢視成員帳戶中的資料，並對成員帳戶調查結果採取特定動作。Security Hub CSPM 管理員邀請其他帳戶成為成員帳戶，並在潛在成員帳戶接受邀請時建立管理員成員關係。

手動帳戶管理不支援使用組態政策。如果沒有組態政策，管理員就無法透過設定不同帳戶的變數設定來集中自訂 Security Hub CSPM。相反地，每個組織帳戶都必須在每個區域中分別啟用和設定 Security Hub CSPM。這可能會讓確保您在使用 Security Hub CSPM 的所有帳戶和區域擁有足夠的安全涵蓋範圍變得更加困難和耗時。它也可能導致組態偏離，因為成員帳戶可以指定自己的設定，而無需管理員輸入。

若要依邀請管理帳戶，請參閱 [在 Security Hub CSPM 中透過邀請管理帳戶](#)。

在 Security Hub CSPM 中管理多個帳戶的建議

下一節摘要說明在 AWS Security Hub CSPM 中管理成員帳戶時應謹記的一些限制和建議。

成員帳戶的數目上限

如果您使用 整合 AWS Organizations，Security Hub CSPM 在每個 中支援每個委派管理員帳戶最多 10,000 個成員帳戶 AWS 區域。如果您手動啟用和管理 Security Hub CSPM，Security Hub CSPM 支援每個區域中每個管理員帳戶最多 1,000 個成員帳戶邀請。

建立管理員成員關係

Note

如果您使用 Security Hub CSPM 整合 AWS Organizations，且尚未手動邀請任何成員帳戶，則本節不適用於您。

帳戶不能同時是管理員帳戶和成員帳戶。

成員帳戶只能與一個管理員帳戶建立關聯。如果組織帳戶由 Security Hub CSPM 管理員帳戶啟用，則帳戶無法接受來自另一個帳戶的邀請。如果帳戶已接受邀請，則組織的 Security Hub CSPM 管理員帳戶無法啟用該帳戶。它也無法接收來自其他帳戶的邀請。

對於手動邀請程序，接受成員資格邀請是選用的。

透過 成為成員 AWS Organizations

如果您將 Security Hub CSPM 與 整合 AWS Organizations，則 Organizations 管理帳戶可以為 Security Hub CSPM 指定委派管理員 (DA) 帳戶。組織管理帳戶無法在 Organizations 中設定為 DA。雖然 Security Hub CSPM 允許這樣做，但我們建議 Organizations 管理帳戶不應是 DA。

建議您在所有區域中選擇相同的 DA 帳戶。如果您使用 [中央組態](#)，則 Security Hub CSPM 會在您為組織設定 Security Hub CSPM 的所有區域中設定相同的 DA 帳戶。

我們也建議您跨 AWS 安全與合規服務選擇相同的 DA 帳戶，協助您在單一面板中管理安全相關問題。

邀請加入

對於透過邀請建立的成員帳戶，管理員-成員帳戶關聯只會在傳送邀請的區域中建立。管理員帳戶必須在您要使用它的每個區域中啟用 Security Hub CSPM。管理員帳戶接著會邀請每個帳戶成為該區域中的成員帳戶。

 Note

我們建議您使用 AWS Organizations 而非 Security Hub CSPM 邀請來管理您的成員帳戶。

協調跨 服務的管理員帳戶

Security Hub CSPM 彙總各種 AWS 服務的問題清單，例如 Amazon GuardDuty、Amazon Inspector 和 Amazon Macie。Security Hub CSPM 也允許使用者從 GuardDuty 調查結果進行樞紐分析，以在 Amazon Detective 中開始調查。

不過，您在這些其他服務中設定的管理員成員關係不會自動套用至 Security Hub CSPM。Security Hub CSPM 建議您在所有這些服務中使用與管理員帳戶相同的帳戶。此管理員帳戶應該是負責安全工具的帳戶。相同的帳戶也應該是 的彙總工具帳戶 AWS Config。

例如，GuardDuty 管理員帳戶 A 的使用者可以在 GuardDuty 主控台上查看 GuardDuty 成員帳戶 B 和 C 的問題清單。如果帳戶 A 接著啟用 Security Hub CSPM，帳戶 A 的使用者不會在 Security Hub CSPM 中自動查看帳戶 B 和 C 的 GuardDuty 調查結果。這些帳戶也需要 Security Hub CSPM 管理員成員關係。

若要這樣做，請將帳戶 A 設為 Security Hub CSPM 管理員帳戶，並讓帳戶 B 和 C 成為 Security Hub CSPM 成員帳戶。

使用 管理多個帳戶的 Security Hub CSPM AWS Organizations

您可以將 AWS Security Hub CSPM 與 整合 AWS Organizations，然後管理組織中帳戶的 Security Hub CSPM。

若要將 Security Hub CSPM 與 整合 AWS Organizations，您可以在其中建立組織 AWS Organizations。Organizations 管理帳戶會將一個帳戶指定為組織的 Security Hub CSPM 委派管理員。委派管理員接著可以為組織中的其他帳戶啟用 Security Hub CSPM，將這些帳戶新增為 Security Hub CSPM 成員帳戶，並對成員帳戶採取允許的動作。Security Hub CSPM 委派管理員最多可為 10,000 個成員帳戶啟用和管理 Security Hub CSPM。

委派管理員的組態功能範圍取決於您是否使用[中央組態](#)。啟用中央組態後，您不需要在每個成員帳戶和 中分別設定 Security Hub CSPM AWS 區域。委派管理員可以跨區域在指定的成員帳戶和組織單位 (OUs) 中強制執行特定 Security Hub CSPM 設定。

Security Hub CSPM 委派管理員帳戶可以對成員帳戶執行下列動作：

- 如果使用中央組態，請透過建立 Security Hub CSPM 組態政策，集中設定成員帳戶和 OUs 的 Security Hub CSPM。組態政策可用來啟用和停用 Security Hub CSPM、啟用和停用標準，以及啟用和停用控制項。
- 加入組織時，自動將新帳戶視為 Security Hub CSPM 成員帳戶。如果您使用中央組態，則與 OU 相關聯的組態政策會包含屬於 OU 一部分的現有和新帳戶。
- 將現有的組織帳戶視為 Security Hub CSPM 成員帳戶。如果您使用中央組態，則會自動發生這種情況。
- 取消關聯屬於組織的成員帳戶。如果您使用中央組態，只有在將成員帳戶指定為自我管理之後，才能取消其關聯。或者，您可以將停用 Security Hub CSPM 的組態政策與特定集中管理的成員帳戶建立關聯。

如果您不選擇加入中央組態，您的組織會使用稱為本機組態的預設組態類型。在本機組態下，委派管理員在成員帳戶中強制執行設定的能力更有限。如需詳細資訊，請參閱[了解 Security Hub CSPM 中的本機組態](#)。

如需委派管理員可在成員帳戶上執行之動作的完整清單，請參閱[Security Hub CSPM 中管理員和成員帳戶允許的動作](#)。

本節中的主題說明如何將 Security Hub CSPM 與 整合，AWS Organizations 以及如何管理組織中帳戶的 Security Hub CSPM。在相關的情況下，每個區段都會識別集中組態使用者的管理優點和差異。

主題

- [將 Security Hub CSPM 與 整合 AWS Organizations](#)
- [在新的組織帳戶中自動啟用 Security Hub CSPM](#)
- [在新的組織帳戶中手動啟用 Security Hub CSPM](#)
- [取消 Security Hub CSPM 成員帳戶與組織的關聯](#)

將 Security Hub CSPM 與 整合 AWS Organizations

若要整合 AWS Security Hub CSPM 和 AWS Organizations，您可以在 Organizations 中建立組織，並使用組織管理帳戶來指定委派的 Security Hub CSPM 管理員帳戶。這可讓 Security Hub CSPM 成為 Organizations 中信任的服務。它還在委派管理員帳戶的目前 AWS 區域中啟用 Security Hub CSPM，並允許委派管理員為成員帳戶啟用 Security Hub CSPM、檢視成員帳戶中的資料，以及在成員帳戶上執行其他[允許的動作](#)。

如果您使用[中央組態](#)，則委派管理員也可以建立 Security Hub CSPM 組態政策，指定如何在組織帳戶中設定 Security Hub CSPM 服務、標準和控制項。

建立組織

組織是您建立來合併的實體，AWS 帳戶讓您可以以單一單位管理它們。

您可以使用 AWS Organizations 主控台或使用來自 AWS CLI 或其中一個 SDK APIs 命令來建立組織。如需詳細說明，請參閱 AWS Organizations 《使用者指南》中的[建立組織](#)。

您可以使用 AWS Organizations 集中檢視和管理組織內的所有帳戶。組織具有一個管理帳戶，以及零個或多個成員帳戶。您可以在階層式樹狀結構中組織帳戶，其根位於根目錄頂端，而組織單位 (OUs) 巢狀在根目錄下。每個帳戶可以直接在根目錄下，或放置在階層中的其中一個 OUs 中。OU 是特定帳戶的容器。例如，您可以建立財務 OU，其中包含與財務操作相關的所有帳戶。

選擇委派 Security Hub CSPM 管理員的建議

如果您擁有來自手動邀請程序的管理員帳戶，並正使用轉換至帳戶管理 AWS Organizations，我們建議您將該帳戶指定為委派的 Security Hub CSPM 管理員。

雖然 Security Hub CSPM APIs 和主控台允許組織管理帳戶成為委派的 Security Hub CSPM 管理員，但我們建議您選擇兩個不同的帳戶。這是因為有權存取組織管理帳戶來管理帳單的使用者，可能與需要存取 Security Hub CSPM 以進行安全管理的使用者不同。

我們建議跨區域使用相同的委派管理員。如果您選擇加入中央組態，Security Hub CSPM 會自動在您的主要區域和任何連結區域中指定相同的委派管理員。

驗證設定委派管理員的許可

若要指定和移除委派的 Security Hub CSPM 管理員帳戶，組織管理帳戶必須具有 Security Hub CSPM 中 `EnableOrganizationAdminAccount` 和 `DisableOrganizationAdminAccount` 動作的許可。Organizations 管理帳戶也必須具有 Organizations 的管理許可。

若要授予所有必要的許可，請將下列 Security Hub CSPM 受管政策連接至組織管理帳戶的 IAM 主體：

- [AWSSecurityHubFullAccess](#)
- [AWSSecurityHubOrganizationsAccess](#)

指定委派管理員

若要指定委派的 Security Hub CSPM 管理員帳戶，您可以使用 Security Hub CSPM 主控台、Security Hub CSPM API 或 AWS CLI。Security Hub CSPM AWS 區域 只會在目前的 中設定委派管理員，您必

須在其他區域中重複 動作。如果您開始使用中央組態，Security Hub CSPM 會自動在主要區域和連結區域中設定相同的委派管理員。

組織管理帳戶不需要啟用 Security Hub CSPM，即可指定委派的 Security Hub CSPM 管理員帳戶。

我們建議組織管理帳戶不是委派的 Security Hub CSPM 管理員帳戶。不過，如果您選擇組織管理帳戶做為 Security Hub CSPM 委派管理員，則管理帳戶必須啟用 Security Hub CSPM。如果管理帳戶未啟用 Security Hub CSPM，您必須手動為其啟用 Security Hub CSPM。無法自動為組織管理帳戶啟用 Security Hub CSPM。

您必須使用下列其中一種方法來指定委派的 Security Hub CSPM 管理員。使用 Organizations APIs 指定委派的 Security Hub CSPM 管理員不會反映在 Security Hub CSPM 中。

選擇您偏好的方法，然後依照步驟指定委派的 Security Hub CSPM 管理員帳戶。

Security Hub CSPM console

在加入時指定委派管理員

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 選擇移至 Security Hub CSPM。系統會提示您登入組織管理帳戶。
3. 在指定委派管理員頁面上，於委派管理員帳戶區段中，指定委派管理員帳戶。我們建議您選擇已為其他 AWS 安全與合規服務設定的相同委派管理員。
4. 選擇設定委派管理員。系統會提示您登入委派管理員帳戶（如果您尚未登入），以繼續加入中央組態。如果您不想啟動中央組態，請選擇取消。您的委派管理員已設定，但您尚未使用中央組態。

從設定頁面指定委派管理員

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在 Security Hub CSPM 導覽窗格中，選擇設定。然後選擇一般。
3. 如果目前已指派 Security Hub CSPM 管理員帳戶，則您必須先移除目前的帳戶，才能指定新帳戶。

在委派管理員下，若要移除目前帳戶，請選擇移除。

4. 輸入您要指定為 Security Hub CSPM 管理員帳戶的帳戶 ID。

您必須在所有區域中指定相同的 Security Hub CSPM 管理員帳戶。如果您指定的帳戶與其他區域中指定的帳戶不同，主控台會傳回錯誤。

5. 選擇委派。

Security Hub CSPM API, AWS CLI

從組織管理帳戶，使用 Security Hub CSPM API [EnableOrganizationAdminAccount](#) 的操作。如果您使用的是 AWS CLI，請執行 [enable-organization-admin-account](#) 命令。提供委派 Security Hub CSPM 管理員的 AWS 帳戶 ID。

下列範例會指定委派的 Security Hub CSPM 管理員。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

移除或變更委派管理員

只有組織管理帳戶可以移除委派的 Security Hub CSPM 管理員帳戶。

若要變更委派的 Security Hub CSPM 管理員，您必須先移除目前的委派管理員帳戶，然後指定新的管理員帳戶。

Warning

當您使用 [中央組態](#) 時，無法使用 Security Hub CSPM 主控台或 Security Hub CSPM APIs 來變更或移除委派的管理員帳戶。如果組織管理帳戶使用 AWS Organizations 主控台或 AWS Organizations APIs 來變更或移除委派的 Security Hub CSPM 管理員，Security Hub CSPM 會自動停止中央組態，並刪除您的組態政策和政策關聯。成員帳戶會保留在委派管理員變更或移除之前所擁有的組態。

如果您使用 Security Hub CSPM 主控台移除一個區域中的委派管理員，則會在所有區域中自動移除。

Security Hub CSPM API 只會從發出 API 呼叫或命令的區域移除委派的 Security Hub CSPM 管理員帳戶。您必須在其他區域中重複動作。

如果您使用 Organizations API 移除委派的 Security Hub CSPM 管理員帳戶，則會在所有區域中自動移除。

移除委派管理員 (Organizations API AWS CLI)

您可以使用 Organizations 移除所有區域中的委派 Security Hub CSPM 管理員。

如果您使用中央組態來管理帳戶，移除委派的管理員帳戶會導致刪除您的組態政策和政策關聯。成員帳戶會保留他們在委派管理員變更或移除之前所擁有的組態。不過，這些帳戶無法再由已移除的委派管理員帳戶管理。它們成為自我管理帳戶，必須在每個區域中分別設定。

選擇您偏好的方法，並依照指示移除委派的 Security Hub CSPM 管理員帳戶 AWS Organizations。

Organizations API, AWS CLI

移除委派的 Security Hub CSPM 管理員

從組織管理帳戶，使用 Organizations API [DeregisterDelegatedAdministrator](#) 的操作。如果您使用的是 AWS CLI，請執行 [deregister-delegated-administrator](#) 命令。提供委派管理員的帳戶 ID，以及 Security Hub CSPM 的服務主體，也就是 `securityhub.amazonaws.com`。

下列範例會移除委派的 Security Hub CSPM 管理員。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --  
service-principal securityhub.amazonaws.com
```

移除委派管理員 (Security Hub CSPM 主控台)

您可以使用 Security Hub CSPM 主控台移除所有區域中的委派 Security Hub CSPM 管理員。

移除委派的 Security Hub CSPM 管理員帳戶時，成員帳戶會與移除的委派 Security Hub CSPM 管理員帳戶取消關聯。

成員帳戶中仍然啟用 Security Hub CSPM。它們會成為獨立帳戶，直到新的 Security Hub CSPM 管理員將其啟用為成員帳戶為止。

如果組織管理帳戶不是 Security Hub CSPM 中已啟用的帳戶，請使用歡迎使用 Security Hub CSPM 頁面上的選項。

從歡迎使用 Security Hub CSPM 頁面移除委派的 Security Hub CSPM 管理員帳戶

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 選擇移至 Security Hub。

3. 在委派管理員下，選擇移除。

如果組織管理帳戶是 Security Hub 中已啟用的帳戶，請使用設定頁面一般索引標籤上的 選項。

從設定頁面移除委派的 Security Hub CSPM 管理員帳戶

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在 Security Hub CSPM 導覽窗格中，選擇設定。然後選擇一般。
3. 在委派管理員下，選擇移除。

移除委派管理員 (Security Hub CSPM API AWS CLI)

您可以使用 Security Hub CSPM API 或 Security Hub CSPM 操作 AWS CLI 來移除委派的 Security Hub CSPM 管理員。當您使用其中一種方法移除委派管理員時，只會在發出 API 呼叫或命令的區域中將其移除。Security Hub CSPM 不會更新其他區域，也不會移除其中的委派管理員帳戶 AWS Organizations。

選擇您偏好的方法，然後依照下列步驟，使用 Security Hub CSPM 移除委派的 Security Hub CSPM 管理員帳戶。

Security Hub CSPM API, AWS CLI

移除委派的 Security Hub CSPM 管理員

從組織管理帳戶，使用 Security Hub CSPM API [DisableOrganizationAdminAccount](#) 的操作。如果您使用的是 AWS CLI，請執行 [disable-organization-admin-account](#) 命令。提供委派 Security Hub CSPM 管理員的帳戶 ID。

下列範例會移除委派的 Security Hub CSPM 管理員。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

停用 Security Hub CSPM 與 整合 AWS Organizations

AWS Organizations 組織與 AWS Security Hub CSPM 整合後，Organizations 管理帳戶隨後可以停用整合。身為 Organizations 管理帳戶的使用者，您可以停用 Security Hub CSPM 的受信任存取權來執行此操作 AWS Organizations。

當您停用 Security Hub CSPM 的受信任存取時，會發生下列情況：

- Security Hub CSPM 失去其信任服務的狀態 AWS Organizations。
- Security Hub CSPM 委派管理員帳戶會失去所有 Security Hub CSPM 成員帳戶對 Security Hub CSPM 設定、資料和資源的存取權 AWS 區域。
- 如果您使用的是[中央組態](#)，Security Hub CSPM 會自動停止將其用於您的組織。您的組態政策和政策關聯會遭到刪除。帳戶會保留在您停用受信任存取之前所擁有的組態。
- 所有 Security Hub CSPM 成員帳戶都會成為獨立帳戶，並保留其目前的設定。如果已在一或多個區域中為成員帳戶啟用 Security Hub CSPM，則會繼續為這些區域中的帳戶啟用 Security Hub CSPM。啟用的標準和控制項也保持不變。您可以在每個帳戶和區域中分別變更這些設定。不過，帳戶不會再與任何區域中的委派管理員建立關聯。

如需停用受信任服務存取結果的詳細資訊，請參閱AWS Organizations 《使用者指南》中的[將 AWS Organizations 與其他 AWS 服務 搭配使用](#)。

若要停用受信任存取，您可以使用 AWS Organizations 主控台、Organizations API 或 AWS CLI。只有 Organizations 管理帳戶的使用者可以停用 Security Hub CSPM 的受信任服務存取。如需所需許可的詳細資訊，請參閱AWS Organizations 《使用者指南》中的[停用受信任存取所需的許可](#)。

在您停用受信任存取之前，建議您與組織的委派管理員合作，以停用成員帳戶中的 Security Hub CSPM，並清除這些帳戶中的 Security Hub CSPM 資源。

選擇您偏好的方法，並依照步驟停用 Security Hub CSPM 的受信任存取。

Organizations console

停用 Security Hub CSPM 的受信任存取

1. AWS 管理主控台 使用 AWS Organizations 管理帳戶的登入資料登入。
2. 在 <https://console.aws.amazon.com/organizations/> 開啟 Organizations 主控台。
3. 在導覽窗格中，選擇服務。
4. 在整合式服務下，選擇 AWS Security Hub CSPM。
5. 選擇停用受信任的存取。
6. 確認您要停用信任的存取。

Organizations API

停用 Security Hub CSPM 的受信任存取

叫用 AWS Organizations API 的 [DisableAWSServiceAccess](#) 操作。針對 ServicePrincipal 參數，指定 Security Hub CSPM 服務主體 (securityhub.amazonaws.com)。

AWS CLI

停用 Security Hub CSPM 的受信任存取

執行 AWS Organizations API 的 [disable-aws-service-access](#) 命令。針對 service-principal 參數，指定 Security Hub CSPM 服務主體 (securityhub.amazonaws.com)。

範例：

```
aws organizations disable-aws-service-access --service-principal
securityhub.amazonaws.com
```

在新的組織帳戶中自動啟用 Security Hub CSPM

當新帳戶加入您的組織時，它們會新增至 AWS Security Hub CSPM 主控台帳戶頁面上的清單。針對組織帳戶，類型為依組織。根據預設，新帳戶在加入組織時不會成為 Security Hub CSPM 成員。他們的狀態為非成員。委派的管理員帳戶可以自動將新帳戶新增為成員，並在這些帳戶加入組織時啟用 Security Hub CSPM。

Note

雖然您的預設為 AWS 區域啟用許多 AWS 帳戶，但您必須手動啟用特定區域。這些區域在本文件中稱為選擇加入區域。若要在選擇加入區域中的新帳戶中自動啟用 Security Hub CSPM，帳戶必須先啟用該區域。只有帳戶擁有者可以啟用選擇加入區域。如需選擇加入區域的詳細資訊，請參閱[指定 AWS 區域 您的帳戶可以使用哪些區域](#)。

此程序會根據您使用的是中央組態（建議）或本機組態而有所不同。

自動啟用新的組織帳戶（中央組態）

如果您使用[中央組態](#)，您可以透過建立啟用 Security Hub CSPM 的組態政策，在新的和現有的組織帳戶中自動啟用 Security Hub CSPM。然後，您可以將政策與組織根或特定組織單位 (OUs) 建立關聯。

如果您將啟用 Security Hub CSPM 的組態政策與特定 OU 建立關聯，Security Hub CSPM 會在屬於該 OU 的所有帳戶（現有和新的）中自動啟用。不屬於 OU 的新帳戶是自我管理的，不會自動啟用 Security Hub CSPM。如果您將啟用 Security Hub CSPM 的組態政策與根建立關聯，則會在加入組織的所有帳戶（現有和新的）中自動啟用 Security Hub CSPM。例外狀況是帳戶透過應用程式或繼承使用不同的政策，或自我管理。

在您的組態政策中，您也可以定義應該在 OU 中啟用哪些安全標準和控制項。若要產生已啟用標準的控制調查結果，OU 中的帳戶必須 AWS Config 已啟用並設定以記錄必要的資源。如需 AWS Config 錄製的詳細資訊，請參閱[啟用和設定 AWS Config](#)。

如需建立組態政策的說明，請參閱[建立和關聯組態政策](#)。

自動啟用新的組織帳戶（本機組態）

當您使用本機組態並開啟預設標準的自動啟用時，Security Hub CSPM 會將新的組織帳戶新增為成員，並在目前區域中啟用 Security Hub CSPM。其他區域不受影響。此外，開啟自動啟用不會在現有組織帳戶中啟用 Security Hub CSPM，除非它們已新增為成員帳戶。

開啟自動啟用後，當新成員帳戶加入組織時，會為目前區域中的新成員帳戶啟用預設安全標準。預設標準是 AWS 基礎安全最佳實務 (FSBP) 和網際網路安全中心 (CIS) AWS Foundations Benchmark 1.2.0 版。您無法變更預設標準。如果您想要在整個組織中啟用其他標準，或啟用特定帳戶和 OUs 的標準，我們建議您使用中央組態。

若要產生預設標準（和其他啟用的標準）的控制調查結果，組織中的帳戶必須 AWS Config 啟用並設定，以記錄所需的資源。如需 AWS Config 錄製的詳細資訊，請參閱[啟用和設定 AWS Config](#)。

選擇您偏好的方法，並依照步驟在新的組織帳戶中自動啟用 Security Hub CSPM。這些指示僅適用於您使用本機組態的情況。

Security Hub CSPM console

以 Security Hub CSPM 成員身分自動啟用新的組織帳戶

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

Sign 使用委派管理員帳戶的登入資料。

2. 在 Security Hub CSPM 導覽窗格中的設定下，選擇組態。
3. 在帳戶區段中，開啟自動啟用帳戶。

Security Hub CSPM API

以 Security Hub CSPM 成員身分自動啟用新的組織帳戶

從委派管理員帳戶叫用 [UpdateOrganizationConfiguration](#) API。將 `AutoEnable` 欄位設定為 `true`，以在新的組織帳戶中自動啟用 Security Hub CSPM。

AWS CLI

以 Security Hub CSPM 成員身分自動啟用新的組織帳戶

從委派管理員帳戶執行 [update-organization-configuration](#) 命令。包含 `auto-enable` 參數，以在新的組織帳戶中自動啟用 Security Hub CSPM。

```
aws securityhub update-organization-configuration --auto-enable
```

在新的組織帳戶中手動啟用 Security Hub CSPM

如果您在新組織帳戶中加入組織時未自動啟用 Security Hub CSPM，則可以將這些帳戶新增為成員，並在他們加入組織後手動啟用 Security Hub CSPM。您還必須在 AWS 帳戶 之前與組織取消關聯的 中手動啟用 Security Hub CSPM。

Note

如果您使用 [中央組態](#)，則本節不適用於您。如果您使用中央組態，則可以建立在指定的成員帳戶和組織單位 (OUs) 組態政策。您也可以在这些帳戶和 OUs 中啟用特定標準和控制項。

如果 Security Hub CSPM 已經是不同組織中的成員帳戶，則您無法在帳戶中啟用該帳戶。

您也無法在目前暫停的帳戶中啟用 Security Hub CSPM。如果您嘗試在暫停的帳戶中啟用服務，帳戶狀態會變更為帳戶暫停。

- 如果帳戶未啟用 Security Hub CSPM，則會在該帳戶中啟用 Security Hub CSPM。除非您關閉預設安全標準，否則帳戶中也會啟用 AWS 基礎安全最佳實務 (FSBP) 標準和 CIS AWS Foundations Benchmark 1.2.0 版。

例外情況是 Organizations 管理帳戶。無法在 Organizations 管理帳戶中自動啟用 Security Hub CSPM。您必須先在 Organizations 管理帳戶中手動啟用 Security Hub CSPM，才能將其新增為成員帳戶。

- 如果帳戶已啟用 Security Hub CSPM，Security Hub CSPM 不會對帳戶進行任何其他變更。它只會啟用 成員資格。

為了讓 Security Hub CSPM 產生控制調查結果，成員帳戶必須 AWS Config 啟用並設定 以記錄必要的資源。如需詳細資訊，請參閱[啟用並設定 AWS Config](#)。

選擇您偏好的方法，並依照步驟將組織帳戶啟用為 Security Hub CSPM 成員帳戶。

Security Hub CSPM console

以 Security Hub CSPM 成員身分手動啟用組織帳戶

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用委派管理員帳戶的登入資料登入。

2. 在 Security Hub CSPM 導覽窗格中的設定下，選擇組態。
3. 在帳戶清單中，選取您要啟用的每個組織帳戶。
4. 選擇動作，然後選擇新增成員。

Security Hub CSPM API

以 Security Hub CSPM 成員身分手動啟用組織帳戶

從委派管理員帳戶叫用 [CreateMembers](#) API。針對每個要啟用的帳戶，提供帳戶 ID。

與手動邀請程序不同，當您叫用 CreateMembers 以啟用組織帳戶時，您不需要傳送邀請。

AWS CLI

以 Security Hub CSPM 成員身分手動啟用組織帳戶

從委派管理員帳戶執行 [create-members](#) 命令。針對每個要啟用的帳戶，提供帳戶 ID。

與手動邀請程序不同，當您執行 create-members 以啟用組織帳戶時，您不需要傳送邀請。

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

範例

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"}, {"AccountId": "123456789222"}]'
```

取消 Security Hub CSPM 成員帳戶與組織的關聯

若要停止接收和檢視 Security AWS Hub CSPM 成員帳戶的問題清單，您可以取消成員帳戶與組織的關聯。

Note

如果您使用 [中央組態](#)，取消關聯的運作方式會有所不同。您可以建立組態政策，在一或多個集中管理的成員帳戶中停用 Security Hub CSPM。之後，這些帳戶仍然是組織的一部分，但不會產生 Security Hub CSPM 調查結果。如果您使用中央組態，但也有手動邀請的成員帳戶，您可以取消一個或多個手動邀請帳戶的關聯。

使用管理的成員帳戶 AWS Organizations 無法取消其帳戶與管理員帳戶的關聯。只有管理員帳戶可以取消成員帳戶的關聯。

取消成員帳戶的關聯不會關閉帳戶。相反地，它會從組織中移除成員帳戶。取消關聯的成員帳戶會成為獨立 AWS 帳戶，不再由 Security Hub CSPM 整合管理 AWS Organizations。

選擇您偏好的方法，並依照步驟取消成員帳戶與組織的關聯。

Security Hub CSPM console

取消成員帳戶與組織的關聯

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用委派管理員帳戶的登入資料登入。

2. 在導覽窗格中的設定下，選擇組態。
3. 在帳戶區段中，選取您要取消關聯的帳戶。如果您使用中央組態，則可以選取要與 Invitation accounts 標籤取消關聯的手動邀請帳戶。只有在您使用中央組態時，才會顯示此標籤。
4. 選擇動作，然後選擇取消關聯帳戶。

Security Hub CSPM API

取消成員帳戶與組織的關聯

從委派的管理員帳戶叫用 [DisassociateMembers](#) API。您必須提供要取消關聯的成員帳戶的 AWS 帳戶 IDs。若要檢視成員帳戶清單，請叫用 [ListMembers](#) API。

AWS CLI

取消成員帳戶與組織的關聯

從委派的管理員帳戶執行 [>disassociate-members](#) 命令。您必須提供要取消關聯的成員帳戶的 AWS 帳戶 IDs。若要檢視成員帳戶清單，請執行 [>list-members](#) 命令。

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

範例

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

您也可以使用 AWS Organizations 主控台 AWS CLI 或 AWS SDKs 取消成員帳戶與組織的關聯。如需詳細資訊，請參閱 AWS Organizations 《使用者指南》中的 [從您的組織移除成員帳戶](#)。

在 Security Hub CSPM 中透過邀請管理帳戶

您可以透過兩種方式集中管理多個 AWS Security Hub CSPM 帳戶，方法是將 Security Hub CSPM 與整合，AWS Organizations 或手動傳送和接受成員資格邀請。如果您有獨立帳戶或未與整合，則必須使用手動程序 AWS Organizations。在手動帳戶管理中，Security Hub CSPM 管理員會邀請帳戶成為成員。當潛在成員接受邀請時，會建立管理員成員關係。Security Hub CSPM 管理員帳戶可以為最多 1,000 個以邀請為基礎的成員帳戶管理 Security Hub CSPM。

Note

如果您在 Security Hub CSPM 中建立以邀請為基礎的組織，您之後可以改為[使用 AWS Organizations](#)。如果您有多個成員帳戶，我們建議您使用 AWS Organizations 而非 Security Hub CSPM 邀請來管理您的成員帳戶。如需相關資訊，請參閱[使用管理多個帳戶的 Security Hub CSPM AWS Organizations](#)。

跨區域彙總問題清單和其他資料可供您透過手動邀請程序邀請的帳戶使用。不過，管理員必須邀請成員帳戶來自彙總區域和所有連結區域，才能跨區域彙總運作。此外，成員帳戶必須在彙總區域和所有連結區域中啟用 Security Hub CSPM，讓管理員能夠檢視成員帳戶中的問題清單。

手動邀請的成員帳戶不支援組態政策。相反地，當您使用手動邀請程序 AWS 區域 時，您必須在每個成員帳戶中分別設定 Security Hub CSPM 設定。

對於不屬於您組織的帳戶，您還必須使用以邀請為基礎的手動程序。例如，您可能不會在組織中包含測試帳戶。或者，您可能想要將來自多個組織的帳戶合併到單一 Security Hub CSPM 管理員帳戶下。Security Hub CSPM 管理員帳戶必須將邀請傳送給屬於其他組織的帳戶。

在 Security Hub CSPM 主控台的組態頁面上，透過邀請新增的帳戶會列在邀請帳戶索引標籤中。如果您使用 [中央組態](#)，但也邀請組織外部的帳戶，您可以在此索引標籤中檢視邀請型帳戶的問題清單。不過，Security Hub CSPM 管理員無法透過使用組態政策跨區域設定邀請型帳戶。

本節中的主題說明如何透過邀請管理成員帳戶。

主題

- [在 Security Hub CSPM 中新增和邀請成員帳戶](#)
- [回應成為 Security Hub CSPM 成員帳戶的邀請](#)
- [在 Security Hub CSPM 中取消關聯成員帳戶](#)
- [在 Security Hub CSPM 中刪除成員帳戶](#)
- [取消與 Security Hub CSPM 管理員帳戶的關聯](#)
- [轉移至 Organizations 以在 Security Hub CSPM 中管理帳戶](#)

在 Security Hub CSPM 中新增和邀請成員帳戶

Note

我們建議您使用 AWS Organizations 而非 Security Hub CSPM 邀請來管理您的成員帳戶。如需相關資訊，請參閱[使用 管理多個帳戶的 Security Hub CSPM AWS Organizations](#)。

您的帳戶會成為接受您邀請成為 AWS Security Hub CSPM 成員帳戶之帳戶的 Security Hub CSPM 管理員。

當您接受來自另一個帳戶的邀請時，您的帳戶會成為成員帳戶，而該帳戶會成為您的管理員。

如果您的帳戶是管理員帳戶，則無法接受成為成員帳戶的邀請。

新增成員帳戶包含下列步驟：

1. 管理員帳戶會將成員帳戶新增至其成員帳戶清單。
2. 管理員帳戶會傳送邀請給成員帳戶。
3. 成員帳戶接受邀請。

新增成員帳戶

從 Security Hub CSPM 主控台，您可以將帳戶新增至成員帳戶清單。在 Security Hub CSPM 主控台中，您可以個別選取帳戶，或上傳包含帳戶資訊.csv的檔案。

對於每個帳戶，您必須提供帳戶 ID 和電子郵件地址。電子郵件地址應該是帳戶安全性問題時要聯絡的電子郵件地址。它不會用來驗證帳戶。

選擇您偏好的方法，然後依照步驟新增成員帳戶。

Security Hub CSPM console

將帳戶新增至成員帳戶清單

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用管理員帳戶的登入資料登入。

2. 在左側窗格中，選擇 Settings (設定)。
3. 在設定頁面上，選擇帳戶，然後選擇新增帳戶。然後，您可以個別新增帳戶或上傳包含帳戶清單.csv的檔案。
4. 若要選取帳戶，請執行下列其中一項操作：
 - 若要個別新增帳戶，請在輸入帳戶下，輸入要新增的帳戶 ID 和電子郵件地址，然後選擇新增。

為每個帳戶重複此程序。

- 若要使用逗號分隔值 (.csv) 檔案來新增多個帳戶，請先建立 檔案。檔案必須包含要新增的每個帳戶的帳戶 ID 和電子郵件地址。

在您的.csv清單中，帳戶必須每行顯示一個。.csv 檔案的第一行必須包含 標頭。在 標頭中，第一欄是 **Account ID**，第二欄是 **Email**。

後續每行都必須包含要新增帳戶的有效帳戶 ID 和電子郵件地址。

以下是在文字編輯器中檢視時 .csv 的檔案範例。

```
Account ID,Email  
111111111111,user@example.com
```

在試算表程式中，欄位會顯示在不同的欄中。基礎格式仍以逗號分隔。您必須將帳戶 IDs 格式化為非小數。例如，帳戶 ID 444455556666 無法格式化為 444455556666.0。此外，請確定數字格式不會從帳戶 ID 中移除任何前導零。

若要選取檔案，請在主控台上選擇上傳清單 (.csv)。然後選擇瀏覽。

選取檔案後，選擇新增帳戶。

5. 完成新增帳戶後，在要新增的帳戶下，選擇下一步。

Security Hub CSPM API

將帳戶新增至成員帳戶清單

從管理員帳戶叫用 [CreateMembers](#) API。對於要新增的每個成員帳戶，您必須提供 AWS 帳戶 ID。

AWS CLI

將帳戶新增至成員帳戶清單

從管理員帳戶執行 [create-members](#) 命令。對於要新增的每個成員帳戶，您必須提供 AWS 帳戶 ID。

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

範例

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},  
{"AccountId": "123456789222"}]'
```

邀請成員帳戶

新增成員帳戶後，您會傳送邀請給成員帳戶。您也可以將邀請重新傳送至與管理員取消關聯的帳戶。

Security Hub CSPM console

邀請潛在成員帳戶

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用管理員帳戶的登入資料登入。

2. 在導覽窗格中，選擇設定，然後選擇帳戶。
3. 對於要邀請的帳戶，請在狀態欄中選擇邀請。
4. 出現確認提示時，請選擇邀請。

Note

若要重新傳送取消關聯帳戶的邀請，請在帳戶頁面上選取每個取消關聯的帳戶。針對動作，選擇重新傳送邀請。

Security Hub CSPM API

邀請潛在成員帳戶

從管理員帳戶叫用 [InviteMembers](#) API。對於每個要邀請的帳戶，您必須提供 AWS 帳戶 ID。

AWS CLI

邀請潛在成員帳戶

從管理員帳戶執行 [invite-members](#) 命令。對於每個要邀請的帳戶，您必須提供 AWS 帳戶 ID。

```
aws securityhub invite-members --account-ids <accountIDs>
```

範例

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

回應成為 Security Hub CSPM 成員帳戶的邀請

Note

我們建議您使用 AWS Organizations 而非 Security Hub CSPM 邀請來管理您的成員帳戶。如需相關資訊，請參閱[使用 管理多個帳戶的 Security Hub CSPM AWS Organizations](#)。

您可以接受或拒絕成為 AWS Security Hub CSPM 成員帳戶的邀請。

如果您接受邀請，您的帳戶會成為 Security Hub CSPM 成員帳戶。傳送邀請的帳戶會成為您的 Security Hub CSPM 管理員帳戶。管理員帳戶使用者可以在 Security Hub CSPM 中檢視成員帳戶的調查結果。

如果您拒絕邀請，則您的 帳戶會在管理員帳戶的成員帳戶清單中標記為已撤銷。

您只能接受一個成為成員帳戶的邀請。

您必須先啟用 Security Hub CSPM，才能接受或拒絕邀請。

請記住，所有 Security Hub CSPM 帳戶必須 AWS Config 已啟用並設定為記錄所有資源。如需 需求的詳細資訊 AWS Config，請參閱[啟用和設定 AWS Config](#)。

接受邀請

您可以從管理員帳戶傳送成為 Security Hub CSPM 成員帳戶的邀請。然後，您可以在登入成員帳戶後接受邀請。

選擇您偏好的方法，並依照步驟接受成為成員帳戶的邀請。

Security Hub CSPM console

接受成員資格邀請

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇設定，然後選擇帳戶。
3. 在管理員帳戶區段中，開啟接受，然後選擇接受邀請。

Security Hub CSPM API

接受成員資格邀請

叫用 [AcceptAdministratorInvitation](#) API。您必須提供邀請識別符和管理員帳戶的 AWS 帳戶 ID。若要擷取邀請的詳細資訊，請使用 [ListInvitations](#) 操作。

AWS CLI

接受成員資格邀請

執行 [accept-administrator-invitation](#) 命令。您必須提供邀請識別符和管理員帳戶的 AWS 帳戶 ID。若要擷取邀請的詳細資訊，請執行 [list-invitations](#) 命令。

```
aws securityhub accept-administrator-invitation --administrator-id <administratorAccountID> --invitation-id <invitationID>
```

範例

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

Note

Security Hub CSPM 主控台會繼續使用 `AcceptInvitation`。它最終會變更為使用 `AcceptAdministratorInvitation`。任何專門控制此函數存取的 IAM 政策都必須繼續使用 `AcceptInvitation`。您也應該將 `AcceptAdministratorInvitation` 新增至政策，以確保在主控台開始使用之後，具有正確的許可 `AcceptAdministratorInvitation`。

拒絕邀請

您可以拒絕成為 Security Hub CSPM 成員帳戶的邀請。當您在 Security Hub CSPM 主控台拒絕邀請時，您的帳戶會在管理員帳戶的成員帳戶清單中標示為已簽署。只有在您使用管理員帳戶登入 Security Hub CSPM 主控台時，才會顯示已退出狀態。不過，在您登入管理員帳戶並刪除邀請之前，成員帳戶的主控台邀請保持不變。

若要拒絕邀請，您必須登入收到邀請的成員帳戶。

選擇您偏好的方法，並依照步驟拒絕成為成員帳戶的邀請。

Security Hub CSPM console

拒絕成員資格邀請

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇設定，然後選擇帳戶。
3. 在管理員帳戶區段中，選擇拒絕邀請。

Security Hub CSPM API

拒絕成員資格邀請

叫用 [DeclineInvitations](#) API。您必須提供發出邀請的管理員帳戶的 AWS 帳戶 ID。若要檢視邀請的相關資訊，請使用 [ListInvitations](#) 操作。

AWS CLI

拒絕成員資格邀請

執行 [decline-invitations](#) 命令。您必須提供發出邀請的管理員帳戶的 AWS 帳戶 ID。若要檢視邀請的相關資訊，請執行 [list-invitations](#) 命令。

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

範例

```
aws securityhub decline-invitations --account-ids "123456789012"
```

在 Security Hub CSPM 中取消關聯成員帳戶

Note

我們建議您使用 AWS Organizations 而非 Security Hub CSPM 邀請來管理您的成員帳戶。如需相關資訊，請參閱 [使用 管理多個帳戶的 Security Hub CSPM AWS Organizations](#)。

AWS Security Hub CSPM 管理員帳戶可以取消成員帳戶的關聯，以停止從該帳戶接收和檢視問題清單。您必須先取消成員帳戶的關聯，才能將其刪除。

當您取消關聯成員帳戶時，其會保留在您的成員帳戶清單中，狀態為已移除（已取消關聯）。您的帳戶已從成員帳戶的管理員帳戶資訊中移除。

若要繼續接收帳戶的調查結果，您可以重新傳送邀請。若要完全移除成員帳戶，您可以刪除成員帳戶。

選擇您偏好的方法，並依照步驟取消手動邀請的成員帳戶與管理員帳戶的關聯。

Security Hub CSPM console

取消手動邀請成員帳戶的關聯

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用管理員帳戶的登入資料登入。

2. 在導覽窗格中的設定下，選擇組態。
3. 在帳戶區段中，選取您要取消關聯的帳戶。
4. 選擇動作，然後選擇取消關聯帳戶。

Security Hub CSPM API

取消手動邀請成員帳戶的關聯

從管理員帳戶叫用 [DisassociateMembers](#) API。您必須提供您要取消關聯的成員帳戶的 AWS 帳戶 IDs。若要檢視成員帳戶清單，請使用 [ListMembers](#) 操作。

AWS CLI

取消手動邀請成員帳戶的關聯

從管理員帳戶執行 [disassociate-members](#) 命令。您必須提供您要取消關聯的成員帳戶的 AWS 帳戶 IDs。若要檢視成員帳戶清單，請執行 [list-members](#) 命令。

```
aws securityhub disassociate-members --account-ids <accountIds>
```

範例

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

在 Security Hub CSPM 中刪除成員帳戶

Note

我們建議您使用 AWS Organizations 而非 Security Hub CSPM 邀請來管理您的成員帳戶。如需相關資訊，請參閱[使用 管理多個帳戶的 Security Hub CSPM AWS Organizations](#)。

作為 AWS Security Hub CSPM 管理員帳戶，您可以刪除透過邀請新增的成員帳戶。您必須先取消關聯，才能刪除已啟用的帳戶。

當您刪除成員帳戶時，該帳戶會從清單中完全移除。若要還原帳戶的成員資格，您必須新增並再次邀請該帳戶，就好像是全新的成員帳戶一樣。

您無法刪除屬於組織且使用 整合管理的帳戶 AWS Organizations。

選擇您偏好的方法，然後依照步驟刪除手動邀請的成員帳戶。

Security Hub CSPM console

刪除手動邀請的成員帳戶

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
使用管理員帳戶登入。
2. 在導覽窗格中，選擇設定，然後選擇組態。
3. 選擇邀請帳戶索引標籤。然後，選取要刪除的帳戶。
4. 選擇動作，然後選擇刪除。只有在您取消關聯帳戶時，才能使用此選項。您必須先取消關聯成員帳戶，才能將其刪除。

Security Hub CSPM API

刪除手動邀請的成員帳戶

從管理員帳戶叫用 [DeleteMembers](#) API。您必須提供要刪除之成員帳戶的 AWS 帳戶 IDs。若要擷取成員帳戶清單，請叫用 [ListMembers](#) API。

AWS CLI

刪除手動邀請的成員帳戶

從管理員帳戶執行 [delete-members](#) 命令。您必須提供要刪除之成員帳戶的 AWS 帳戶 IDs。若要擷取成員帳戶的清單，請執行 [list-members](#) 命令。

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

範例

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

取消與 Security Hub CSPM 管理員帳戶的關聯

Note

我們建議您使用 AWS Organizations 而非 Security Hub CSPM 邀請來管理您的成員帳戶。如需相關資訊，請參閱 [使用 管理多個帳戶的 Security Hub CSPM AWS Organizations](#)。

如果您的帳戶透過邀請新增為 AWS Security Hub CSPM 成員帳戶，您可以取消成員帳戶與管理員帳戶的關聯。取消關聯成員帳戶之後，Security Hub CSPM 不會將問題清單從帳戶傳送到管理員帳戶。

使用 整合管理的成員帳戶 AWS Organizations 無法取消其帳戶與管理員帳戶的關聯。只有 Security Hub CSPM 委派管理員可以取消與 Organizations 管理的成員帳戶關聯。

當您取消與管理員帳戶的關聯時，您的帳戶會保留在管理員帳戶的成員清單中，狀態為已撤銷。不過，管理員帳戶不會收到您帳戶的任何調查結果。

在您將自己與管理員帳戶取消關聯之後，成為成員的邀請仍然存在。您可以在未來再次接受邀請。

Security Hub CSPM console

取消與管理員帳戶的關聯

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇設定，然後選擇帳戶。
3. 在管理員帳戶區段中，關閉接受，然後選擇更新。

Security Hub CSPM API

取消與管理員帳戶的關聯

叫用 [DisassociateFromAdministratorAccount](#) API。

AWS CLI

取消與管理員帳戶的關聯

執行 [disassociate-from-administrator-account](#) 命令。

```
aws securityhub disassociate-from-administrator-account
```

Note

Security Hub CSPM 主控台會繼續使用 `DisassociateFromMasterAccount`。它最終會變更為使用 `DisassociateFromAdministratorAccount`。任何專門控制此函數存取的 IAM 政策都必須繼續使用 `DisassociateFromMasterAccount`。您也應該 `DisassociateFromAdministratorAccount` 將新增至政策，以確保在主控台開始使用之後，具有正確的許可 `DisassociateFromAdministratorAccount`。

轉移至 Organizations 以在 Security Hub CSPM 中管理帳戶

當您在 AWS Security Hub CSPM 中手動管理帳戶時，您必須邀請潛在成員帳戶，並在每個帳戶中分別設定每個成員帳戶 AWS 區域。

透過整合 Security Hub CSPM 和 AWS Organizations，您可以消除傳送邀請的需求，並進一步控制 Security Hub CSPM 在組織中的設定和自訂方式。因此，我們建議您使用 AWS Organizations 而非 Security Hub CSPM 邀請來管理您的成員帳戶。如需相關資訊，請參閱[使用 管理多個帳戶的 Security Hub CSPM AWS Organizations](#)。

您可以使用使用 AWS Organizations 整合的合併方法，但也可以手動邀請組織外部的帳戶。不過，我們建議僅使用 Organizations 整合。[中央組態](#)是一項可協助您跨多個帳戶和區域管理 Security Hub CSPM 的功能，只有在您與 Organizations 整合時才能使用。

本節說明如何從以邀請為基礎的手動帳戶管理轉換到使用 管理帳戶 AWS Organizations。

將 Security Hub CSPM 與 整合 AWS Organizations

首先，您必須整合 Security Hub CSPM 和 AWS Organizations。

您可以透過完成下列步驟來整合這些服務：

- 在 中建立組織 AWS Organizations。如需說明，請參閱AWS Organizations 《使用者指南》中的[建立組織](#)。
- 從 Organizations 管理帳戶，指定 Security Hub CSPM 委派管理員帳戶。

Note

組織管理帳戶無法設定為 DA 帳戶。

如需詳細說明，請參閱 [將 Security Hub CSPM 與 整合 AWS Organizations](#)。

透過完成上述步驟，您授予 Security Hub CSPM 的[受信任存取權](#) AWS Organizations。這也 AWS 區域 會在委派管理員帳戶的目前 中啟用 Security Hub CSPM。

委派管理員可以在 Security Hub CSPM 中管理組織，主要是透過將組織的帳戶新增為 Security Hub CSPM 成員帳戶。管理員也可以存取這些帳戶的特定 Security Hub CSPM 設定、資料和資源。

當您使用 Organizations 轉換為帳戶管理時，邀請型帳戶不會自動成為 Security Hub CSPM 成員。只有您新增至新組織的帳戶才能成為 Security Hub CSPM 成員。

啟用整合之後，您可以使用 Organizations 管理帳戶。如需相關資訊，請參閱[使用 管理多個帳戶的 Security Hub CSPM AWS Organizations](#)。帳戶管理會根據組織的組態類型而有所不同。

Security Hub CSPM 中管理員和成員帳戶允許的動作

管理員和成員帳戶可存取下表所述的 AWS Security Hub CSPM 動作。在表格中，這些值具有下列含義：

- 任何 – 帳戶可以對相同管理員下的任何成員帳戶執行 動作。
- 目前 – 帳戶只能為自己執行動作（您目前登入的帳戶）。
- Dash – 表示帳戶無法執行動作。

如表格中所述，允許的動作會根據您是否與整合，AWS Organizations 以及組織使用的組態類型而有所不同。如需中央和本機組態之間差異的資訊，請參閱 [使用管理帳戶 AWS Organizations](#)。

Security Hub CSPM 不會將成員帳戶調查結果複製到管理員帳戶。在 Security Hub CSPM 中，所有調查結果都會擷取至特定帳戶的特定區域。在每個區域中，管理員帳戶可以檢視和管理該區域中成員帳戶的問題清單。

如果您設定彙總區域，管理員帳戶可以從複寫到彙總區域的連結區域中檢視和管理成員帳戶問題清單。如需跨區域彙總的詳細資訊，請參閱[跨區域彙總](#)。

下表指定管理員和成員帳戶的預設許可。您可以使用自訂 IAM 政策來進一步限制 Security Hub CSPM 功能和函數的存取。如需指引和範例，請參閱部落格文章將 [IAM 政策對齊 AWS Security Hub CSPM 的使用者角色](#)。

如果您與 Organizations 整合並使用中央組態，則允許動作

如果您與 Organizations 整合並使用中央組態，管理員和成員帳戶可以存取 Security Hub CSPM 動作，如下所示。

Action	Security Hub CSPM 委派管理員帳戶	集中管理的成員帳戶	自我管理成員帳戶
建立和管理 Security Hub CSPM 組態政策	適用於自我和集中管理的帳戶	–	–
檢視組織帳戶	任何	–	–
取消關聯成員帳戶	任何	–	–
刪除成員帳戶	任何非組織帳戶	–	–
停用 Security Hub CSPM	對於目前帳戶和集中管理帳戶	–	目前（必須與管理員帳戶取消關聯）
檢視問題清單和問題清單歷史記錄	任何	Current	Current
更新問題清單	任何	Current	Current
檢視洞見結果	任何	Current	Current

Action	Security Hub CSPM 委派管理員帳戶	集中管理的成員帳戶	自我管理成員帳戶
檢視控制項詳細資訊	任何	Current	Current
開啟或關閉合併控制 問題清單	任何	–	–
啟用和停用標準	對於目前帳戶和集中 管理帳戶	–	Current
啟用和停用控制項	對於目前帳戶和集中 管理帳戶	–	Current
啟用和停用整合	Current	Current	Current
設定跨區域彙總	任何	–	–
選取主要區域和連結 的區域	任何（必須停止並重 新啟動中央組態，才 能變更主區域）	–	–
設定自訂動作	Current	Current	Current
設定自動化規則	任何	–	–
設定自訂洞見	Current	Current	Current

如果您與 Organizations 整合並使用本機組態，則允許 動作

如果您與 Organizations 整合並使用本機組態，管理員和成員帳戶可以存取 Security Hub CSPM 動作，如下所示。

Action	Security Hub CSPM 委派管理 員帳戶	成員帳戶
建立和管理 Security Hub CSPM 組態政策	–	–

Action	Security Hub CSPM 委派管理員帳戶	成員帳戶
檢視組織帳戶	任何	–
取消關聯成員帳戶	任何	–
刪除成員帳戶	–	–
停用 Security Hub CSPM	–	目前（如果帳戶與委派管理員取消關聯）
檢視問題清單和問題清單歷史記錄	任何	Current
更新問題清單	任何	Current
檢視洞見結果	任何	Current
檢視控制項詳細資訊	任何	Current
開啟或關閉合併控制問題清單	任何	–
啟用和停用標準	Current	Current
在新的組織帳戶中自動啟用 Security Hub CSPM 和預設標準	對於目前帳戶和新組織帳戶	–
啟用和停用控制項	Current	Current
啟用和停用整合	Current	Current
設定跨區域彙總	任何	–
設定自訂動作	Current	Current
設定自動化規則	任何	–
設定自訂洞見	Current	Current

以邀請為基礎的帳戶的允許動作

如果您使用以邀請為基礎的方法來手動管理帳戶，而不是與整合，管理員和成員帳戶可以存取 Security Hub CSPM 動作，如下所示 AWS Organizations。

Action	Security Hub CSPM 管理員帳戶	成員帳戶
建立和管理 Security Hub CSPM 組態政策	–	–
檢視組織帳戶	任何	–
取消關聯成員帳戶	任何	Current
刪除成員帳戶	任何	–
停用 Security Hub CSPM	目前（如果沒有啟用的成員帳戶）	目前（如果帳戶與管理員帳戶取消關聯）
檢視問題清單和問題清單歷史記錄	任何	Current
更新問題清單	任何	Current
檢視洞見結果	任何	Current
檢視控制項詳細資訊	任何	Current
開啟或關閉合併控制問題清單	任何	–
啟用和停用標準	Current	Current
在新的組織帳戶中自動啟用 Security Hub CSPM 和預設標準	–	–
啟用和停用控制項	Current	Current
啟用和停用整合	Current	Current

Action	Security Hub CSPM 管理員帳戶	成員帳戶
設定跨區域彙總	任何	–
設定自訂動作	Current	Current
設定自動化規則	任何	–
設定自訂洞見	Current	Current

帳戶動作對 Security Hub CSPM 資料的影響

這些帳戶動作對 AWS Security Hub CSPM 資料有下列影響。

Security Hub CSPM 已停用

如果您使用[中央組態](#)，委派管理員 (DA) 可以建立 Security Hub CSPM 組態政策，在特定帳戶和組織單位 (OUs) 中停用 AWS Security Hub CSPM。在此情況下，Security Hub CSPM 會在您主要區域和任何連結區域中的指定帳戶和 OUs 中停用。如果您不使用中央組態，則必須在啟用它的每個帳戶和區域中分別停用 Security Hub CSPM。如果在 DA 帳戶中停用 Security Hub CSPM，則無法使用中央組態。

如果在管理員帳戶中停用 Security Hub CSPM，則不會為管理員帳戶產生或更新問題清單。現有的封存問題清單會在 30 天後刪除。現有的作用中問題清單會在 90 天後刪除。

AWS 服務 會移除與其他 的整合。

已啟用的安全標準和控制項已停用。

其他 Security Hub CSPM 資料和設定，包括第三方產品的自訂動作、洞見和訂閱會保留 90 天。

與管理員帳戶取消關聯的成員帳戶

當成員帳戶與管理員帳戶取消關聯時，管理員帳戶會失去檢視成員帳戶中問題清單的許可。不過，兩個帳戶中仍然啟用 Security Hub CSPM。

如果您使用中央組態，則 DA 無法為與 DA 帳戶取消關聯的成員帳戶設定 Security Hub CSPM。

為管理員帳戶定義的自訂設定或整合不會套用至前成員帳戶中的問題清單。例如，帳戶取消關聯後，您可能在管理員帳戶中有一個自訂動作，用作 Amazon EventBridge 規則中的事件模式。不過，此自訂動作無法在成員帳戶中使用。

在 Security Hub CSPM 管理員帳戶的帳戶清單中，移除的帳戶的狀態為取消關聯。

成員帳戶已從組織中移除

從組織移除成員帳戶時，Security Hub CSPM 管理員帳戶會失去檢視成員帳戶中問題清單的許可。不過，兩個帳戶中的 Security Hub CSPM 在移除前仍會啟用相同的設定。

如果您使用中央組態，則無法在從委派管理員所屬組織移除成員帳戶之後，為該帳戶設定 Security Hub CSPM。不過，除非您手動變更設定，否則帳戶會保留在移除之前擁有的設定。

在 Security Hub CSPM 管理員帳戶的帳戶清單中，移除的帳戶狀態為已刪除。

帳戶已暫停

AWS 帳戶 當 暫停時，帳戶會失去在 Security Hub CSPM 中檢視其問題清單的許可。不會產生或更新該帳戶的調查結果。暫停帳戶的管理員帳戶可以檢視帳戶的現有問題清單。

對於組織帳戶，成員帳戶狀態也可以變更為帳戶已暫停。如果帳戶在管理員帳戶嘗試啟用帳戶的同時遭到暫停，就會發生這種情況。帳戶暫停帳戶的管理員帳戶無法檢視該帳戶的調查結果。否則，暫停狀態不會影響成員帳戶狀態。

如果您使用中央組態，且委派管理員嘗試將組態政策與暫停的帳戶建立關聯，則政策關聯會失敗。

90 天後，帳戶將被終止或重新激活。重新啟用帳戶時，會還原其 Security Hub CSPM 許可。如果成員帳戶狀態為帳戶已暫停，則管理員帳戶必須手動啟用帳戶。

帳戶已關閉

AWS 帳戶 關閉 時，Security Hub CSPM 會回應關閉，如下所示。

如果帳戶是 Security Hub CSPM 管理員帳戶，則會將其移除為管理員帳戶，並移除所有成員帳戶。如果帳戶是成員帳戶，則會取消關聯並從 Security Hub CSPM 管理員帳戶移除成員身分。

Security Hub CSPM 會保留帳戶中現有的封存問題清單 30 天。對於控制項調查結果，30 天的計算是根據調查結果 UpdatedAt 欄位的值。對於其他類型的調查結果，計算是根據調查結果的 UpdatedAt 或 ProcessedAt 欄位的值，以最晚的日期為準。在此 30 天期間結束時，Security Hub CSPM 會從帳戶永久刪除問題清單。

Security Hub CSPM 會保留帳戶中現有的作用中問題清單 90 天。對於控制項調查結果，90 天的計算是根據調查結果 UpdatedAt 欄位的值。對於其他類型的調查結果，計算是根據調查結果的 UpdatedAt 或 ProcessedAt 欄位的值，以最晚的日期為準。在此 90 天期間結束時，Security Hub CSPM 會從帳戶永久刪除問題清單。

如需長期保留現有問題清單，您可以將問題清單匯出至 S3 儲存貯體。您可以搭配 Amazon EventBridge 規則使用自訂動作來執行此操作。如需詳細資訊，請參閱[使用 EventBridge 進行自動回應和修復](#)。

Important

對於 中的客戶 AWS GovCloud (US) Regions，請在關閉帳戶之前備份並刪除您的政策資料和其他帳戶資源。關閉帳戶後，您將無法存取資源和資料。

如需詳細資訊，請參閱《AWS 帳戶管理 參考指南》中的[關閉 AWS 帳戶](#)。

了解 Security Hub CSPM 中的跨區域彙總

Note

彙總區域現在稱為主區域。有些 Security Hub CSPM API 操作仍會使用較舊的詞彙彙總區域。

透過在 AWS Security Hub CSPM 中使用跨區域彙總，您可以將調查結果、調查結果更新、洞見、控制合規狀態和安全分數從多個 彙總 AWS 區域 到單一主區域。然後，您可以從主要區域管理所有這些資料。

假設您將美國東部（維吉尼亞北部）設定為主要區域，並將美國西部（奧勒岡）和美國西部（加利佛尼亞北部）設定為連結區域。當您檢視美國東部（維吉尼亞北部）的調查結果頁面時，您會看到所有三個區域的調查結果。這些調查結果的更新也會反映在所有三個區域中。

Note

在 中 AWS GovCloud (US)，僅對問題清單、問題清單更新和洞見支援跨區域彙總 AWS GovCloud (US)。具體而言，您只能彙總問題清單、問題清單更新，以及 AWS GovCloud（美國東部）和 AWS GovCloud（美國西部）之間的洞見。在中國區域中，僅支援跨區域彙總中

國區域的調查結果、調查結果更新和洞見。具體而言，您只能彙總中國（北京）和中國（寧夏）之間的問題清單、問題清單更新和洞見。

如果在連結的區域中啟用控制項，但在主要區域中停用，您可以從主要區域查看控制項的合規狀態，但您無法從主要區域啟用或停用該控制項。例外狀況是如果您使用[中央組態](#)。如果您使用中央組態，委派的 Security Hub CSPM 管理員可以設定主區域中的控制項，以及主區域中的連結區域。

如果您已設定主區域，[則安全分數](#)會考慮所有 中的控制狀態連結的區域。若要檢視跨區域安全分數和合規狀態，請將下列許可新增至使用 Security Hub CSPM 的 IAM 角色：

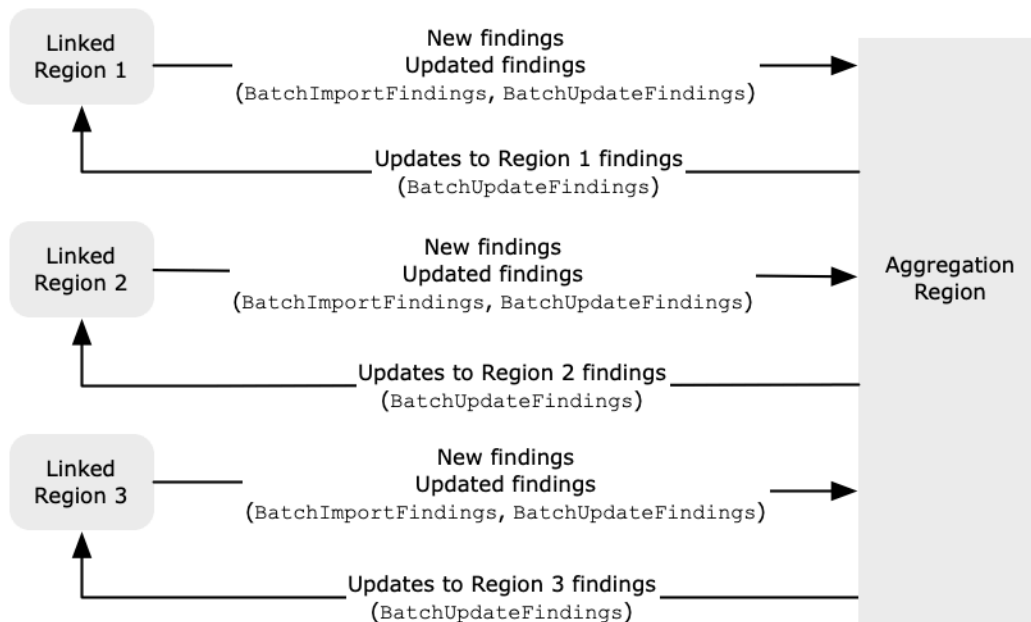
- [ListSecurityControlDefinitions](#)
- [BatchGetStandardsControlAssociations](#)
- [BatchUpdateStandardsControlAssociations](#)

彙總的資料類型

使用一或多個連結區域啟用跨區域彙總時，Security Hub CSPM 會將下列資料從連結區域複寫至主要區域。每個已啟用跨區域彙總的帳戶都會發生這種情況。

- 調查結果
- 洞見
- 控制合規狀態
- 安全性分數

除了先前清單中的新資料之外，Security Hub CSPM 也會在連結的區域和主要區域之間複寫此資料的更新。在連結區域中發生的更新會複寫至主要區域。主要區域中發生的更新會複寫回連結的區域。如果主要區域和連結區域有衝突的更新，則會使用最新的更新。



跨區域彙總不會增加 Security Hub CSPM 的成本。當 Security Hub CSPM 複寫新資料或更新時，您不需要付費。

在主區域中，摘要頁面提供跨連結區域的作用中問題清單檢視。如需詳細資訊，請參閱[依嚴重性檢視問題清單的跨區域摘要](#)。其他分析調查結果的摘要頁面面板也會顯示來自連結區域的資訊。

主區域中的安全分數是透過比較傳遞的控制項數量與所有連結區域中啟用的控制項數量來計算。此外，如果在至少一個連結區域中啟用控制項，它會顯示在主要區域的安全標準詳細資訊頁面上。標準詳細資訊頁面上控制項的合規狀態會反映連結區域的調查結果。如果與控制項相關聯的安全檢查在一或多個連結區域中失敗，則該控制項的合規狀態會在主要區域的標準詳細資訊頁面上顯示為失敗。安全檢查的數量包含所有連結區域的調查結果。

Security Hub CSPM 只會從帳戶已啟用 Security Hub CSPM 的區域彙總資料。帳戶不會根據跨區域彙總組態自動啟用 Security Hub CSPM。

可以在未選取任何連結區域的情況下啟用跨區域彙總。在此情況下，不會發生資料複寫。

管理員和成員帳戶的彙總

獨立帳戶、成員帳戶和管理員帳戶可以設定跨區域彙總。如果由管理員設定，則管理員帳戶的存在對於跨區域彙總在受管帳戶中運作至關重要。如果管理員帳戶已從成員帳戶移除或取消關聯，則成員帳戶的跨區域彙總會停止。即使帳戶在管理員成員關係開始之前已啟用跨區域彙總，也是如此。

當管理員帳戶啟用跨區域彙總時，Security Hub CSPM 會將管理員帳戶在所有連結區域中產生的資料複寫至主要區域。此外，Security Hub CSPM 會識別與該管理員相關聯的成員帳戶，而且每個成員帳

戶都會繼承管理員的跨區域彙總設定。Security Hub CSPM 會將成員帳戶在所有連結區域中產生的資料複寫至主要區域。

管理員可以存取和管理受管區域內所有成員帳戶的安全調查結果。不過，身為 Security Hub CSPM 管理員，您必須登入主要區域，才能檢視來自所有成員帳戶和連結區域的彙總資料。

作為 Security Hub CSPM 成員帳戶，您必須登入主區域，以檢視來自所有連結區域的帳戶彙總資料。成員帳戶沒有檢視其他成員帳戶資料的權限。

管理員帳戶可以手動邀請成員帳戶，或擔任與整合之組織的委派管理員 AWS Organizations。對於[手動邀請的成員帳戶](#)，管理員必須邀請來自主區域和所有連結區域的帳戶，才能跨區域彙總運作。此外，成員帳戶必須在主區域和所有連結區域中啟用 Security Hub CSPM，讓管理員能夠檢視成員帳戶中的問題清單。如果您不將主區域用於其他用途，您可以停用該區域中的 Security Hub CSPM 標準和整合，以防止產生費用。

如果您計劃使用跨區域彙總，並擁有多個管理員帳戶，建議您遵循下列最佳實務：

- 每個管理員帳戶都有不同的成員帳戶。
- 每個管理員帳戶在各區域都有相同的成員帳戶。
- 每個管理員帳戶使用不同的主區域。

Note

若要了解跨區域彙總如何影響中央組態，請參閱 [中央組態對跨區域彙總的影響](#)。

中央組態對跨區域彙總的影響

中央組態是 AWS Security Hub CSPM 中的選擇加入功能，如果您與整合，則可以使用此功能 AWS Organizations。如果您使用中央組態，委派的管理員帳戶可以為組織中的帳戶和組織單位 (OU) 設定 Security Hub CSPM 服務、標準和控制項。若要設定帳戶和 OUs，委派管理員會建立 Security Hub CSPM 組態政策。組態政策可用來定義 Security Hub CSPM 是否啟用或停用，以及啟用哪些標準和控制項。委派管理員會將組態政策與特定帳戶、OUs 或根（整個組織）建立關聯。

委派管理員只能從主要區域為組織建立和管理組態政策。此外，組態政策會在主要區域和所有連結區域中生效。您無法建立僅適用於某些連結區域而非其他區域的組態政策。如需跨區域彙總的資訊，請參閱[跨區域彙總](#)。

若要使用中央組態，您必須指定主要區域。或者，您可以選擇一或多個區域做為連結的區域。您也可以選擇指定不含任何連結區域的主區域。

變更跨區域彙總設定可能會影響您的組態政策。當您新增連結的區域時，您的組態政策會在該區域中生效。如果區域是[選擇加入區域](#)，則必須啟用該區域，您的組態政策才能在那裡生效。相反地，當您移除連結的區域時，組態政策不會再在該區域中生效。在該區域中，帳戶會維護其在移除連結區域時所擁有的設定。您可以變更這些設定，但必須在每個帳戶和區域中個別變更。

如果您移除或變更主要區域，則會刪除您的組態政策和政策關聯。您無法再在任何區域中使用中央組態或建立組態政策。帳戶會維護在主區域變更或移除之前所擁有的設定。您可以隨時變更這些設定，但由於您不再使用中央組態，因此必須在每個帳戶和區域中分別修改設定。如果您指定新的主要區域，則可以使用中央組態並再次建立組態政策。

如需中央組態的詳細資訊，請參閱 [了解 Security Hub CSPM 中的中央組態](#)。

啟用跨區域彙總

Note

彙總區域現在稱為主區域。有些 Security Hub CSPM API 操作仍會使用較舊的詞彙彙總區域。

您必須從 AWS 區域 要指定為主要區域的 啟用跨區域彙總。

若要啟用跨區域彙總，您可以建立稱為調查結果彙總工具的 Security Hub CSPM 資源。問題清單彙總工具資源會指定您的主要區域和連結的區域（如果有的話）。

您無法使用預設為停用 AWS 區域 的 做為您的主要區域。如需預設停用的區域清單，請參閱《》中的[啟用區域](#)AWS 一般參考。

當您啟用跨區域彙總時，您可以選擇視需要指定一或多個連結區域。您也可以選擇在 Security Hub CSPM 開始支援區域，且您已選擇加入區域時，是否自動連結新區域。

Security Hub CSPM console

啟用跨區域彙總

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 使用 AWS 區域 選擇器，登入您要用作彙總區域的 區域。

3. 在 Security Hub CSPM 導覽功能表中，選擇設定，然後選擇區域。
4. 針對問題清單彙總，選擇設定問題清單彙總。

根據預設，主區域設定為無彙總區域。

5. 在彙總區域下，選取 選項，將目前區域指定為主要區域。
6. 或者，對於連結的區域，選取要從中彙總資料的區域。
7. 若要自動彙總分割區中新區域的資料，因為 Security Hub CSPM 支援它們並選擇加入它們，請選取連結未來區域。
8. 選擇儲存。

Security Hub CSPM API

從您要用作主區域的區域中，使用 Security Hub CSPM API [CreateFindingAggregator](#) 的操作。如果您使用 AWS CLI，請執行 [create-finding-aggregator](#) 命令。

針對 RegionLinkingMode，請選擇下列其中一種選項：

- ALL_REGIONS – Security Hub CSPM 彙總來自所有區域的資料。Security Hub CSPM 也會彙總來自新區域的資料，因為它們受到支援且您選擇加入它們。
- ALL_REGIONS_EXCEPT_SPECIFIED – Security Hub CSPM 會彙總所有區域的資料，但您想要排除的區域除外。Security Hub CSPM 也會彙總來自新區域的資料，因為它們受到支援且您選擇加入它們。使用 Regions 提供要從彙總中排除的區域清單。
- SPECIFIED_REGIONS – Security Hub CSPM 會從選取的區域清單中彙總資料。Security Hub CSPM 不會自動彙總來自新區域的資料。使用 Regions 提供要從中彙總的區域清單。
- NO_REGIONS – Security Hub CSPM 不會彙總資料，因為您未選取任何連結的區域。

下列範例會設定跨區域彙總。主要區域是美國東部（維吉尼亞北部）。連結的區域是美國西部（加利佛尼亞北部）和美國西部（奧勒岡）。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

檢閱跨區域彙總設定

Note

彙總區域現在稱為主區域。有些 Security Hub CSPM API 操作仍會使用較舊的詞彙彙總區域。

您可以從任何 中檢視 AWS Security Hub CSPM 中目前的跨區域彙總組態 AWS 區域。組態包含主區域、連結的區域（如果有的話），以及是否要在 Security Hub CSPM 支援時自動連結新區域。

成員帳戶可以檢視管理員帳戶設定的跨區域彙總設定。

選擇您偏好的方法，然後依照步驟檢視您目前的跨區域彙總設定。

Security Hub CSPM console

檢視跨區域彙總設定（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇設定，然後選擇區域索引標籤。

如果未啟用跨區域彙總，則區域索引標籤會顯示啟用跨區域彙總的選項。只有管理員帳戶和獨立帳戶可以啟用跨區域彙總。

如果啟用跨區域彙總，則區域索引標籤會顯示下列資訊：

- 主要區域
- 是否自動彙總 Security Hub CSPM 支援且您選擇加入之新區域的調查結果、洞見、控制狀態和安全分數
- 連結區域清單（如果有選取）

Security Hub CSPM API

若要檢閱跨區域彙總設定 (Security Hub CSPM API)

使用 Security Hub CSPM API [GetFindingAggregator](#) 的操作。如果您使用 AWS CLI，請執行 [get-finding-aggregator](#) 命令。

當您提出請求時，請提供調查結果彙總器 ARN。若要取得問題清單彙總工具 ARN，請使用 [ListFindingAggregators](#) 操作或 [list-finding-aggregators](#) 命令。

下列範例顯示指定調查結果彙總器 ARN 的跨區域彙總設定。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 換行字元來改善可讀性

```
$aws securityhub get-finding-aggregator --finding-aggregator-  
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-  
e89b-12d3-a456-426652340000
```

更新跨區域彙總設定

Note

彙總區域現在稱為主區域。有些 Security Hub CSPM API 操作仍會使用較舊的詞彙彙總區域。

您可以透過變更連結區域或目前的主區域，在 AWS Security Hub CSPM 中更新目前的跨區域彙總設定。您也可以變更是否要從 AWS 區域 Security Hub CSPM 支援的新自動彙總資料。

除非您在 中啟用區域，否則不會針對選擇加入區域實作跨區域彙總的變更 AWS 帳戶。在 2019 年 3 月 20 日當天或之後 AWS 推出的區域為選擇加入區域。

當您停止從連結區域彙總資料時，AWS Security Hub CSPM 不會從主要區域中可存取的該區域移除任何現有的彙總資料。

您無法使用本節中的更新程序來變更主要區域。若要變更主要區域，您必須執行下列動作：

1. 停止跨區域彙總。如需說明，請參閱[the section called “停止彙總”](#)。
2. 變更為您希望成為新主區域的區域。
3. 啟用跨區域彙總。如需說明，請參閱[the section called “啟用彙總”](#)。

您必須從目前的主區域更新跨區域彙總組態。

Security Hub CSPM console

變更連結的區域

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

登入目前的彙總區域。

2. 在 Security Hub CSPM 導覽功能表中，選擇設定，然後選擇區域。
3. 針對問題清單彙總，選擇編輯。
4. 針對連結區域，更新選取的連結區域。
5. 如有需要，請變更是否選取連結未來區域。此設定會決定 Security Hub CSPM 在新增支援區域時是否自動連結新區域，而且您可以選擇加入這些區域。
6. 選擇儲存。

Security Hub CSPM API

使用 [UpdateFindingAggregator](#) 操作。如果您使用 AWS CLI，請執行 [update-finding-aggregator](#) 命令。若要識別問題清單彙總工具，您必須提供問題清單彙總工具 ARN。若要取得問題清單彙總工具 ARN，請使用 [ListFindingAggregators](#) 操作或 [list-finding-aggregators](#) 命令。

如果連結模式是 ALL_REGIONS_EXCEPT_SPECIFIED 或 SPECIFIED_REGIONS，您可以變更排除或包含區域的清單。如果您想要將區域連結模式變更為 NO_REGIONS，則不應提供區域清單。

當您變更排除或包含區域的清單時，您必須提供更新的完整清單。例如，假設您目前彙總了美國東部（俄亥俄）的問題清單，也想要彙總美國西部（奧勒岡）的問題清單。您必須提供包含美國東部（俄亥俄）和美國西部（奧勒岡）的 Regions 清單。

下列範例會將跨區域彙總更新為選取的區域。命令是從目前的主區域執行，也就是美國東部（維吉尼亞北部）。連結的區域為美國西部（加利佛尼亞北部）和美國西部（奧勒岡）。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```


停止跨區域彙總

Note

彙總區域現在稱為主區域。有些 Security Hub CSPM API 操作仍會使用較舊的詞彙彙總區域。

如果您不希望 AWS Security Hub CSPM 彙總資料，您可以刪除問題清單彙總工具。或者，您可以將現有的彙總工具更新 AWS 區域 為連結模式，以保留問題清單彙總工具，但不能將任何 NO_REGIONS 連結到主要區域。

若要變更您的主要區域，您必須刪除目前的問題清單彙總工具，並建立新的問題清單彙總工具。

當您刪除問題清單彙總工具時，Security Hub CSPM 會停止彙總資料。它不會從主要區域移除任何現有的彙總資料。

刪除問題清單彙總工具（主控台）

您只能從目前的主區域刪除問題清單彙總器。

在主區域以外的區域中，Security Hub CSPM 主控台上的問題清單彙總面板會顯示訊息，您必須編輯主區域中的組態。選擇此訊息以顯示切換至主要區域的連結。

Security Hub CSPM console

停止跨區域彙總（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 確保您已登入目前的主區域。
3. 在 Security Hub CSPM 導覽功能表中，選擇設定，然後選擇區域。
4. 在問題清單彙總下，選擇編輯。
5. 在彙總區域下，選擇無彙總區域。
6. 選擇儲存。
7. 在確認對話方塊的確認欄位中，輸入 **Confirm**。
8. 選擇確認。

Security Hub CSPM API

使用 Security Hub CSPM API [DeleteFindingAggregator](#) 的操作。如果您使用的是 AWS CLI，請執行 [delete-finding-aggregator](#) 命令。

若要識別要刪除的問題清單彙總工具，請提供問題清單彙總工具 ARN。若要取得問題清單彙總工具 ARN，請使用 [ListFindingAggregators](#) 操作或 [list-finding-aggregators](#) 命令。

下列範例會刪除問題清單彙總工具。命令是從目前的主區域執行，也就是美國東部（維吉尼亞北部）。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --region us-east-1
```

了解 Security Hub CSPM 中的安全標準

在 AWS Security Hub CSPM 中，安全標準是根據法規架構、產業最佳實務或公司政策的一組要求。如需 Security Hub CSPM 目前支援之標準的詳細資訊，包括適用於每個標準的安全控制，請參閱 [Security Hub CSPM 的標準參考](#)。

當您啟用標準時，Security Hub CSPM 會自動啟用適用於標準的所有控制項。Security Hub CSPM 接著會對控制項執行安全檢查，這會產生 Security Hub CSPM 調查結果。您可以視需要停用和之後重新啟用個別控制項。您也可以完全停用標準。如果您停用標準，Security Hub CSPM 會停止對適用於標準的控制項執行安全檢查。問題清單不會再針對控制項產生。

除了調查結果之外，Security Hub CSPM 還會為您啟用的每個標準產生安全分數。分數是根據適用於標準之控制項的狀態。如果您設定彙總區域，標準的安全分數會反映所有連結區域中控制項的狀態。如果您是組織的 Security Hub CSPM 管理員，分數會反映組織中所有帳戶的控制項狀態。如需詳細資訊，請參閱[計算安全分數](#)。

若要檢閱和管理標準，您可以使用 Security Hub CSPM 主控台或 Security Hub CSPM API。在主控台上，安全標準頁面會顯示 Security Hub CSPM 目前支援的所有安全標準。這包括每個標準的描述，以及標準的目前狀態。如果您啟用標準，您也可以使用此頁面來存取標準的其他詳細資訊。例如，您可以檢閱：

- 標準目前的安全分數。
- 適用於標準之控制項的彙總統計資料。
- 適用於標準且目前已啟用的控制項清單，包括每個控制項的合規狀態。

- 適用於標準但目前已停用的控制項清單。

若要進行更深入的分析，您可以篩選和排序資料，並向下切入以檢閱適用於標準之個別控制項的詳細資訊。

您可以個別啟用單一帳戶和的標準 AWS 區域。不過，為了節省時間並減少多帳戶和多區域環境中的組態偏離，我們建議您使用[中央組態](#)來啟用和管理標準。透過中央組態，委派的 Security Hub CSPM 管理員可以建立政策，指定如何在多個帳戶和區域中設定標準。

主題

- [Security Hub CSPM 的標準參考](#)
- [啟用安全標準](#)
- [檢閱安全標準的詳細資訊](#)
- [關閉自動啟用的安全標準](#)
- [停用安全標準](#)

Security Hub CSPM 的標準參考

在 AWS Security Hub CSPM 中，安全標準是根據法規架構、產業最佳實務或公司政策的一組要求。Security Hub CSPM 會將這些需求映射至控制項，並對控制項執行安全檢查，以評估是否符合標準的需求。每個標準都包含多個控制項。

Security Hub CSPM 目前支援下列標準：

- AWS 基礎安全最佳實務 – 此標準由 AWS 和 業界專業人員開發，是組織安全最佳實務的編譯，無論產業或大小。它提供一組控制項，可偵測您的 AWS 帳戶 和資源何時偏離安全最佳實務。它還提供有關如何改善和維護安全狀態的規範性指導。
- AWS 資源標記 – 此標準由 Security Hub CSPM 開發，可協助您判斷 AWS 資源是否具有標籤。標籤是做為 AWS 資源中繼資料的鍵/值對。標籤可協助您識別、分類、管理和搜尋 AWS 資源。例如，您可以使用標籤，依用途、擁有者或環境來分類資源。
- CIS AWS Foundations Benchmark – 此標準由網際網路安全中心 (CIS) 開發，提供 的安全組態準則 AWS。它為 和 資源的子集指定一組安全組態準則 AWS 服務 和最佳實務，強調基礎、可測試和架構無關的設定。這些準則包括明確的step-by-step實作和評估程序。
- NIST SP 800-53 修訂版 5 – 此標準符合國家標準技術研究所 (NIST) 的要求，以保護資訊系統和關鍵資源的機密性、完整性和可用性。相關聯的架構通常適用於與美國聯邦機構或資訊系統合作的美國聯邦機構或組織。不過，私有組織也可以使用需求做為指導架構。

- NIST SP 800-171 修訂版 2 – 此標準符合 NIST 安全建議和要求，以保護不屬於美國政府的系統和組織中受控未分類資訊 (CUI) 的機密性。CUI 是不符合政府分類標準，但被視為敏感的資訊，由美國聯邦政府或代表美國聯邦政府的其他實體建立或擁有。
- PCI DSS – 此標準符合 PCI 安全標準委員會 (SSC) 定義的支付卡產業資料安全標準 (PCI DSS) 合規架構。框架提供一組規則和準則，以安全地處理信用卡和簽帳金融卡資訊。此架構通常適用於存放、處理或傳輸持卡人資料的組織。
- 服務受管標準 – AWS Control Tower 此標準可協助您設定 Security Hub CSPM 提供的偵測性控制 AWS Control Tower。AWS Control Tower 提供簡單的方法來設定和管理 AWS 多帳戶環境，並遵循規範的最佳實務。

Security Hub CSPM 標準和控制項不保證符合任何法規架構或稽核。反之，它們提供了評估和監控 AWS 帳戶 和 資源狀態的方法。我們建議您啟用與您的業務需求、產業或使用案例相關的每個標準。

個別控制項可以套用至多個標準。如果您啟用多個標準，我們建議您也啟用合併的控制調查結果。如果您這樣做，即使控制項套用到多個標準，Security Hub CSPM 也會為每個控制項產生單一問題清單。如果您未開啟合併控制調查結果，Security Hub CSPM 會為每個控制項套用的已啟用標準產生個別調查結果。例如，如果您啟用兩個標準，且控制項適用於這兩個標準，則會收到兩個單獨的控制項調查結果，每個標準各一個。如果您啟用合併的控制項問題清單，則只會收到一個控制項的問題清單。如需詳細資訊，請參閱[合併的控制問題清單](#)。

標準的詳細參考

- [AWS Security Hub CSPM 中的基礎安全最佳實務標準](#)
- [AWS Security Hub CSPM 中的資源標記標準](#)
- [Security Hub CSPM 中的 CIS AWS Foundations 基準](#)
- [Security Hub CSPM 中的 NIST SP 800-53 修訂版 5](#)
- [Security Hub CSPM 中的 NIST SP 800-171 修訂版 2](#)
- [Security Hub CSPM 中的 PCI DSS](#)
- [Security Hub CSPM 中的服務受管標準](#)

AWS Security Hub CSPM 中的基礎安全最佳實務標準

由 AWS 和業界專業人員開發，AWS 基礎安全最佳實務 (FSBP) 標準是組織安全最佳實務的編譯，無論組織部門或大小。它提供一組控制項，可偵測 AWS 帳戶 和資源何時偏離安全最佳實務。它還提供有關如何改善和維護組織安全狀態的規範性指導。

在 AWS Security Hub CSPM 中，AWS 基礎安全最佳實務標準包含持續評估 AWS 帳戶 和 工作負載的控制項，並協助您識別偏離安全最佳實務的領域。這些控制項包含來自多個 資源的安全最佳實務 AWS 服務。每個控制項都會指派一個類別，以反映控制項套用的安全函數。如需類別和其他詳細資訊的清單，請參閱 [控制類別](#)。

適用於標準的控制項

以下清單指定哪些 AWS Security Hub CSPM 控制項適用於基礎安全最佳實務標準 AWS (v1.0.0)。若要檢閱控制項的詳細資訊，請選擇控制項。

[【Account.1】 應針對 提供安全性聯絡資訊 AWS 帳戶](#)

[【ACM.1】 匯入和 ACM 發行的憑證應在指定的期間之後續約](#)

[【ACM.2】 由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)

[【APIGateway.1】 應啟用 API Gateway REST 和 WebSocket API 執行記錄](#)

[【APIGateway.2】 API Gateway REST API 階段應設定為使用 SSL 憑證進行後端身分驗證](#)

[【APIGateway.3】 API Gateway REST API 階段應該已啟用 AWS X-Ray 追蹤](#)

[【APIGateway.4】 API Gateway 應與 WAF Web ACL 建立關聯](#)

[【APIGateway.5】 API Gateway REST API 快取資料應靜態加密](#)

[【APIGateway.8】 API Gateway 路由應指定授權類型](#)

[【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)

[【APIGateway.10】 API Gateway V2 整合應使用 HTTPS 進行私有連線](#)

[【APIGateway.11】 API Gateway 網域名稱應使用建議的安全政策](#)

[【AppSync.1】 AWS AppSync API 快取應靜態加密](#)

[【AppSync.2】 AWS AppSync 應該啟用欄位層級記錄](#)

[【AppSync.5】 AWS AppSync GraphQL APIs 不應使用 API 金鑰進行身分驗證](#)

[【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)

[【Athena.4】 Athena 工作群組應該已啟用記錄](#)

[【AutoScaling.1】與負載平衡器相關聯的 Auto Scaling 群組應使用 ELB 運作狀態檢查](#)

[【AutoScaling.2】Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域](#)

[【AutoScaling.3】Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)

[【Autoscaling.5】使用 Auto Scaling 群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址](#)

[【AutoScaling.6】Auto Scaling 群組應在多個可用區域中使用多個執行個體類型](#)

[【AutoScaling.9】Amazon EC2 Auto Scaling 群組應使用 Amazon EC2 啟動範本](#)

[【Backup.1】AWS Backup 復原點應靜態加密](#)

[【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)

[【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)

[【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)

[【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)

[【CloudFormation.3】CloudFormation 堆疊應啟用終止保護](#)

[【CloudFormation.4】CloudFormation 堆疊應具有相關聯的服務角色](#)

[【CloudFront.1】CloudFront 分佈應設定預設根物件](#)

[【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)

[【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)

[【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)

[【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)

[【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)

[【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)

[【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)

[【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)

[【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)

[【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)

[【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)

[【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)

[【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)

[【CloudTrail.1】CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤](#)

[【CloudTrail.2】CloudTrail 應啟用靜態加密](#)

[【CloudTrail.4】應啟用 CloudTrail 日誌檔案驗證](#)

[【CloudTrail.5】CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合](#)

[【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料](#)

[【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料](#)

[【CodeBuild.3】CodeBuild S3 日誌應加密](#)

[【CodeBuild.4】CodeBuild AWS Config專案環境應具有記錄 URL](#)

[【CodeBuild.7】CodeBuild 報告群組匯出應靜態加密](#)

[【Cognito.2】Cognito 身分集區不應允許未驗證的身分](#)

[【Cognito.3】Cognito 使用者集區的密碼政策應具有強大的組態](#)

[【Cognito.4】Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證](#)

[【Cognito.5】應為 Cognito 使用者集區啟用 MFA](#)

[【Cognito.6】Cognito 使用者集區應啟用刪除保護](#)

[【Config.1】AWS Config 應啟用並使用服務連結角色進行資源記錄](#)

[【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)

[【DataFirehose.1】 Firehose 交付串流應靜態加密](#)

[【DataSync.1】 DataSync 任務應該已啟用記錄](#)

[【DMS.1】 Database Migration Service 複寫執行個體不應為公有](#)

[【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級](#)

[【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)

[【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)

[【DMS.9】 DMS 端點應使用 SSL](#)

[【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)

[【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制](#)

[【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)

[【DMS.13】 DMS 複寫執行個體應設定為使用多個可用區域](#)

[【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)

[【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)

[【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)

[【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)

[【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)

[【DocumentDB.6】 Amazon DocumentDB 叢集應在傳輸中加密](#)

[【DynamoDB.1】 DynamoDB 資料表應隨著需求自動擴展容量](#)

[【DynamoDB.2】 DynamoDB 資料表應該啟用point-in-time復原](#)

[【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)

[【DynamoDB.6】 DynamoDB 資料表應該已啟用刪除保護](#)

[【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)

[【EC2.1】 Amazon EBS 快照不應設定為可公開還原](#)

[【EC2.2】 VPC 預設安全群組不應允許傳入或傳出流量](#)

[【EC2.3】 連接的 Amazon EBS 磁碟區應靜態加密](#)

[【EC2.4】 已停止的 EC2 執行個體應在指定的期間之後移除](#)

[【EC2.6】 應在所有 VPC 中啟用 VPCs 流程記錄](#)

[【EC2.7】 應啟用 EBS 預設加密](#)

[【EC2.8】 EC2 執行個體應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)

[【EC2.9】 Amazon EC2 執行個體不應具有公有 IPv4 地址](#)

[【EC2.10】 Amazon EC2 應設定為使用為 Amazon EC2 服務建立的 VPC 端點](#)

[【EC2.15】 Amazon EC2 子網路不應自動指派公有 IP 地址](#)

[【EC2.16】 應該移除未使用的網路存取控制清單](#)

[【EC2.17】 Amazon EC2 執行個體不應使用多個 ENIs](#)

[【EC2.18】 安全群組應僅允許授權連接埠不受限制的傳入流量](#)

[【EC2.19】 安全群組不應允許無限制存取高風險的連接埠](#)

[【EC2.20】 用於 an AWS Site-to-Site VPN 連線的兩個 VPN 通道都應啟動](#)

[【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)

[【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)

[【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)

[【EC2.25】 Amazon EC2 啟動範本不應將公 IPs 指派給網路介面](#)

[【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)

[【EC2.55】 VPCs 應使用 ECR API 的介面端點進行設定](#)

[【EC2.56】 VPCs 應使用 Docker 登錄檔的介面端點進行設定](#)

[【EC2.57】 VPCs應使用 Systems Manager 的介面端點進行設定](#)

[【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)

[【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)

[【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)

[【EC2.171】 EC2 VPN 連線應該已啟用記錄](#)

[【EC2.172】 EC2 VPC 封鎖公開存取設定應封鎖網際網路閘道流量](#)

[【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)

[【EC2.180】 EC2 網路介面應啟用來源/目的地檢查](#)

[【EC2.181】 EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)

[【EC2.182】 應為 Amazon EBS 快照啟用封鎖公開存取設定](#)

[【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定](#)

[【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)

[【ECR.2】 ECR 私有儲存庫應設定標籤不可變性](#)

[【ECR.3】 ECR 儲存庫應至少設定一個生命週期政策](#)

[【ECS.1】 Amazon ECS 任務定義應具有安全的聯網模式和使用使用者定義](#)

[【ECS.2】 ECS 服務不應自動為其指派公有 IP 地址](#)

[【ECS.3】 ECS 任務定義不應共用主機的程序命名空間](#)

[【ECS.4】 ECS 容器應以非特殊權限執行](#)

[【ECS.5】 ECS 任務定義應將容器設定為僅限對根檔案系統的唯讀存取](#)

[【ECS.8】 不應將秘密做為容器環境變數傳遞](#)

[【ECS.9】 ECS 任務定義應具有記錄組態](#)

[【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行](#)

[【ECS.12】 ECS 叢集應使用 Container Insights](#)

[【ECS.16】 ECS 任務集不應自動指派公有 IP 地址](#)

[【ECS.18】 ECS 任務定義應針對 EFS 磁碟區使用傳輸中加密](#)

[【ECS.19】 ECS 容量提供者應啟用受管終止保護](#)

[【ECS.20】 ECS 任務定義應在 Linux 容器定義中設定非根使用者](#)

[【ECS.21】 ECS 任務定義應在 Windows 容器定義中設定非管理員使用者](#)

[【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)

[【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)

[【EFS.3】 EFS 存取點應強制執行根目錄](#)

[【EFS.4】 EFS 存取點應強制執行使用者身分](#)

[【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯](#)

[【EFS.7】 EFS 檔案系統應該啟用自動備份](#)

[【EFS.8】 EFS 檔案系統應靜態加密](#)

[【EKS.1】 不應公開存取 EKS 叢集端點](#)

[【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)

[【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密](#)

[【EKS.8】 EKS 叢集應該啟用稽核記錄](#)

[【EKS.9】 EKS 節點群組應在支援的 Kubernetes 版本上執行](#)

[【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)

[【ElastiCache.2】 ElastiCache 叢集應該啟用自動次要版本升級](#)

[【ElastiCache.3】 ElastiCache 複寫群組應該啟用自動容錯移轉](#)

[【ElastiCache.4】 ElastiCache 複寫群組應靜態加密](#)

[【ElastiCache.5】ElastiCache 複寫群組應在傳輸中加密](#)

[【ElastiCache.6】舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)

[【ElastiCache.7】ElastiCache 叢集不應使用預設子網路群組](#)

[【ElasticBeanstalk.1】Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)

[【ElasticBeanstalk.2】應啟用 Elastic Beanstalk 受管平台更新](#)

[【ElasticBeanstalk.3】Elastic Beanstalk 應將日誌串流至 CloudWatch](#)

[【ELB.1】Application Load Balancer 應設定為將所有 HTTP 請求重新導向至 HTTPS](#)

[【ELB.2】具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)

[【ELB.3】Classic Load Balancer 接聽程式應使用 HTTPS 或 TLS 終止設定](#)

[【ELB.4】Application Load Balancer 應設定為捨棄無效的 http 標頭](#)

[【ELB.5】應啟用應用程式和 Classic Load Balancer 記錄](#)

[【ELB.6】應用程式、閘道和 Network Load Balancer 應啟用刪除保護](#)

[【ELB.7】Classic Load Balancer 應啟用連線耗盡](#)

[【ELB.8】具有 SSL AWS Config接聽程式的 Classic Load Balancer 應使用預先定義的安全政策，該政策具有強烈驅動](#)

[【ELB.9】Classic Load Balancer 應啟用跨區域負載平衡](#)

[【ELB.10】Classic Load Balancer 應跨越多個可用區域](#)

[【ELB.12】Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)

[【ELB.13】應用程式、網路和閘道負載平衡器應跨越多個可用區域](#)

[【ELB.14】Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)

[【ELB.17】具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)

[【ELB.18】應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)

[【ELB.21】應用程式和 Network Load Balancer 目標群組應使用加密的運作狀態檢查通訊協定](#)

[【ELB.22】ELB 目標群組應使用加密傳輸通訊協定](#)

[【EMR.1】Amazon EMR 叢集主節點不應具有公有 IP 地址](#)

[【EMR.2】應啟用 Amazon EMR 封鎖公開存取設定](#)

[【EMR.3】Amazon EMR 安全組態應靜態加密](#)

[【EMR.4】Amazon EMR 安全組態應在傳輸中加密](#)

[【ES.1】Elasticsearch 網域應該啟用靜態加密](#)

[【ES.2】不應公開存取 Elasticsearch 網域](#)

[【ES.3】Elasticsearch 網域應該加密節點之間傳送的資料](#)

[【ES.4】應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)

[【ES.5】Elasticsearch 網域應該啟用稽核記錄](#)

[【ES.6】Elasticsearch 網域應至少具有三個資料節點](#)

[【ES.7】Elasticsearch 網域應該至少設定三個專用主節點](#)

[【ES.8】應使用最新的 TLS 安全政策加密與 Elasticsearch 網域的連線](#)

[【EventBridge.3】EventBridge 自訂事件匯流排應連接以資源為基礎的政策](#)

[【FSx.1】FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)

[【FSx.2】FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)

[【FSx.3】FSx for OpenZFS 檔案系統應設定為異地同步備份部署](#)

[【FSx.4】FSx for NetApp ONTAP 檔案系統應設定為異地同步備份部署](#)

[【FSx.5】FSx for Windows File Server 檔案系統應設定為異地同步備份部署](#)

[【Glue.3】AWS Glue 機器學習轉換應該靜態加密](#)

[【Glue.4】AWS Glue Spark 任務應在支援的版本上執行 AWS Glue](#)

[【GuardDuty.1】應啟用 GuardDuty](#)

[【GuardDuty.5】應啟用 GuardDuty EKS 稽核日誌監控](#)

[【GuardDuty.6】應啟用 GuardDuty Lambda 保護](#)

[【GuardDuty.7】應啟用 GuardDuty EKS 執行期監控](#)

[【GuardDuty.8】應啟用 EC2 的 GuardDuty 惡意軟體防護](#)

[【GuardDuty.9】應啟用 GuardDuty RDS 保護](#)

[【GuardDuty.10】應啟用 GuardDuty S3 保護](#)

[【GuardDuty.11】應啟用 GuardDuty 執行期監控](#)

[【GuardDuty.12】應啟用 GuardDuty ECS 執行期監控](#)

[【GuardDuty.13】應啟用 GuardDuty EC2 執行期監控](#)

[【IAM.1】IAM 政策不應允許完整的「*」管理權限](#)

[【IAM.2】IAM 使用者不應連接 IAM 政策](#)

[【IAM.3】IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)

[【IAM.4】IAM 根使用者存取金鑰不應存在](#)

[【IAM.5】應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)

[【IAM.6】應為根使用者啟用硬體 MFA](#)

[【IAM.7】IAM 使用者的密碼政策應具有強大的組態](#)

[【IAM.8】應移除未使用的 IAM 使用者登入資料](#)

[【IAM.21】您建立的 IAM 客戶受管政策不應允許服務的萬用字元動作](#)

[【Inspector.1】應啟用 Amazon Inspector EC2 掃描](#)

[【Inspector.2】應啟用 Amazon Inspector ECR 掃描](#)

[【Inspector.3】應啟用 Amazon Inspector Lambda 程式碼掃描](#)

[【Inspector.4】應啟用 Amazon Inspector Lambda 標準掃描](#)

[【Kinesis.1】Kinesis 串流應靜態加密](#)

[【Kinesis.3】Kinesis 串流應具有足夠的資料保留期](#)

[【KMS.1】IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)

[【KMS.2】IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)

[【KMS.3】AWS KMS keys 不應意外刪除](#)

[【KMS.5】不應公開存取 KMS 金鑰](#)

[【Lambda.1】Lambda 函數政策應禁止公開存取](#)

[【Lambda.2】Lambda 函數應使用支援的執行時間](#)

[【Lambda.5】VPC Lambda 函數應該在多個可用區域中操作](#)

[【Macie.1】應啟用 Amazon Macie](#)

[【Macie.2】應啟用 Macie 自動化敏感資料探索](#)

[【MQ.2】ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)

[【MQ.3】Amazon MQ 代理程式應該啟用自動次要版本升級](#)

[【MSK.1】MSK 叢集應在代理程式節點之間傳輸時加密](#)

[【MSK.3】MSK Connect 連接器應在傳輸中加密](#)

[【MSK.4】MSK 叢集應停用公有存取](#)

[【MSK.5】MSK 連接器應該已啟用記錄](#)

[【MSK.6】MSK 叢集應停用未驗證的存取](#)

[【Neptune.1】Neptune 資料庫叢集應靜態加密](#)

[【Neptune.2】Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)

[【Neptune.3】Neptune 資料庫叢集快照不應公開](#)

[【Neptune.4】Neptune 資料庫叢集應啟用刪除保護](#)

[【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)

[【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)

[【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)

[【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)

[【NetworkFirewall.2】 應啟用網路防火牆記錄](#)

[【NetworkFirewall.3】 網路防火牆政策應至少有一個相關聯的規則群組](#)

[【NetworkFirewall.4】 Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)

[【NetworkFirewall.5】 網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)

[【NetworkFirewall.6】 無狀態網路防火牆規則群組不應為空](#)

[【NetworkFirewall.9】 網路防火牆防火牆應啟用刪除保護](#)

[【NetworkFirewall.10】 網路防火牆防火牆應啟用子網路變更保護](#)

[【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)

[【Opensearch.2】 不應公開存取 OpenSearch 網域](#)

[【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)

[【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)

[【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)

[【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)

[【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)

[【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)

[【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)

[【PCA.1】 應停用 AWS 私有 CA 根憑證授權單位](#)

[【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)

[【RDS.1】 RDS 快照應為私有](#)

[【RDS.2】 RDS 資料庫執行個體應禁止公開存取，由 PubliclyAccessible 組態決定](#)

[\[RDS.3\] RDS 資料庫執行個體應啟用靜態加密](#)

[【RDS.4】 RDS 叢集快照和資料庫快照應靜態加密](#)

[【RDS.5】 RDS 資料庫執行個體應該設定多個可用區域](#)

[【RDS.6】 應為 RDS 資料庫執行個體設定增強型監控](#)

[【RDS.7】 RDS 叢集應該啟用刪除保護](#)

[【RDS.8】 RDS 資料庫執行個體應啟用刪除保護](#)

[【RDS.9】 RDS 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)

[【RDS.10】 應為 RDS 執行個體設定 IAM 身分驗證](#)

[【RDS.11】 RDS 執行個體應該啟用自動備份](#)

[【RDS.12】 應為 RDS 叢集設定 IAM 身分驗證](#)

[【RDS.13】 應啟用 RDS 自動次要版本升級](#)

[【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)

[【RDS.15】 應為多個可用區域設定 RDS 資料庫叢集](#)

[【RDS.16】 Aurora 資料庫叢集應設定為將標籤複製到資料庫快照](#)

[【RDS.17】 RDS 資料庫執行個體應設定為將標籤複製到快照](#)

[【RDS.19】 應為關鍵叢集事件設定現有的 RDS 事件通知訂閱](#)

[【RDS.20】 應為關鍵資料庫執行個體事件設定現有的 RDS 事件通知訂閱](#)

[【RDS.21】 應為關鍵資料庫參數群組事件設定 RDS 事件通知訂閱](#)

[【RDS.22】 應為關鍵資料庫安全群組事件設定 RDS 事件通知訂閱](#)

[【RDS.23】 RDS 執行個體不應使用資料庫引擎預設連接埠](#)

[【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱](#)

[【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)

[【RDS.27】 RDS 資料庫叢集應靜態加密](#)

[【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)

[【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)

[【RDS.36】 RDS for PostgreSQL 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)

[【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)

[【RDS.40】 RDS for SQL Server 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)

[【RDS.41】 RDS for SQL Server 資料庫執行個體應在傳輸中加密](#)

[【RDS.42】 RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)

[【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密](#)

[【RDS.44】 RDS for MariaDB 資料庫執行個體應在傳輸中加密](#)

[【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)

[【RDS.46】 RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中](#)

[【RDS.47】 RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)

[【RDS.48】 RDS for MySQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)

[【RDS.50】 RDS 資料庫叢集應設定足夠的備份保留期間](#)

[【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)

[【Redshift.1】 Amazon Redshift 叢集應禁止公開存取](#)

[【Redshift.2】 與 Amazon Redshift 叢集的連線應在傳輸中加密](#)

[【Redshift.3】 Amazon Redshift 叢集應該啟用自動快照](#)

[【Redshift.4】 Amazon Redshift 叢集應該啟用稽核記錄](#)

[【Redshift.6】 Amazon Redshift 應已啟用主要版本的自動升級](#)

[【Redshift.7】 Redshift 叢集應使用增強型 VPC 路由](#)

[【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱](#)

[【Redshift.10】 應靜態加密 Redshift 叢集](#)

[【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠](#)

[【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)

[【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)

[【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)

[【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)

[【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)

[【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)

[【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定](#)

[【S3.2】 S3 一般用途儲存貯體應封鎖公開讀取存取](#)

[【S3.3】 S3 一般用途儲存貯體應封鎖公有寫入存取](#)

[【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL](#)

[【S3.6】 S3 一般用途儲存貯體政策應限制對其他 的存取 AWS 帳戶](#)

[【S3.8】 S3 一般用途儲存貯體應封鎖公開存取](#)

[【S3.9】 S3 一般用途儲存貯體應啟用伺服器存取記錄](#)

[【S3.12】 ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取](#)

[【S3.13】 S3 一般用途儲存貯體應具有生命週期組態](#)

[【S3.19】 S3 存取點應啟用封鎖公開存取設定](#)

[【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)

[【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)

[【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)

[【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)

[【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)

[【SageMaker.4】SageMaker 端點生產變體的初始執行個體計數應大於 1](#)

[【SageMaker.5】SageMaker 模型應該啟用網路隔離](#)

[【SageMaker.8】SageMaker 筆記本執行個體應在支援的平台上執行](#)

[【SageMaker.9】SageMaker 資料品質任務定義應該啟用容器間流量加密](#)

[【SageMaker.10】SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)

[【SageMaker.11】SageMaker 資料品質任務定義應該啟用網路隔離](#)

[【SageMaker.12】SageMaker 模型偏差任務定義應該啟用網路隔離](#)

[【SageMaker.13】SageMaker 模型品質任務定義應該啟用容器間流量加密](#)

[【SageMaker.14】SageMaker 監控排程應該啟用網路隔離](#)

[【SageMaker.15】SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)

[【SageMaker.16】SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)

[【SageMaker.17】SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)

[【SageMaker.19】SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)

[【SecretsManager.1】Secrets Manager 秘密應該已啟用自動輪換](#)

[【SecretsManager.2】設定自動輪換的 Secrets Manager 秘密應能成功輪換](#)

[【SecretsManager.3】移除未使用的 Secrets Manager 秘密](#)

[【SecretsManager.4】Secrets Manager 秘密應在指定的天數內輪換](#)

[【ServiceCatalog.1】Service Catalog 產品組合只能在 AWS 組織內共用](#)

[【SES.3】SES 組態集應啟用 TLS 以傳送電子郵件](#)

[【SNS.4】SNS 主題存取政策不應允許公開存取](#)

[【SQS.1】Amazon SQS 佇列應靜態加密](#)

[【SQS.3】SQS 佇列存取政策不應允許公開存取](#)

[【SSM.1】Amazon EC2 執行個體應該由 管理 AWS Systems Manager](#)

[【SSM.2】 Systems Manager 管理的 Amazon EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態](#)

[【SSM.3】 Systems Manager 管理的 Amazon EC2 執行個體應具有 COMPLIANT 的關聯合規狀態](#)

[【SSM.4】 SSM 文件不應公開](#)

[【SSM.6】 SSM Automation 應該啟用 CloudWatch 記錄](#)

[【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)

[【StepFunctions.1】 Step Functions 狀態機器應該已開啟記錄](#)

[【Transfer.2】 Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線](#)

[【Transfer.3】 Transfer Family 連接器應該已啟用記錄](#)

[【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)

[【WAF.2】 AWS WAF 傳統區域規則應至少有一個條件](#)

[【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)

[【WAF.4】 AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組](#)

[【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)

[【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)

[【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

[【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)

[【WAF.12】 AWS WAF 規則應啟用 CloudWatch 指標](#)

[【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)

[【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

AWS Security Hub CSPM 中的資源標記標準

AWS Security Hub CSPM 開發 AWS 的資源標記標準可協助您判斷 AWS 資源是否遺失標籤。標籤是鍵/值對，可做為組織 AWS 資源的中繼資料。對於大多數 AWS 資源，您可以在建立資源時或建立資源

之後，選擇將標籤新增至資源。資源的範例包括 Amazon CloudFront 分佈、Amazon Elastic Compute Cloud (Amazon EC2) 執行個體和 中的秘密 AWS Secrets Manager。標籤可協助您管理、識別、組織、搜尋和篩選 AWS 資源。

每個 標籤都有兩個部分：

- 標籤索引鍵 - 例如 CostCenter、Environment 或 Project。標籤金鑰會區分大小寫。
- 標籤值 - 例如，111122223333 或 Production。與標籤金鑰相同，標籤值會區分大小寫。

您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。如需將標籤新增至 AWS 資源的詳細資訊，請參閱 [標記 AWS 資源和標籤編輯器使用者指南](#)。

對於適用於 Security Hub CSPM 中 AWS 資源標記標準的每個控制項，您可以選擇使用支援的參數來指定要控制項檢查的標籤金鑰。如果您未指定任何標籤索引鍵，控制項只會檢查是否存在至少一個標籤索引鍵，如果資源沒有任何標籤索引鍵，則 會失敗。

啟用 AWS 資源標記標準之前，請務必在其中啟用和設定資源記錄 AWS Config。當您設定資源記錄時，也請務必針對套用標準之控制項檢查的所有 AWS 資源類型啟用它。否則，Security Hub CSPM 可能無法評估適當的資源，並為適用於標準的控制項產生準確的調查結果。如需詳細資訊，包括要記錄的資源類型清單，請參閱 [控制問題清單所需的 AWS Config 資源](#)。

啟用 AWS 資源標記標準之後，您會開始接收適用於標準之控制項的調查結果。請注意，Security Hub CSPM 最多可能需要 18 小時才能產生控制項的問題清單，這些控制項使用相同的 AWS Config 服務連結規則做為適用於其他已啟用標準的控制項。如需詳細資訊，請參閱 [執行安全檢查的排程](#)。

AWS 資源標記標準具有下列 Amazon Resource Name

(ARN)：arn:aws:securityhub:*region*::standards/aws-resource-tagging-standard/v/1.0.0，其中 *region* 是適用的區域代碼 AWS 區域。您也可以使用 Security Hub CSPM API 的 [GetEnabledStandards](#) 操作來擷取目前啟用的標準 ARN。

 Note

[AWS 資源標記標準](#) 不適用於亞太區域（紐西蘭）和亞太區域（台北）區域。

適用於標準的控制項

下列清單指定哪些 AWS Security Hub CSPM 控制項適用於 AWS 資源標記標準 (v1.0.0)。若要檢閱控制項的詳細資訊，請選擇控制項。

- [【ACM.3】 ACM 憑證應加上標籤](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppConfig.1】 AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】 AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】 AWS AppConfig 環境應加上標籤](#)
- [【AppConfig.4】 AWS AppConfig 應標記延伸關聯](#)
- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)
- [【AppSync.4】 AWS AppSync GraphQL APIs應加上標籤](#)
- [【Athena.2】 應標記 Athena 資料目錄](#)
- [【Athena.3】 應標記 Athena 工作群組](#)
- [【AutoScaling.10】 應標記 EC2 Auto Scaling 群組](#)
- [【Backup.2】 AWS Backup 復原點應加上標籤](#)
- [【Backup.3】 保存 AWS Backup 庫應加上標籤](#)
- [【Backup.4】 應標記 AWS Backup 報告計劃](#)
- [【Backup.5】 AWS Backup 備份計劃應加上標籤](#)
- [【Batch.1】 批次任務佇列應加上標籤](#)
- [【Batch.2】 批次排程政策應加上標籤](#)
- [【Batch.3】 批次運算環境應加上標籤](#)
- [【Batch.4】 應標記受管批次運算環境中的運算資源屬性](#)
- [【CloudFormation.2】 應標記 CloudFormation 堆疊](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudTrail.9】 應標記 CloudTrail 追蹤](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【DataSync.2】 應標記 DataSync 任務](#)

- [【Detective.1】 應標記 Detective 行為圖表](#)
- [【DMS.2】 DMS 憑證應加上標籤](#)
- [【DMS.3】 DMS 事件訂閱應加上標籤](#)
- [【DMS.4】 DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】 DMS 複寫子網路群組應加上標籤](#)
- [【DynamoDB.5】 DynamoDB 資料表應加上標籤](#)
- [【EC2.33】 EC2 傳輸閘道附件應加上標籤](#)
- [【EC2.34】 EC2 傳輸閘道路由表應加上標籤](#)
- [【EC2.35】 EC2 網路介面應加上標籤](#)
- [【EC2.36】 EC2 客戶閘道應加上標籤](#)
- [【EC2.37】 EC2 彈性 IP 地址應加上標籤](#)
- [【EC2.38】 應標記 EC2 執行個體](#)
- [【EC2.39】 EC2 網際網路閘道應加上標籤](#)
- [【EC2.40】 EC2 NAT 閘道應加上標籤](#)
- [【EC2.41】 EC2 網路 ACLs 應加上標籤](#)
- [【EC2.42】 EC2 路由表應加上標籤](#)
- [【EC2.43】 EC2 安全群組應加上標籤](#)
- [【EC2.44】 EC2 子網路應加上標籤](#)
- [【EC2.45】 EC2 磁碟區應加上標籤](#)
- [【EC2.46】 Amazon VPCs 應加上標籤](#)
- [【EC2.47】 Amazon VPC 端點服務應加上標籤](#)
- [【EC2.48】 Amazon VPC 流程日誌應加上標籤](#)
- [【EC2.49】 Amazon VPC 互連連線應加上標籤](#)
- [【EC2.50】 EC2 VPN 閘道應加上標籤](#)
- [【EC2.52】 EC2 傳輸閘道應加上標籤](#)
- [【EC2.174】 EC2 DHCP 選項集應加上標籤](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.176】 EC2 字首清單應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.178】 應標記 EC2 流量鏡像篩選條件](#)

- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ECS.13】 ECS 服務應加上標籤](#)
- [【ECS.14】 ECS 叢集應加上標籤](#)
- [【ECS.15】 ECS 任務定義應加上標籤](#)
- [【EFS.5】 EFS 存取點應加上標籤](#)
- [【EKS.6】 EKS 叢集應加上標籤](#)
- [【EKS.7】 EKS 身分提供者組態應加上標籤](#)
- [【ES.9】 應標記 Elasticsearch 網域](#)
- [【EventBridge.2】 應標記 EventBridge 事件匯流排](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【Glue.1】 AWS Glue 工作應加上標籤](#)
- [【GuardDuty.2】 GuardDuty 篩選條件應加上標籤](#)
- [【GuardDuty.3】 GuardDuty IPSets 應加上標籤](#)
- [【GuardDuty.4】 GuardDuty 偵測器應加上標籤](#)
- [【IAM.23】 IAM Access Analyzer 分析器應加上標籤](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】 AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】 AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】 AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)

- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtTwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtTwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtTwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtTwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Kinesis.2】 Kinesis 串流應加上標籤](#)
- [【Lambda.6】 應標記 Lambda 函數](#)
- [【MQ.4】 Amazon MQ 代理程式應加上標籤](#)
- [【NetworkFirewall.7】 應標記網路防火牆](#)
- [【NetworkFirewall.8】 應標記網路防火牆防火牆政策](#)
- [【Opensearch.9】 應標記 OpenSearch 網域](#)
- [【PCA.2】 應標記 AWS 私有 CA 憑證授權單位](#)
- [【RDS.28】 RDS 資料庫叢集應加上標籤](#)
- [【RDS.29】 應標記 RDS 資料庫叢集快照](#)
- [【RDS.30】 RDS 資料庫執行個體應加上標籤](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.32】 RDS 資料庫快照應加上標籤](#)
- [【RDS.33】 RDS 資料庫子網路群組應加上標籤](#)

- [【Redshift.11】應標記 Redshift 叢集](#)
- [【Redshift.12】應標記 Redshift 事件通知訂閱](#)
- [【Redshift.13】應標記 Redshift 叢集快照](#)
- [【Redshift.14】應標記 Redshift 叢集子網路群組](#)
- [【Redshift.17】應標記 Redshift 叢集參數群組](#)
- [【Route53.1】應標記 Route 53 運作狀態檢查](#)
- [【SageMaker.6】應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】應標記 SageMaker 映像](#)
- [【SecretsManager.5】Secrets Manager 秘密應加上標籤](#)
- [【SES.1】SES 聯絡人清單應加上標籤](#)
- [【SES.2】SES 組態集應加上標籤](#)
- [【SNS.3】SNS 主題應加上標籤](#)
- [【SQS.2】SQS 佇列應加上標籤](#)
- [【SSM.5】SSM 文件應加上標籤](#)
- [【StepFunctions.2】應標記 Step Functions 活動](#)
- [【Transfer.1】AWS Transfer Family 工作流程應加上標籤](#)
- [【Transfer.4】Transfer Family 協議應加上標籤](#)
- [【Transfer.5】Transfer Family 憑證應加上標籤](#)
- [【Transfer.6】Transfer Family 連接器應加上標籤](#)
- [【Transfer.7】轉移系列設定檔應加上標籤](#)

Security Hub CSPM 中的 CIS AWS Foundations 基準

Center for Internet Security (CIS) AWS Foundations Benchmark 可做為一組安全組態最佳實務 AWS。這些業界認可的最佳實務可為您提供清晰的step-by-step實作和評估程序。從作業系統到雲端服務和網路裝置，此基準中的控制項可協助您保護組織使用的特定系統。

AWS Security Hub CSPM 支援 CIS AWS Foundations Benchmark 5.0.0、3.0.0、1.4.0 和 1.2.0 版。此頁面列出每個版本支援的安全性控制項。它也提供 版本的比較。

CIS AWS Foundations Benchmark 5.0.0 版

Security Hub CSPM 支援 CIS AWS Foundations Benchmark 的 5.0.0 版 (5.0.0 版)。Security Hub CSPM 已滿足 CIS 安全軟體認證的要求，並已獲得下列 CIS 基準的 CIS 安全軟體認證：

- CIS AWS Foundations Benchmark 的 CIS 基準，第 5.0.0 版，第 1 級
- CIS AWS Foundations Benchmark 的 CIS 基準指標，第 5.0.0 版，第 2 級

適用於 CIS AWS Foundations Benchmark 5.0.0 版的控制項

[【Account.1】 應針對 提供安全性聯絡資訊 AWS 帳戶](#)

[【CloudTrail.1】 CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤](#)

[\[CloudTrail.2\] CloudTrail 應啟用靜態加密](#)

[【CloudTrail.4】 應啟用 CloudTrail 日誌檔案驗證](#)

[【CloudTrail.7】 確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)

[【Config.1】 AWS Config 應啟用並使用服務連結角色進行資源記錄](#)

[【EC2.2】 VPC 預設安全群組不應允許傳入或傳出流量](#)

[【EC2.6】 應在所有 VPC 中啟用 VPCs 流程記錄](#)

[【EC2.7】 應啟用 EBS 預設加密](#)

[【EC2.8】 EC2 執行個體應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)

[【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)

[【EC2.53】 EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠](#)

[【EC2.54】 EC2 安全群組不應允許從 :::/0 傳入遠端伺服器管理連接埠](#)

[【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)

[【EFS.8】 EFS 檔案系統應靜態加密](#)

[【IAM.2】 IAM 使用者不應連接 IAM 政策](#)

[【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)

[【IAM.4】 IAM 根使用者存取金鑰不應存在](#)

[\[IAM.5\] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)

[\[IAM.6\] 應為根使用者啟用硬體 MFA](#)

[【IAM.9】 應為根使用者啟用 MFA](#)

[【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)

[【IAM.16】 確保 IAM 密碼政策防止密碼重複使用](#)

[【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)

[【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)

[【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)

[【IAM.27】 IAM 身分不應連接 AWSCloudShellFullAccess 政策](#)

[【IAM.28】 應啟用 IAM Access Analyzer 外部存取分析器](#)

[【KMS.4】 應啟用 AWS KMS 金鑰輪換](#)

[【RDS.2】 RDS 資料庫執行個體應禁止公開存取，由 PubliclyAccessible 組態決定](#)

[\[RDS.3\] RDS 資料庫執行個體應啟用靜態加密](#)

[【RDS.5】 RDS 資料庫執行個體應該設定多個可用區域](#)

[【RDS.13】 應啟用 RDS 自動次要版本升級](#)

[【RDS.15】 應為多個可用區域設定 RDS 資料庫叢集](#)

[【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定](#)

[【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL](#)

[【S3.8】 S3 一般用途儲存貯體應封鎖公開存取](#)

[【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除](#)

[【S3.22】 S3 一般用途儲存貯體應記錄物件層級寫入事件](#)

[【S3.23】 S3 一般用途儲存貯體應記錄物件層級讀取事件](#)

CIS AWS Foundations Benchmark 3.0.0 版

Security Hub CSPM 支援 CIS AWS Foundations Benchmark 的 3.0.0 版 (v3.0.0)。Security Hub CSPM 已滿足 CIS 安全軟體認證的要求，並已獲得下列 CIS 基準的 CIS 安全軟體認證：

- CIS AWS Foundations Benchmark 的 CIS Benchmark，第 3.0.0 版，第 1 級
- CIS AWS Foundations Benchmark 的 CIS 基準指標，第 3.0.0 版，第 2 級

適用於 CIS AWS Foundations Benchmark 3.0.0 版的控制項

[【Account.1】應針對提供安全性聯絡資訊 AWS 帳戶](#)

[【CloudTrail.1】CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤](#)

[【CloudTrail.2】CloudTrail 應啟用靜態加密](#)

[【CloudTrail.4】應啟用 CloudTrail 日誌檔案驗證](#)

[【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)

[【Config.1】AWS Config 應啟用並使用服務連結角色進行資源記錄](#)

[【EC2.2】VPC 預設安全群組不應允許傳入或傳出流量](#)

[【EC2.6】應在所有 VPC 中啟用 VPCs 流程記錄](#)

[【EC2.7】應啟用 EBS 預設加密](#)

[【EC2.8】EC2 執行個體應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)

[【EC2.21】網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)

[【EC2.53】EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠](#)

[【EC2.54】EC2 安全群組不應允許從 :::/0 傳入遠端伺服器管理連接埠](#)

[【EFS.1】彈性檔案系統應設定為使用加密靜態檔案資料 AWS KMS](#)

[【IAM.2】IAM 使用者不應連接 IAM 政策](#)

[【IAM.3】IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)

[【IAM.4】IAM 根使用者存取金鑰不應存在](#)

[【IAM.5】應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)

[【IAM.6】應為根使用者啟用硬體 MFA](#)

[【IAM.9】 應為根使用者啟用 MFA](#)

[【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)

[【IAM.16】 確保 IAM 密碼政策防止密碼重複使用](#)

[【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)

[【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)

[【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)

[【IAM.27】 IAM 身分不應連接 AWSCloudShellFullAccess 政策](#)

[【IAM.28】 應啟用 IAM Access Analyzer 外部存取分析器](#)

[【KMS.4】 應啟用 AWS KMS 金鑰輪換](#)

[【RDS.2】 RDS 資料庫執行個體應禁止公開存取，由 PubliclyAccessible 組態決定](#)

[【RDS.3】 RDS 資料庫執行個體應啟用靜態加密](#)

[【RDS.13】 應啟用 RDS 自動次要版本升級](#)

[【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定](#)

[【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL](#)

[【S3.8】 S3 一般用途儲存貯體應封鎖公開存取](#)

[【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除](#)

[【S3.22】 S3 一般用途儲存貯體應記錄物件層級寫入事件](#)

[【S3.23】 S3 一般用途儲存貯體應記錄物件層級讀取事件](#)

CIS AWS Foundations Benchmark 1.4.0 版

Security Hub CSPM 支援 CIS AWS Foundations Benchmark 的 1.4.0 版 (1.4.0 版)。

適用於 CIS AWS Foundations Benchmark 1.4.0 版的控制項

[【CloudTrail.1】 CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤](#)

[\[CloudTrail.2\] CloudTrail 應啟用靜態加密](#)[【CloudTrail.4】應啟用 CloudTrail 日誌檔案驗證](#)[【CloudTrail.5】CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合](#)[【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)[【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)[【CloudWatch.1】應該存在日誌指標篩選條件和警示以使用「根」使用者](#)[【CloudWatch.4】確保 IAM 政策變更存在日誌指標篩選條件和警示](#)[【CloudWatch.5】確保 CloudTrail 組態變更存在日誌指標篩選條件和警示](#)[【CloudWatch.6】確保 AWS 管理主控台 驗證失敗時存在日誌指標篩選條件和警示](#)[【CloudWatch.7】確保日誌指標篩選條件和警示存在，以停用或排程刪除客戶受管金鑰](#)[【CloudWatch.8】確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示](#)[【CloudWatch.9】確保 AWS Config 組態變更存在日誌指標篩選條件和警示](#)[【CloudWatch.10】確保安全群組變更存在日誌指標篩選條件和警示](#)[【CloudWatch.11】確定網路存取控制清單 \(NACL\) 的變更存在日誌指標篩選條件和警示](#)[【CloudWatch.12】確保網路閘道變更存在日誌指標篩選條件和警示](#)[【CloudWatch.13】確保路由表變更存在日誌指標篩選條件和警示](#)[【CloudWatch.14】確保 VPC 變更存在日誌指標篩選條件和警示](#)[【Config.1】AWS Config 應啟用並使用服務連結角色進行資源記錄](#)[【EC2.2】VPC 預設安全群組不應允許傳入或傳出流量](#)[【EC2.6】應在所有 VPC 中啟用 VPCs 流程記錄](#)[【EC2.7】應啟用 EBS 預設加密](#)[【EC2.21】網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)

[【IAM.1】 IAM 政策不應允許完整的「*」管理權限](#)

[【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)

[【IAM.4】 IAM 根使用者存取金鑰不應存在](#)

[\[IAM.5\] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)

[\[IAM.6\] 應為根使用者啟用硬體 MFA](#)

[【IAM.9】 應為根使用者啟用 MFA](#)

[【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)

[【IAM.16】 確保 IAM 密碼政策防止密碼重複使用](#)

[【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)

[【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)

[【KMS.4】 應啟用 AWS KMS 金鑰輪換](#)

[\[RDS.3\] RDS 資料庫執行個體應啟用靜態加密](#)

[【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定](#)

[【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL](#)

[【S3.8】 S3 一般用途儲存貯體應封鎖公開存取](#)

[【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除](#)

CIS AWS Foundations Benchmark 1.2.0 版

Security Hub CSPM 支援 CIS AWS Foundations Benchmark 的 1.2.0 版 (1.2.0 版)。Security Hub CSPM 已滿足 CIS 安全軟體認證的要求，並已獲得下列 CIS 基準的 CIS 安全軟體認證：

- CIS AWS Foundations Benchmark 的 CIS 基準，第 1.2.0 版，第 1 級
- CIS AWS Foundations Benchmark 的 CIS Benchmark，第 1.2.0 版，第 2 級

適用於 CIS AWS Foundations Benchmark 1.2.0 版的控制項

[【CloudTrail.1】 CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤](#)

[\[CloudTrail.2\] CloudTrail 應啟用靜態加密](#)[【CloudTrail.4】應啟用 CloudTrail 日誌檔案驗證](#)[【CloudTrail.5】CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合](#)[【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)[【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)[【CloudWatch.1】應該存在日誌指標篩選條件和警示以使用「根」使用者](#)[【CloudWatch.2】確保未經授權的 API 呼叫存在日誌指標篩選條件和警示](#)[【CloudWatch.3】確保沒有 MFA 的管理主控台登入存在日誌指標篩選條件和警示](#)[【CloudWatch.4】確保 IAM 政策變更存在日誌指標篩選條件和警示](#)[【CloudWatch.5】確保 CloudTrail 組態變更存在日誌指標篩選條件和警示](#)[【CloudWatch.6】確保 AWS 管理主控台 驗證失敗時存在日誌指標篩選條件和警示](#)[【CloudWatch.7】確保日誌指標篩選條件和警示存在，以停用或排程刪除客戶受管金鑰](#)[【CloudWatch.8】確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示](#)[【CloudWatch.9】確保 AWS Config 組態變更存在日誌指標篩選條件和警示](#)[【CloudWatch.10】確保安全群組變更存在日誌指標篩選條件和警示](#)[【CloudWatch.11】確定網路存取控制清單 \(NACL\) 的變更存在日誌指標篩選條件和警示](#)[【CloudWatch.12】確保網路閘道變更存在日誌指標篩選條件和警示](#)[【CloudWatch.13】確保路由表變更存在日誌指標篩選條件和警示](#)[【CloudWatch.14】確保 VPC 變更存在日誌指標篩選條件和警示](#)[【Config.1】AWS Config 應啟用並使用服務連結角色進行資源記錄](#)[【EC2.2】VPC 預設安全群組不應允許傳入或傳出流量](#)[【EC2.6】應在所有 VPC 中啟用 VPCs 流程記錄](#)[【EC2.13】安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 22](#)

[【EC2.14】安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389](#)

[【IAM.1】IAM 政策不應允許完整的「*」管理權限](#)

[【IAM.2】IAM 使用者不應連接 IAM 政策](#)

[【IAM.3】IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)

[【IAM.4】IAM 根使用者存取金鑰不應存在](#)

[\[IAM.5\] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)

[\[IAM.6\] 應為根使用者啟用硬體 MFA](#)

[【IAM.8】應移除未使用的 IAM 使用者登入資料](#)

[【IAM.9】應為根使用者啟用 MFA](#)

[【IAM.11】確保 IAM 密碼政策至少需要一個大寫字母](#)

[【IAM.12】確保 IAM 密碼政策至少需要一個小寫字母](#)

[【IAM.13】確保 IAM 密碼政策至少需要一個符號](#)

[【IAM.14】確保 IAM 密碼政策至少需要一個數字](#)

[【IAM.15】確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)

[【IAM.16】確保 IAM 密碼政策防止密碼重複使用](#)

[【IAM.17】確保 IAM 密碼政策在 90 天內過期密碼](#)

[【IAM.18】確保已建立支援角色來使用管理事件 AWS 支援](#)

[【KMS.4】應啟用 AWS KMS 金鑰輪換](#)

CIS AWS Foundations Benchmark 的版本比較

本節摘要說明 Center for Internet Security (CIS) AWS Foundations Benchmark—

v5.0.0、v3.0.0、v1.4.0 和 v1.2.0 的特定版本之間的差異。AWS Security Hub CSPM 支援 CIS AWS Foundations Benchmark 的每個版本。不過，我們建議您使用 v5.0.0 來保持最新的安全最佳實務。您可以同時啟用多個版本的 CIS AWS Foundations Benchmark 標準。如需啟用標準的資訊，請參閱 [啟用安全標準](#)。如果您想要升級至 v5.0.0，請在停用舊版之前啟用它。這可以防止安全檢查中的差距。如

果您使用 Security Hub CSPM 與 整合，AWS Organizations 並想要在多個帳戶中批次啟用 v5.0.0，我們建議您使用[中央組態](#)。

將控制項映射至每個版本中的 CIS 需求

了解哪些 控制 CIS AWS Foundations Benchmark 支援的每個版本。

控制項 ID 和標題	CIS v5.0.0 需求	CIS v3.0.0 需求	CIS v1.4.0 需求	CIS v1.2.0 需求
【Account.1】應針對提供安全性聯絡資訊 AWS 帳戶	1.2	1.2	1.2	1.18
【CloudTrail.1】CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤	3.1	3.1	3.1	2.1
【CloudTrail.2】CloudTrail 應該啟用靜態加密	3.5	3.5	3.7	2.7
【CloudTrail.4】應啟用 CloudTrail 日誌檔案驗證	3.2	3.2	3.2	2.2
【CloudTrail.5】CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	3.4	2.4
【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	3.3	2.3
【CloudTrail.7】確定 CloudTrail 在 S3 儲存貯體上已啟用 S3 儲存貯體存取記錄	3.4	3.4	3.6	2.6
【CloudWatch.1】應該存在日誌指標篩選條件和警示以使用「根」使用者	不支援 – 手動檢查	不支援 – 手動檢查	4.3	3.3

控制項 ID 和標題	CIS v5.0.0 需求	CIS v3.0.0 需求	CIS v1.4.0 需求	CIS v1.2.0 需求
【CloudWatch.2】確保未經授權的 API 呼叫存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	不支援 – 手動檢查	3.1
【CloudWatch.3】確保沒有 MFA 的管理主控台登入存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	不支援 – 手動檢查	3.2
【CloudWatch.4】確保 IAM 政策變更存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	4.4	3.4
【CloudWatch.5】確保 CloudTrail 組態變更存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	4.5	3.5
【CloudWatch.6】確保 AWS 管理主控台 驗證失敗時存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	4.6	3.6
【CloudWatch.7】確保日誌指標篩選條件和警示存在，以停用或排程刪除客戶受管金鑰	不支援 – 手動檢查	不支援 – 手動檢查	4.7	3.7
【CloudWatch.8】確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	4.8	3.8
【CloudWatch.9】確保 AWS Config 組態變更存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	4.9	3.9
【CloudWatch.10】確保安全群組變更存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	4.10	3.10

控制項 ID 和標題	CIS v5.0.0 需求	CIS v3.0.0 需求	CIS v1.4.0 需求	CIS v1.2.0 需求
【CloudWatch.11】確定網路存取控制清單 (NACL) 的變更存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	4.11	3.11
【CloudWatch.12】確保網路閘道變更存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	4.12	3.12
【CloudWatch.13】確保路由表變更存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	4.13	3.13
【CloudWatch.14】確保 VPC 變更存在日誌指標篩選條件和警示	不支援 – 手動檢查	不支援 – 手動檢查	4.14	3.14
【Config.1】AWS Config 應啟用並使用服務連結角色進行資源記錄	3.3	3.3	3.5	2.5
【EC2.2】VPC 預設安全群組不應允許傳入或傳出流量	5.5	5.4	5.3	4.3
【EC2.6】應在所有 VPC 中啟用 VPCs 流程記錄	3.7	3.7	3.9	2.9
【EC2.7】應啟用 EBS 預設加密	5.1.1	2.2.1	2.2.1	不支援
【EC2.8】EC2 執行個體應使用執行個體中繼資料服務第 2 版 (IMDSv2)	5.7	5.6	不支援	不支援
【EC2.13】安全群組不應允許從 0.0.0.0/0 或 :::/0 傳入連接埠 22	不支援 – 由需求 5.3 和 5.4 取代	不支援 – 由需求 5.2 和 5.3 取代	不支援 – 由需求 5.2 和 5.3 取代	4.1

控制項 ID 和標題	CIS v5.0.0 需求	CIS v3.0.0 需求	CIS v1.4.0 需求	CIS v1.2.0 需求
【EC2.14】安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389	不支援 – 由需求 5.3 和 5.4 取代	不支援 – 由需求 5.2 和 5.3 取代	不支援 – 由需求 5.2 和 5.3 取代	4.2
【EC2.21】網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389	5.2	5.1	5.1	不支援
【EC2.53】EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠	5.3	5.2	不支援	不支援
【EC2.54】EC2 安全群組不應允許從 ::/0 傳入遠端伺服器管理連接埠	5.4	5.3	不支援	不支援
【EFS.1】彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS	2.3.1	2.4.1	不支援	不支援
【EFS.8】EFS 檔案系統應靜態加密	2.3.1	不支援	不支援	不支援
【IAM.1】IAM 政策不應允許完整的「*」管理權限	不支援	不支援	1.16	1.22
【IAM.2】IAM 使用者不應連接 IAM 政策	1.14	1.15	不支援	1.16
【IAM.3】IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次	1.13	1.14	1.14	1.4
【IAM.4】IAM 根使用者存取金鑰不應存在	1.3	1.4	1.4	1.12

控制項 ID 和標題	CIS v5.0.0 需求	CIS v3.0.0 需求	CIS v1.4.0 需求	CIS v1.2.0 需求
[IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA	1.9	1.10	1.10	1.2
[IAM.6] 應為根使用者啟用硬體 MFA	1.5	1.6	1.6	1.14
【IAM.8】 應移除未使用的 IAM 使用者登入資料	不支援 – 請 【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料改為參閱	不支援 – 請 【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料改為參閱	不支援 – 請 【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料改為參閱	1.3
【IAM.9】 應為根使用者啟用 MFA	1.4	1.5	1.5	1.13
【IAM.11】 確保 IAM 密碼政策至少需要一個大寫字母	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	1.5
【IAM.12】 確保 IAM 密碼政策至少需要一個小寫字母	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	1.6
【IAM.13】 確保 IAM 密碼政策至少需要一個符號	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	1.7
【IAM.14】 確保 IAM 密碼政策至少需要一個數字	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	1.8
【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高	1.7	1.8	1.8	1.9
【IAM.16】 確保 IAM 密碼政策防止密碼重複使用	1.8	1.9	1.9	1.10

控制項 ID 和標題	CIS v5.0.0 需求	CIS v3.0.0 需求	CIS v1.4.0 需求	CIS v1.2.0 需求
【IAM.17】 確保 IAM 密碼政策在 90 天內過期密碼	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	1.11
【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援	1.16	1.17	1.17	1.2
【IAM.20】 避免使用根使用者	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	不支援 – CIS 已移除此要求	1.1
【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料	1.11	1.12	1.12	不支援 – CIS 在較新版本中新增此需求
【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證	1.18	1.19	不支援 – CIS 在較新版本中新增此需求	不支援 – CIS 在較新版本中新增此需求
【IAM.27】 IAM 身分不應連接 AWSCloudShellFullAccess 政策	1.21	1.22	不支援 – CIS 在較新版本中新增此需求	不支援 – CIS 在較新版本中新增此需求
【IAM.28】 應啟用 IAM Access Analyzer 外部存取分析器	1.19	1.20	不支援 – CIS 在較新版本中新增此需求	不支援 – CIS 在較新版本中新增此需求
【KMS.4】 應啟用 AWS KMS 金鑰輪換	3.6	3.6	3.8	2.8
【Macie.1】 應啟用 Amazon Macie	不支援 – 手動檢查	不支援 – 手動檢查	不支援 – 手動檢查	不支援 – 手動檢查
【RDS.2】 RDS 資料庫執行個體應禁止公開存取，由 PubliclyAccessible 組態決定	2.2.3	2.3.3	不支援 – CIS 在較新版本中新增此需求	不支援 – CIS 在較新版本中新增此需求

控制項 ID 和標題	CIS v5.0.0 需求	CIS v3.0.0 需求	CIS v1.4.0 需求	CIS v1.2.0 需求
[RDS.3] RDS 資料庫執行個體應啟用靜態加密	2.2.1	2.3.1	2.3.1	不支援 – CIS 在較新版本中新增此需求
【RDS.5】 RDS 資料庫執行個體應該設定多個可用區域	2.2.4	不支援 – CIS 在較新版本中新增此需求	不支援 – CIS 在較新版本中新增此需求	不支援 – CIS 在較新版本中新增此需求
【RDS.13】 應啟用 RDS 自動次要版本升級	2.2.2	2.3.2	不支援 – CIS 在較新版本中新增此需求	不支援 – CIS 在較新版本中新增此需求
【RDS.15】 應為多個可用區域設定 RDS 資料庫叢集	2.2.4	不支援 – CIS 在較新版本中新增此需求	不支援 – CIS 在較新版本中新增此需求	不支援 – CIS 在較新版本中新增此需求
【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定	2.1.4	2.1.4	2.1.5	不支援 – CIS 在較新版本中新增此需求
【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL	2.1.1	2.1.1	2.1.2	不支援 – CIS 在較新版本中新增此需求
【S3.8】 S3 一般用途儲存貯體應封鎖公開存取	2.1.4	2.1.4	2.1.5	不支援 – CIS 在較新版本中新增此需求
【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除	2.1.2	2.1.2	2.1.3	不支援 – CIS 在較新版本中新增此需求

CIS AWS Foundations Benchmarks ARNs

當您啟用一個或多個版本的 CIS AWS Foundations Benchmark 時，您會開始在 AWS 安全調查結果格式 (ASFF) 中接收調查結果。在 ASFF 中，每個版本使用以下 Amazon Resource Name (ARN)：

CIS AWS Foundations Benchmark 5.0.0 版

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/5.0.0
```

CIS AWS Foundations Benchmark 3.0.0 版

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/3.0.0
```

CIS AWS Foundations Benchmark 1.4.0 版

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/1.4.0
```

CIS AWS Foundations Benchmark 1.2.0 版

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

您可以使用 Security Hub CSPM API [GetEnabledStandards](#) 的操作來尋找已啟用標準的 ARN。

上述值適用於 StandardsArn。不過，StandardsSubscriptionArn 是指 Security Hub CSPM 在您透過 [BatchEnableStandards](#) 在區域中呼叫 來訂閱標準時建立的標準訂閱資源。

Note

當您啟用 CIS AWS Foundations Benchmark 版本時，Security Hub CSPM 最多可能需要 18 小時才能產生調查結果，這些控制項使用與其他已啟用標準中已啟用之控制項相同的 AWS Config 服務連結規則。如需產生控制項調查結果之排程的詳細資訊，請參閱 [執行安全檢查的排程](#)。

如果您開啟合併控制問題清單，問題清單欄位會有所不同。如需這些差異的詳細資訊，請參閱 [整合對 ASFF 欄位和值的影響](#)。如需範例控制調查結果，請參閱 [控制問題清單的範例](#)。

Security Hub CSPM 中不支援的 CIS 需求

如上表所述，Security Hub CSPM 不支援每個 CIS AWS Foundations Benchmark 版本中的每個 CIS 要求。許多不支援的需求只能透過手動檢閱 AWS 資源的狀態來評估。

Security Hub CSPM 中的 NIST SP 800-53 修訂版 5

NIST 特別出版物 800-53 修訂版 5 (NIST SP 800-53 修訂版 5) 是由國家標準技術研究所 (NIST) 開發的網路安全和合規架構，該機構是美國商務部的一部分。此合規架構提供安全和隱私權要求的目錄，以保護資訊系統和重要資源的機密性、完整性和可用性。美國聯邦政府機構和承包商必須遵守這些要求，以保護其系統和組織。私有組織也可以自願使用這些要求做為降低網路安全風險的指導方針架構。如需架構及其需求的詳細資訊，請參閱 [NIST 電腦安全資源中心的 NIST SP 800-53 修訂版 5](#)。

AWS Security Hub CSPM 提供安全控制，支援 NIST SP 800-53 修訂版 5 要求的子集。這些控制項會針對特定 AWS 服務和資源執行自動安全檢查。若要啟用和管理這些控制項，您可以在 Security Hub CSPM 中啟用 NIST SP 800-53 修訂版 5 架構作為標準。請注意，控制項不支援需要手動檢查的 NIST SP 800-53 修訂版 5 要求。

與其他架構不同，NIST SP 800-53 修訂版 5 架構並未規定應如何評估其需求。反之，架構會提供指導方針。在 Security Hub CSPM 中，NIST SP 800-53 修訂版 5 標準和控制項代表服務對這些準則的理解。

主題

- [設定適用於標準之控制項的資源記錄](#)
- [判斷哪些控制項適用於標準](#)

設定適用於標準之控制項的資源記錄

若要最佳化涵蓋範圍和調查結果的準確性，請務必在 AWS Security Hub CSPM 中啟用 NIST SP 800-53 修訂版 5 標準 AWS Config 之前，先在中啟用和設定資源記錄。當您設定資源記錄時，也請務必針對套用到標準之控制項檢查的所有 AWS 資源類型啟用它。這主要適用於具有變更觸發排程類型的控制項。不過，某些具有定期排程類型的控制項也需要資源記錄。如果未啟用或正確設定資源記錄，Security Hub CSPM 可能無法評估適當的資源，並針對適用於標準的控制項產生準確的調查結果。

如需 Security Hub CSPM 如何在中使用資源錄製的資訊 AWS Config，請參閱 [啟用和設定 AWS Config Security Hub CSPM](#)。如需有關在中設定資源錄製的資訊 AWS Config，請參閱《AWS Config 開發人員指南》中的[使用組態記錄器](#)。

下表指定適用於 Security Hub CSPM 中 NIST SP 800-53 修訂版 5 標準的控制項要記錄的資源類型。

AWS 服務	資源類型
Amazon API Gateway	AWS::ApiGateway::Stage , AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint
Amazon Bedrock AgentCore	AWS::BedrockAgentCore::Gateway , AWS::BedrockAgentCore::Memory
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
AWS CodeBuild	AWS::CodeBuild::Project
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint , AWS::DMS:: ReplicationInstance , AWS::DMS:: ReplicationTask
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::EIP , AWS::EC2::Instance , AWS::EC2::LaunchTemplate , AWS::EC2::NetworkAcl , AWS::EC2:: NetworkInterface , AWS::EC2:: SecurityGroup , AWS::EC2::Subnet , AWS::EC2::TransitGateway , AWS::EC2::VPNConnection , AWS::EC2:: Volume

AWS 服務	資源類型
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup , AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster , AWS::ECS::Service , AWS::ECS::TaskDefinition
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS::Cluster
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer , AWS::ElasticLoadBalancingV2::Listener , AWS::ElasticLoadBalancingV2::LoadBalancer
Amazon ElasticSearch	AWS::Elasticsearch::Domain
Amazon EMR	AWS::EMR::SecurityConfiguration
Amazon EventBridge	AWS::Events::Endpoint , AWS::Events::EventBus
AWS Glue	AWS::Glue::Job
AWS Identity and Access Management (IAM)	AWS::IAM::Group , AWS::IAM::Policy , AWS::IAM::Role , AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias , AWS::KMS::Key

AWS 服務	資源類型
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	AWS::MSK::Cluster
Amazon MQ	AWS::AmazonMQ::Broker
AWS Network Firewall	AWS::NetworkFirewall::Firewall , AWS::NetworkFirewall::FirewallPolicy , AWS::NetworkFirewall::RuleGroup
Amazon OpenSearch Service	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster , AWS::RDS::DBClusterSnapshot , AWS::RDS::DBInstance , AWS::RDS::DBSnapshot , AWS::RDS::EventSubscription
Amazon Redshift	AWS::Redshift::Cluster , AWS::Redshift::ClusterSubnetGroup
Amazon Route 53	AWS::Route53::HostedZone
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint , AWS::S3::AccountPublicAccessBlock , AWS::S3::Bucket
AWS Service Catalog	AWS::ServiceCatalog::Portfolio
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue

AWS 服務	資源類型
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance , AWS::SSM::ManagedInstanceInventory , AWS::SSM::PatchCompliance
Amazon SageMaker AI	AWS::SageMaker::FeatureGroup , AWS::SageMaker::NotebookInstance
AWS Secrets Manager	AWS::SecretsManager::Secret
AWS Transfer Family	AWS::Transfer::Connector
AWS WAF	AWS::WAF::Rule , AWS::WAF::RuleGroup , AWS::WAF::WebACL , AWS::WAFRegional::Rule , AWS::WAFRegional::RuleGroup , AWS::WAFRegional::WebACL , AWS::WAFv2::RuleGroup , AWS::WAFv2::WebACL

判斷哪些控制項適用於標準

以下清單指定支援 NIST SP 800-53 修訂版 5 要求的控制項，並適用於 AWS Security Hub CSPM 中的 NIST SP 800-53 修訂版 5 標準。如需控制項支援的特定需求詳細資訊，請選擇控制項。然後，請參閱控制項詳細資訊中的相關需求欄位。此欄位指定控制項支援的每個 NIST 需求。如果 欄位未指定特定的 NIST 需求，則控制項不支援該需求。

- [【Account.1】 應針對 提供安全性聯絡資訊 AWS 帳戶](#)
- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【ACM.1】 匯入和 ACM 發行的憑證應在指定的期間之後續約](#)
- [【APIGateway.1】 應啟用 API Gateway REST 和 WebSocket API 執行記錄](#)
- [【APIGateway.2】 API Gateway REST API 階段應設定為使用 SSL 憑證進行後端身分驗證](#)
- [【APIGateway.3】 API Gateway REST API 階段應該已啟用 AWS X-Ray 追蹤](#)
- [【APIGateway.4】 API Gateway 應與 WAF Web ACL 建立關聯](#)
- [【APIGateway.5】 API Gateway REST API 快取資料應靜態加密](#)

- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)
- [【AppSync.5】 AWS AppSync GraphQL APIs不應使用 API 金鑰進行身分驗證](#)
- [【AutoScaling.1】 與負載平衡器相關聯的 Auto Scaling 群組應使用 ELB 運作狀態檢查](#)
- [【AutoScaling.2】 Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域](#)
- [【AutoScaling.3】 Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【Autoscaling.5】 使用 Auto Scaling 群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址](#)
- [【AutoScaling.6】 Auto Scaling 群組應在多個可用區域中使用多個執行個體類型](#)
- [【AutoScaling.9】 Amazon EC2 Auto Scaling 群組應使用 Amazon EC2 啟動範本](#)
- [【Backup.1】 AWS Backup 復原點應靜態加密](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudTrail.1】 CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤](#)
- [【CloudTrail.2】 CloudTrail 應啟用靜態加密](#)
- [【CloudTrail.4】 應啟用 CloudTrail 日誌檔案驗證](#)
- [【CloudTrail.5】 CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合](#)
- [【CloudTrail.10】 CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys](#)
- [【CloudWatch.15】 CloudWatch 警示應已設定指定的動作](#)
- [【CloudWatch.16】 CloudWatch 日誌群組應保留一段指定的時間](#)

- [【CloudWatch.17】應啟用 CloudWatch 警示動作](#)
- [【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料](#)
- [【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料](#)
- [【CodeBuild.3】CodeBuild S3 日誌應加密](#)
- [【CodeBuild.4】CodeBuild AWS Config專案環境應具有記錄 URL](#)
- [【Config.1】AWS Config 應啟用並使用服務連結角色進行資源記錄](#)
- [【DataFirehose.1】Firehose 交付串流應靜態加密](#)
- [【DMS.1】Database Migration Service 複寫執行個體不應為公有](#)
- [【DMS.6】DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】DMS 端點應使用 SSL](#)
- [【DMS.10】Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DocumentDB.1】Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DynamoDB.1】DynamoDB 資料表應隨著需求自動擴展容量](#)
- [【DynamoDB.2】DynamoDB 資料表應該啟用point-in-time復原](#)
- [【DynamoDB.3】DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.4】DynamoDB 資料表應存在於備份計畫中](#)
- [【DynamoDB.6】DynamoDB 資料表應該已啟用刪除保護](#)
- [【DynamoDB.7】DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.1】Amazon EBS 快照不應設定為可公開還原](#)
- [【EC2.2】VPC 預設安全群組不應允許傳入或傳出流量](#)
- [【EC2.3】連接的 Amazon EBS 磁碟區應靜態加密](#)
- [【EC2.4】已停止的 EC2 執行個體應在指定的期間之後移除](#)

- [【EC2.6】應在所有 VPC 中啟用 VPCs 流程記錄](#)
- [【EC2.7】應啟用 EBS 預設加密](#)
- [【EC2.8】EC2 執行個體應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.9】Amazon EC2 執行個體不應具有公有 IPv4 地址](#)
- [【EC2.10】Amazon EC2 應設定為使用為 Amazon EC2 服務建立的 VPC 端點](#)
- [【EC2.12】應移除未使用的 Amazon EC2 EIPs](#)
- [【EC2.13】安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 22](#)
- [【EC2.15】Amazon EC2 子網路不應自動指派公有 IP 地址](#)
- [【EC2.16】應該移除未使用的網路存取控制清單](#)
- [【EC2.17】Amazon EC2 執行個體不應使用多個 ENIs](#)
- [【EC2.18】安全群組應僅允許授權連接埠不受限制的傳入流量](#)
- [【EC2.19】安全群組不應允許無限制存取高風險的連接埠](#)
- [【EC2.20】用於 an AWS Site-to-Site VPN 連線的兩個 VPN 通道都應啟動](#)
- [【EC2.21】網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)
- [【EC2.23】Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】Amazon EC2 啟動範本不應將公 IPs 指派給網路介面](#)
- [【EC2.28】備份計畫應涵蓋 EBS 磁碟區](#)
- [【EC2.51】EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.55】VPCs 應使用 ECR API 的介面端點進行設定](#)
- [【EC2.56】VPCs 應使用 Docker 登錄檔的介面端點進行設定](#)
- [【EC2.57】VPCs 應使用 Systems Manager 的介面端點進行設定](#)
- [【EC2.58】VPCs 應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】VPCs 應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【ECR.1】ECR 私有儲存庫應設定映像掃描](#)
- [【ECR.2】ECR 私有儲存庫應設定標籤不可變性](#)
- [【ECR.3】ECR 儲存庫應至少設定一個生命週期政策](#)
- [【ECR.5】ECR 儲存庫應使用客戶受管加密 AWS KMS keys](#)
- [【ECS.1】Amazon ECS 任務定義應具有安全的聯網模式和使用使用者定義](#)
- [【ECS.2】ECS 服務不應自動為其指派公有 IP 地址](#)

- [【ECS.3】 ECS 任務定義不應共用主機的程序命名空間](#)
- [【ECS.4】 ECS 容器應以非特殊權限執行](#)
- [【ECS.5】 ECS 任務定義應將容器設定為僅限對根檔案系統的唯讀存取](#)
- [【ECS.8】 不應將秘密做為容器環境變數傳遞](#)
- [【ECS.9】 ECS 任務定義應具有記錄組態](#)
- [【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行](#)
- [【ECS.12】 ECS 叢集應使用 Container Insights](#)
- [【ECS.17】 ECS 任務定義不應使用主機網路模式](#)
- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【EFS.3】 EFS 存取點應強制執行根目錄](#)
- [【EFS.4】 EFS 存取點應強制執行使用者身分](#)
- [【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯](#)
- [【EKS.1】 不應公開存取 EKS 叢集端點](#)
- [【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)
- [【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密](#)
- [【EKS.8】 EKS 叢集應該啟用稽核記錄](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.2】 ElastiCache 叢集應該啟用自動次要版本升級](#)
- [【ElastiCache.3】 ElastiCache 複寫群組應該啟用自動容錯移轉](#)
- [【ElastiCache.4】 ElastiCache 複寫群組應靜態加密](#)
- [【ElastiCache.5】 ElastiCache 複寫群組應在傳輸中加密](#)
- [【ElastiCache.6】 舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】 ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ELB.1】 Application Load Balancer 應設定為將所有 HTTP 請求重新導向至 HTTPS](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【ELB.3】 Classic Load Balancer 接聽程式應使用 HTTPS 或 TLS 終止設定](#)
- [【ELB.4】 Application Load Balancer 應設定為捨棄無效的 http 標頭](#)

- [【ELB.5】應啟用應用程式和 Classic Load Balancer 記錄](#)
- [【ELB.6】應用程式、閘道和 Network Load Balancer 應啟用刪除保護](#)
- [【ELB.7】Classic Load Balancer 應啟用連線耗盡](#)
- [【ELB.8】具有 SSL AWS Config 接聽程式的 Classic Load Balancer 應使用預先定義的安全政策，該政策具有強烈驅動](#)
- [【ELB.9】Classic Load Balancer 應啟用跨區域負載平衡](#)
- [【ELB.10】Classic Load Balancer 應跨越多個可用區域](#)
- [【ELB.12】Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.13】應用程式、網路和閘道負載平衡器應跨越多個可用區域](#)
- [【ELB.14】Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.16】Application Load Balancer 應與 AWS WAF Web ACL 建立關聯](#)
- [【ELB.17】具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【EMR.1】Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【EMR.2】應啟用 Amazon EMR 封鎖公開存取設定](#)
- [【EMR.3】Amazon EMR 安全組態應靜態加密](#)
- [【EMR.4】Amazon EMR 安全組態應在傳輸中加密](#)
- [【ES.1】Elasticsearch 網域應該啟用靜態加密](#)
- [【ES.2】不應公開存取 Elasticsearch 網域](#)
- [【ES.3】Elasticsearch 網域應該加密節點之間傳送的資料](#)
- [【ES.4】應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【ES.5】Elasticsearch 網域應該啟用稽核記錄](#)
- [【ES.6】Elasticsearch 網域應至少具有三個資料節點](#)
- [【ES.7】Elasticsearch 網域應該至少設定三個專用主節點](#)
- [【ES.8】應使用最新的 TLS 安全政策加密與 Elasticsearch 網域的連線](#)
- [【EventBridge.3】EventBridge 自訂事件匯流排應連接以資源為基礎的政策](#)
- [【EventBridge.4】EventBridge 全域端點應啟用事件複寫](#)
- [【FSx.1】FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)
- [【FSx.2】FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)
- [【Glue.4】AWS Glue Spark 任務應在支援的版本上執行 AWS Glue](#)
- [【GuardDuty.1】應啟用 GuardDuty](#)
- [【IAM.1】IAM 政策不應允許完整的「*」管理權限](#)

- [【IAM.2】 IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】 IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.6】 應為根使用者啟用硬體 MFA](#)
- [【IAM.7】 IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.9】 應為根使用者啟用 MFA](#)
- [【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【Kinesis.1】 Kinesis 串流應靜態加密](#)
- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【KMS.3】 AWS KMS keys 不應意外刪除](#)
- [【KMS.4】 應啟用 AWS KMS 金鑰輪換](#)
- [【Lambda.1】 Lambda 函數政策應禁止公開存取](#)
- [【Lambda.2】 Lambda 函數應使用支援的執行時間](#)
- [【Lambda.3】 Lambda 函數應該位於 VPC 中](#)
- [【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密](#)
- [【MSK.2】 MSK 叢集應已設定增強型監控](#)
- [【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MQ.3】 Amazon MQ 代理程式應該啟用自動次要版本升級](#)
- [【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式](#)
- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)

- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【NetworkFirewall.1】 網路防火牆防火牆應部署在多個可用區域](#)
- [【NetworkFirewall.2】 應啟用網路防火牆記錄](#)
- [【NetworkFirewall.3】 網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.4】 Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)
- [【NetworkFirewall.5】 網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】 無狀態網路防火牆規則群組不應為空](#)
- [【NetworkFirewall.9】 網路防火牆防火牆應啟用刪除保護](#)
- [【NetworkFirewall.10】 網路防火牆防火牆應啟用子網路變更保護](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【PCA.1】 應停用 AWS 私有 CA 根憑證授權單位](#)
- [【RDS.1】 RDS 快照應為私有](#)
- [【RDS.2】 RDS 資料庫執行個體應禁止公開存取，由 PubliclyAccessible 組態決定](#)
- [【RDS.3】 RDS 資料庫執行個體應啟用靜態加密](#)
- [【RDS.4】 RDS 叢集快照和資料庫快照應靜態加密](#)

- [【RDS.5】 RDS 資料庫執行個體應該設定多個可用區域](#)
- [【RDS.6】 應為 RDS 資料庫執行個體設定增強型監控](#)
- [【RDS.7】 RDS 叢集應該啟用刪除保護](#)
- [【RDS.8】 RDS 資料庫執行個體應啟用刪除保護](#)
- [【RDS.9】 RDS 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.10】 應為 RDS 執行個體設定 IAM 身分驗證](#)
- [【RDS.11】 RDS 執行個體應該啟用自動備份](#)
- [【RDS.12】 應為 RDS 叢集設定 IAM 身分驗證](#)
- [【RDS.13】 應啟用 RDS 自動次要版本升級](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.15】 應為多個可用區域設定 RDS 資料庫叢集](#)
- [【RDS.16】 Aurora 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.17】 RDS 資料庫執行個體應設定為將標籤複製到快照](#)
- [【RDS.19】 應為關鍵叢集事件設定現有的 RDS 事件通知訂閱](#)
- [【RDS.20】 應為關鍵資料庫執行個體事件設定現有的 RDS 事件通知訂閱](#)
- [【RDS.21】 應為關鍵資料庫參數群組事件設定 RDS 事件通知訂閱](#)
- [【RDS.22】 應為關鍵資料庫安全群組事件設定 RDS 事件通知訂閱](#)
- [【RDS.23】 RDS 執行個體不應使用資料庫引擎預設連接埠](#)
- [【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱](#)
- [【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)
- [【RDS.26】 RDS 資料庫執行個體應受備份計劃保護](#)
- [【RDS.27】 RDS 資料庫叢集應靜態加密](#)
- [【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.40】 RDS for SQL Server 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.42】 RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【Redshift.1】 Amazon Redshift 叢集應禁止公開存取](#)
- [【Redshift.2】 與 Amazon Redshift 叢集的連線應在傳輸中加密](#)
- [【Redshift.3】 Amazon Redshift 叢集應該啟用自動快照](#)

- [【Redshift.4】 Amazon Redshift 叢集應該啟用稽核記錄](#)
- [【Redshift.6】 Amazon Redshift 應已啟用主要版本的自動升級](#)
- [【Redshift.7】 Redshift 叢集應使用增強型 VPC 路由](#)
- [【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定](#)
- [【S3.2】 S3 一般用途儲存貯體應封鎖公開讀取存取](#)
- [【S3.3】 S3 一般用途儲存貯體應封鎖公有寫入存取](#)
- [【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL](#)
- [【S3.6】 S3 一般用途儲存貯體政策應限制對其他 的存取 AWS 帳戶](#)
- [【S3.7】 S3 一般用途儲存貯體應使用跨區域複寫](#)
- [【S3.8】 S3 一般用途儲存貯體應封鎖公開存取](#)
- [【S3.9】 S3 一般用途儲存貯體應啟用伺服器存取記錄](#)
- [【S3.10】 已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態](#)
- [【S3.11】 S3 一般用途儲存貯體應啟用事件通知](#)
- [【S3.12】 ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取](#)
- [【S3.13】 S3 一般用途儲存貯體應具有生命週期組態](#)
- [【S3.14】 S3 一般用途儲存貯體應該已啟用版本控制](#)
- [【S3.15】 S3 一般用途儲存貯體應啟用物件鎖定](#)
- [【S3.17】 S3 一般用途儲存貯體應使用 靜態加密 AWS KMS keys](#)
- [【S3.19】 S3 存取點應啟用封鎖公開存取設定](#)
- [【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.4】 SageMaker 端點生產變體的初始執行個體計數應大於 1](#)
- [【SageMaker.18】 使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SecretsManager.1】 Secrets Manager 秘密應該已啟用自動輪換](#)

- [【SecretsManager.2】設定自動輪換的 Secrets Manager 秘密應能成功輪換](#)
- [【SecretsManager.3】移除未使用的 Secrets Manager 秘密](#)
- [【SecretsManager.4】Secrets Manager 秘密應在指定的天數內輪換](#)
- [【ServiceCatalog.1】Service Catalog 產品組合只能在 AWS 組織內共用](#)
- [【SNS.1】SNS 主題應使用 進行靜態加密 AWS KMS](#)
- [【SQS.1】Amazon SQS 佇列應靜態加密](#)
- [【SSM.1】Amazon EC2 執行個體應該由 管理 AWS Systems Manager](#)
- [【SSM.2】Systems Manager 管理的 Amazon EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態](#)
- [【SSM.3】Systems Manager 管理的 Amazon EC2 執行個體應具有 COMPLIANT 的關聯合規狀態](#)
- [【SSM.4】SSM 文件不應公開](#)
- [【Transfer.2】Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線](#)
- [【Transfer.3】Transfer Family 連接器應該已啟用記錄](#)
- [【WAF.1】應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.2】AWS WAF 傳統區域規則應至少有一個條件](#)
- [【WAF.3】AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.4】AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.6】AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.11】應該啟用 AWS WAF Web ACL 記錄](#)
- [【WAF.12】AWS WAF 規則應啟用 CloudWatch 指標](#)

Security Hub CSPM 中的 NIST SP 800-171 修訂版 2

NIST 特別出版物 800-171 修訂版 2 (NIST SP 800-171 修訂版 2) 是由國家標準技術研究所 (NIST) 所開發的網路安全和合規架構，該機構是美國商務部的一部分。此合規架構提供建議的安全要求，以保護不屬於美國聯邦政府的系統和組織中受控未分類資訊的機密性。受控未分類資訊也稱為 CUI，是不符合政府分類標準的敏感資訊，但必須受到保護。這是視為敏感的資訊，由美國聯邦政府或代表美國聯邦政府的其他實體建立或擁有。

NIST SP 800-171 修訂版 2 在以下情況提供保護 CUI 機密性的建議安全要求：

- 資訊位於非聯合系統和組織中，
- 非聯合組織不會代表聯邦機構收集或維護資訊，也不會代表機構使用或操作系統，以及
- 對於 CUI 登錄檔中列出的 CUI 類別，對於授權法律、法規或全政府政策所規定的 CUI 機密性，沒有特定的保護要求。

這些要求適用於處理、存放或傳輸 CUI 或為元件提供安全保護的非聯合系統和組織的所有元件。如需詳細資訊，請參閱 [NIST 電腦安全資源中心的 NIST SP 800-171 修訂版 2](#)。

AWS Security Hub CSPM 提供安全控制，支援 NIST SP 800-171 修訂版 2 要求的子集。這些控制項會針對特定 AWS 服務和資源執行自動安全檢查。若要啟用和管理這些控制項，您可以在 Security Hub CSPM 中啟用 NIST SP 800-171 修訂版 2 架構作為標準。請注意，控制項不支援需要手動檢查的 NIST SP 800-171 修訂版 2 要求。

主題

- [設定適用於標準之控制項的資源記錄](#)
- [判斷哪些控制項適用於標準](#)

設定適用於標準之控制項的資源記錄

若要最佳化涵蓋範圍和調查結果的準確性，請務必在 AWS Security Hub CSPM 中啟用 NIST SP 800-171 修訂版 2 標準 AWS Config 之前，先在中啟用和設定資源記錄。當您設定資源記錄時，也請務必針對套用到標準之控制項檢查的所有 AWS 資源類型啟用它。否則，Security Hub CSPM 可能無法評估適當的資源，並為適用於標準的控制項產生準確的調查結果。

如需 Security Hub CSPM 如何在中使用資源錄製的資訊 AWS Config，請參閱 [啟用和設定 AWS Config Security Hub CSPM](#)。如需有關在中設定資源錄製的資訊 AWS Config，請參閱《AWS Config 開發人員指南》中的[使用組態記錄器](#)。

下表指定適用於 Security Hub CSPM 中 NIST SP 800-171 修訂版 2 標準之控制項要記錄的資源類型。

AWS 服務	資源類型
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
Amazon API Gateway	AWS::ApiGateway::Stage
Amazon CloudFront	AWS::CloudFront::Distribution

AWS 服務	資源類型
Amazon CloudWatch	AWS::CloudWatch::Alarm
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::NetworkAcl , AWS::EC2:: SecurityGroup , AWS::EC2::VPC , AWS::EC2::VPNConnection
Elastic Load Balancing	AWS::ElasticLoadBalancing:: LoadBalancer
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias , AWS::KMS::Key
AWS Network Firewall	AWS::NetworkFirewall::Firew allPolicy , AWS::NetworkFirewa ll::RuleGroup
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
AWS Systems Manager (SSM)	AWS::SSM::PatchCompliance
AWS WAF	AWS::WAFv2::RuleGroup

判斷哪些控制項適用於標準

以下清單指定支援 NIST SP 800-171 修訂版 2 要求的控制項，並適用於 AWS Security Hub CSPM 中的 NIST SP 800-171 修訂版 2 標準。如需控制項支援的特定需求詳細資訊，請選擇控制項。然後，請參閱控制項詳細資訊中的相關需求欄位。此欄位指定控制項支援的每個 NIST 需求。如果 欄位未指定特定的 NIST 需求，則控制項不支援該需求。

- [【ACM.1】匯入和 ACM 發行的憑證應在指定的期間之後續約](#)
- [【APIGateway.2】API Gateway REST API 階段應設定為使用 SSL 憑證進行後端身分驗證](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)

- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudTrail.2】 CloudTrail 應啟用靜態加密](#)
- [【CloudTrail.3】 至少應啟用一個 CloudTrail 追蹤](#)
- [【CloudTrail.4】 應啟用 CloudTrail 日誌檔案驗證](#)
- [【CloudWatch.1】 應該存在日誌指標篩選條件和警示以使用「根」使用者](#)
- [【CloudWatch.2】 確保未經授權的 API 呼叫存在日誌指標篩選條件和警示](#)
- [【CloudWatch.4】 確保 IAM 政策變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.5】 確保 CloudTrail 組態變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.6】 確保 AWS 管理主控台 驗證失敗時存在日誌指標篩選條件和警示](#)
- [【CloudWatch.7】 確保日誌指標篩選條件和警示存在，以停用或排程刪除客戶受管金鑰](#)
- [【CloudWatch.8】 確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.9】 確保 AWS Config 組態變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.10】 確保安全群組變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.11】 確定網路存取控制清單 \(NACL\) 的變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.12】 確保網路閘道變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.13】 確保路由表變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.14】 確保 VPC 變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.15】 CloudWatch 警示應已設定指定的動作](#)
- [【EC2.6】 應在所有 VPC 中啟用 VPCs 流程記錄](#)
- [【EC2.10】 Amazon EC2 應設定為使用為 Amazon EC2 服務建立的 VPC 端點](#)
- [【EC2.13】 安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 22](#)
- [【EC2.16】 應該移除未使用的網路存取控制清單](#)
- [【EC2.18】 安全群組應僅允許授權連接埠不受限制的傳入流量](#)
- [【EC2.19】 安全群組不應允許無限制存取高風險的連接埠](#)
- [【EC2.20】 用於 an AWS Site-to-Site VPN 連線的兩個 VPN 通道都應啟動](#)
- [【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)
- [【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【ELB.3】 Classic Load Balancer 接聽程式應使用 HTTPS 或 TLS 終止設定](#)

- [【ELB.8】 具有 SSL AWS Config 接聽程式的 Classic Load Balancer 應使用預先定義的安全政策，該政策具有強烈驅動](#)
- [【GuardDuty.1】 應啟用 GuardDuty](#)
- [【IAM.1】 IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】 IAM 使用者不應連接 IAM 政策](#)
- [【IAM.7】 IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.10】 IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.11】 確保 IAM 密碼政策至少需要一個大寫字母](#)
- [【IAM.12】 確保 IAM 密碼政策至少需要一個小寫字母](#)
- [【IAM.13】 確保 IAM 密碼政策至少需要一個符號](#)
- [【IAM.14】 確保 IAM 密碼政策至少需要一個數字](#)
- [【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)
- [【IAM.16】 確保 IAM 密碼政策防止密碼重複使用](#)
- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【NetworkFirewall.2】 應啟用網路防火牆記錄](#)
- [【NetworkFirewall.3】 網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.5】 網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】 無狀態網路防火牆規則群組不應為空](#)
- [【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL](#)
- [【S3.6】 S3 一般用途儲存貯體政策應限制對其他 的存取 AWS 帳戶](#)
- [【S3.9】 S3 一般用途儲存貯體應啟用伺服器存取記錄](#)
- [【S3.11】 S3 一般用途儲存貯體應啟用事件通知](#)
- [【S3.14】 S3 一般用途儲存貯體應該已啟用版本控制](#)
- [【S3.17】 S3 一般用途儲存貯體應使用 靜態加密 AWS KMS keys](#)
- [【SNS.1】 SNS 主題應使用 進行靜態加密 AWS KMS](#)
- [【SSM.2】 Systems Manager 管理的 Amazon EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態](#)

- [【WAF.12】 AWS WAF 規則應啟用 CloudWatch 指標](#)

Security Hub CSPM 中的 PCI DSS

支付卡產業資料安全標準 (PCI DSS) 是第三方合規架構，提供一組規則和準則，以安全地處理信用卡和簽帳金融卡資訊。PCI 安全標準委員會 (SSC) 會建立和更新此架構。

AWS Security Hub CSPM 提供 PCI DSS 標準，可協助您遵守此第三方架構。您可以使用此標準來探索處理持卡人資料之 AWS 資源中的安全漏洞。建議您在具有儲存、處理或傳輸持卡人資料或敏感身分驗證資料之資源 AWS 帳戶 的 中啟用此標準。PCI SSC 的評估驗證了此標準。

Security Hub CSPM 支援 PCI DSS v3.2.1 和 PCI DSS v4.0.1。建議使用 v4.0.1 來保持最新的安全最佳實務。您可以同時啟用兩個版本的標準。如需啟用標準的資訊，請參閱 [啟用安全標準](#)。如果您目前使用 v3.2.1，但只想要使用 v4.0.1，請先啟用較新版本，再停用較舊版本。這可以防止安全檢查中的差距。如果您使用 Security Hub CSPM 整合與 [AWS Organizations](#) 並想要在多個帳戶中批次啟用 v4.0.1，我們建議您使用 [中央組態](#) 來執行此操作。

下列各節指定哪些控制項適用於 PCI DSS v3.2.1 和 PCI DSS v4.0.1。

適用於 PCI DSS v3.2.1 的控制項

以下清單指定哪些 Security Hub CSPM 控制項適用於 PCI DSS v3.2.1。若要檢閱控制項的詳細資訊，請選擇控制項。

[【AutoScaling.1】 與負載平衡器相關聯的 Auto Scaling 群組應使用 ELB 運作狀態檢查](#)

[\[CloudTrail.2\] CloudTrail 應啟用靜態加密](#)

[【CloudTrail.3】 至少應啟用一個 CloudTrail 追蹤](#)

[【CloudTrail.4】 應啟用 CloudTrail 日誌檔案驗證](#)

[【CloudTrail.5】 CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合](#)

[【CloudWatch.1】 應該存在日誌指標篩選條件和警示以使用「根」使用者](#)

[【CodeBuild.1】 CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料](#)

[【CodeBuild.2】 CodeBuild 專案環境變數不應包含純文字登入資料](#)

[【Config.1】 AWS Config 應啟用並使用服務連結角色進行資源記錄](#)

[【DMS.1】 Database Migration Service 複寫執行個體不應為公有](#)

[【EC2.1】 Amazon EBS 快照不應設定為可公開還原](#)

[【EC2.2】 VPC 預設安全群組不應允許傳入或傳出流量](#)

[【EC2.6】 應在所有 VPC 中啟用 VPCs 流程記錄](#)

[【EC2.12】 應移除未使用的 Amazon EC2 EIPs](#)

[【EC2.13】 安全群組不應允許從 0.0.0.0/0 或 :::/0 傳入連接埠 22](#)

[【ELB.1】 Application Load Balancer 應設定為將所有 HTTP 請求重新導向至 HTTPS](#)

[【ES.1】 Elasticsearch 網域應該啟用靜態加密](#)

[【ES.2】 不應公開存取 Elasticsearch 網域](#)

[【GuardDuty.1】 應啟用 GuardDuty](#)

[【IAM.1】 IAM 政策不應允許完整的「*」管理權限](#)

[【IAM.2】 IAM 使用者不應連接 IAM 政策](#)

[【IAM.4】 IAM 根使用者存取金鑰不應存在](#)

[【IAM.6】 應為根使用者啟用硬體 MFA](#)

[【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)

[【IAM.9】 應為根使用者啟用 MFA](#)

[【IAM.10】 IAM 使用者的密碼政策應具有強大的組態](#)

[【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)

[【KMS.4】 應啟用 AWS KMS 金鑰輪換](#)

[【Lambda.1】 Lambda 函數政策應禁止公開存取](#)

[【Lambda.3】 Lambda 函數應該位於 VPC 中](#)

[【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)

[【Opensearch.2】 不應公開存取 OpenSearch 網域](#)

[【RDS.1】 RDS 快照應為私有](#)

[【RDS.2】 RDS 資料庫執行個體應禁止公開存取，由 PubliclyAccessible 組態決定](#)

[【Redshift.1】 Amazon Redshift 叢集應禁止公開存取](#)

[【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定](#)

[【S3.2】 S3 一般用途儲存貯體應封鎖公開讀取存取](#)

[【S3.3】 S3 一般用途儲存貯體應封鎖公有寫入存取](#)

[【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL](#)

[【S3.7】 S3 一般用途儲存貯體應使用跨區域複寫](#)

[【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)

[【SSM.1】 Amazon EC2 執行個體應該由 管理 AWS Systems Manager](#)

[【SSM.2】 Systems Manager 管理的 Amazon EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態](#)

[【SSM.3】 Systems Manager 管理的 Amazon EC2 執行個體應具有 COMPLIANT 的關聯合規狀態](#)

適用於 PCI DSS v4.0.1 的控制項

以下清單指定哪些 Security Hub CSPM 控制項適用於 PCI DSS v4.0.1。若要檢閱控制項的詳細資訊，請選擇控制項。

[【ACM.1】 匯入和 ACM 發行的憑證應在指定的期間之後續約](#)

[【ACM.2】 由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)

[【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)

[【AppSync.2】 AWS AppSync 應該啟用欄位層級記錄](#)

[【AutoScaling.3】 Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)

[【Autoscaling.5】 使用 Auto Scaling 群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址](#)

[【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)

[【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)

[【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)

[【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)

[【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)

[【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)

[【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)

[\[CloudTrail.2\] CloudTrail 應啟用靜態加密](#)

[【CloudTrail.3】至少應啟用一個 CloudTrail 追蹤](#)

[【CloudTrail.4】應啟用 CloudTrail 日誌檔案驗證](#)

[【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)

[【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)

[【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料](#)

[【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料](#)

[【CodeBuild.3】CodeBuild S3 日誌應加密](#)

[【DMS.1】 Database Migration Service 複寫執行個體不應為公有](#)

[【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)

[【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制](#)

[【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)

[【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級](#)

[【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)

[【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)

[【DMS.9】 DMS 端點應使用 SSL](#)

[【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)

[【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)

[【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)

[【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)

[【EC2.13】 安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 22](#)

[【EC2.14】 安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389](#)

[【EC2.15】 Amazon EC2 子網路不應自動指派公有 IP 地址](#)

[【EC2.16】 應該移除未使用的網路存取控制清單](#)

[【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)

[【EC2.171】 EC2 VPN 連線應該已啟用記錄](#)

[【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)

[【EC2.25】 Amazon EC2 啟動範本不應將公 IPs 指派給網路介面](#)

[【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)

[【EC2.53】 EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠](#)

[【EC2.54】 EC2 安全群組不應允許從 ::/0 傳入遠端伺服器管理連接埠](#)

[【EC2.8】 EC2 執行個體應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)

[【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)

[【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行](#)

[【ECS.16】 ECS 任務集不應自動指派公有 IP 地址](#)

[【ECS.2】 ECS 服務不應自動為其指派公有 IP 地址](#)

[【ECS.8】 不應將秘密做為容器環境變數傳遞](#)

[【EFS.4】 EFS 存取點應強制執行使用者身分](#)

[【EKS.1】 不應公開存取 EKS 叢集端點](#)

[【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)

[【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密](#)

[【EKS.8】 EKS 叢集應該啟用稽核記錄](#)

[【ElastiCache.2】 ElastiCache 叢集應該啟用自動次要版本升級](#)

[【ElastiCache.5】 ElastiCache 複寫群組應在傳輸中加密](#)

[【ElastiCache.6】 舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)

[【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)

[【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)

[【ELB.12】 Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)

[【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)

[【ELB.3】 Classic Load Balancer 接聽程式應使用 HTTPS 或 TLS 終止設定](#)

[【ELB.4】 Application Load Balancer 應設定為捨棄無效的 http 標頭](#)

[【ELB.8】 具有 SSL AWS Config接聽程式的 Classic Load Balancer 應使用預先定義的安全政策，該政策具有強烈驅動](#)

[【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)

[【EMR.2】 應啟用 Amazon EMR 封鎖公開存取設定](#)

[【ES.2】 不應公開存取 Elasticsearch 網域](#)

[【ES.3】 Elasticsearch 網域應該加密節點之間傳送的資料](#)

[【ES.5】 Elasticsearch 網域應該啟用稽核記錄](#)

[【ES.8】 應使用最新的 TLS 安全政策加密與 Elasticsearch 網域的連線](#)

[【EventBridge.3】 EventBridge 自訂事件匯流排應連接以資源為基礎的政策](#)

[【GuardDuty.1】 應啟用 GuardDuty](#)

[【GuardDuty.10】 應啟用 GuardDuty S3 保護](#)

[【GuardDuty.6】 應啟用 GuardDuty Lambda 保護](#)

[【GuardDuty.7】 應啟用 GuardDuty EKS 執行期監控](#)

[【GuardDuty.9】 應啟用 GuardDuty RDS 保護](#)

[【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)

[\[IAM.5\] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)

[\[IAM.6\] 應為根使用者啟用硬體 MFA](#)

[【IAM.7】 IAM 使用者的密碼政策應具有強大的組態](#)

[【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)

[【IAM.9】 應為根使用者啟用 MFA](#)

[【IAM.11】 確保 IAM 密碼政策至少需要一個大寫字母](#)

[【IAM.12】 確保 IAM 密碼政策至少需要一個小寫字母](#)

[【IAM.14】 確保 IAM 密碼政策至少需要一個數字](#)

[【IAM.16】 確保 IAM 密碼政策防止密碼重複使用](#)

[【IAM.17】 確保 IAM 密碼政策在 90 天內過期密碼](#)

[【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)

[【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)

[【Inspector.1】 應啟用 Amazon Inspector EC2 掃描](#)

[【Inspector.2】 應啟用 Amazon Inspector ECR 掃描](#)

[【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)

[【Inspector.4】 應啟用 Amazon Inspector Lambda 標準掃描](#)

[【KMS.4】 應啟用 AWS KMS 金鑰輪換](#)

[【Lambda.1】 Lambda 函數政策應禁止公開存取](#)

[【Lambda.2】 Lambda 函數應使用支援的執行時間](#)

[【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)

[【MQ.3】 Amazon MQ 代理程式應該啟用自動次要版本升級](#)

[【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密](#)

[【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)

[【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)

[【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)

[【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)

[【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)

[【RDS.13】 應啟用 RDS 自動次要版本升級](#)

[【RDS.2】 RDS 資料庫執行個體應禁止公開存取，由 PubliclyAccessible 組態決定](#)

[【RDS.20】 應為關鍵資料庫執行個體事件設定現有的 RDS 事件通知訂閱](#)

[【RDS.21】 應為關鍵資料庫參數群組事件設定 RDS 事件通知訂閱](#)

[【RDS.22】 應為關鍵資料庫安全群組事件設定 RDS 事件通知訂閱](#)

[【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱](#)

[【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)

[【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)

[【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)

[【RDS.36】 RDS for PostgreSQL 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)

[【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)

[【RDS.9】 RDS 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)

[【Redshift.1】 Amazon Redshift 叢集應禁止公開存取](#)

[【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠](#)

[【Redshift.2】 與 Amazon Redshift 叢集的連線應在傳輸中加密](#)

[【Redshift.4】 Amazon Redshift 叢集應該啟用稽核記錄](#)

[【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)

[【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定](#)

[【S3.15】 S3 一般用途儲存貯體應啟用物件鎖定](#)

[【S3.17】 S3 一般用途儲存貯體應使用 靜態加密 AWS KMS keys](#)

[【S3.19】 S3 存取點應啟用封鎖公開存取設定](#)

[【S3.22】 S3 一般用途儲存貯體應記錄物件層級寫入事件](#)

[【S3.23】 S3 一般用途儲存貯體應記錄物件層級讀取事件](#)

[【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)

[【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL](#)

[【S3.8】 S3 一般用途儲存貯體應封鎖公開存取](#)

[【S3.9】 S3 一般用途儲存貯體應啟用伺服器存取記錄](#)

[【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)

[【SecretsManager.1】 Secrets Manager 秘密應該已啟用自動輪換](#)

[【SecretsManager.2】 設定自動輪換的 Secrets Manager 秘密應能成功輪換](#)

[【SecretsManager.4】 Secrets Manager 秘密應在指定的天數內輪換](#)

[【SSM.2】 Systems Manager 管理的 Amazon EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態](#)

[【SSM.3】 Systems Manager 管理的 Amazon EC2 執行個體應具有 COMPLIANT 的關聯合規狀態](#)

[【StepFunctions.1】 Step Functions 狀態機器應該已開啟記錄](#)

[【Transfer.2】 Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線](#)

[【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)

[【WAF.11】 應該啟用 AWS WAF Web ACL 記錄](#)

Security Hub CSPM 中的服務受管標準

服務受管標準是另一個 AWS 服務 管理的安全標準，但您可以在 Security Hub CSPM 中檢視。例如，[服務受管標準：AWS Control Tower](#) 是 AWS Control Tower 管理的服務受管標準。服務受管標準與 AWS Security Hub CSPM 以下列方式管理的安全標準不同：

- 標準建立和刪除 – 您可以使用管理服務的主控制台或 API，或使用 建立和刪除服務受管標準 AWS CLI。在您以其中一種方式在管理服務中建立標準之前，該標準不會出現在 Security Hub CSPM 主控台中，且 Security Hub CSPM API 或 無法存取 AWS CLI。

- 不自動啟用控制項 – 當您建立服務受管標準時，Security Hub CSPM 和管理服務不會自動啟用適用於標準的控制項。此外，當 Security Hub CSPM 發行標準的新控制項時，它們不會自動啟用。這是偏離 Security Hub CSPM 管理的標準。如需在 Security Hub CSPM 中設定控制項之一般方式的詳細資訊，請參閱 [了解 Security Hub CSPM 中的安全控制](#)。
- 啟用和停用控制項 – 建議您在管理服務中啟用和停用控制項，以避免偏離。
- 控制項的可用性 – 管理服務會選擇哪些控制項可作為服務受管標準的一部分。可用的控制項可能包含現有 Security Hub CSPM 控制項的全部或一部分。

管理服務建立服務受管標準並為其提供控制項後，您可以在 Security Hub CSPM 主控台、Security Hub CSPM API 或中存取控制項問題清單、控制項狀態和標準安全分數 AWS CLI。管理服務中也可能提供部分或全部此資訊。

從下列清單中選擇服務受管標準，以檢視其詳細資訊。

服務受管標準

- [服務受管標準：AWS Control Tower](#)

服務受管標準：AWS Control Tower

本節提供有關服務受管標準的資訊：AWS Control Tower。

什麼是服務受管標準：AWS Control Tower？

服務受管標準：AWS Control Tower 是一種服務受管標準，可 AWS Control Tower 管理支援 Security Hub 控制項子集的。此標準專為 AWS Security Hub CSPM 和的使用者而設計 AWS Control Tower。它可讓您從 AWS Control Tower 服務設定 Security Hub CSPM 的偵測控制。

Detective 控制項可偵測 內資源的不合規（例如設定錯誤）AWS 帳戶。

Tip

服務受管標準與 AWS Security Hub CSPM 管理的標準不同。例如，您必須在管理服務中建立和刪除服務受管標準。如需詳細資訊，請參閱[Security Hub CSPM 中的服務受管標準](#)。

當您透過 啟用 Security Hub CSPM 控制時 AWS Control Tower，如果尚未啟用，Control Tower 也會在這些特定帳戶和區域中為您啟用 Security Hub CSPM。在 Security Hub CSPM 主控台和 API 中，一

且啟用標準，您就可以檢視服務受管標準：AWS Control Tower 以及其他 Security Hub CSPM 標準 AWS Control Tower。

如需此標準的詳細資訊，請參閱AWS Control Tower 《使用者指南》中的 [Security Hub CSPM 控制項](#)。

建立標準

只有在您從中啟用 Security Hub CSPM 控制項時，此標準才適用於 Security Hub CSPM AWS Control Tower。AWS Control Tower 會在您第一次使用下列其中一種方法啟用適用的控制項時建立標準：

- AWS Control Tower 主控台
- AWS Control Tower API (呼叫 [EnableControl](#) API)
- AWS CLI (執行 [enable-control](#)命令)

當您透過 啟用 Security Hub CSPM 控制時 AWS Control Tower，如果您尚未啟用 Security Hub CSPM，AWS Control Tower 也會在這些特定帳戶和區域中為您啟用 Security Hub CSPM。

若要透過 Control Catalog 中的控制項 ID 來識別 Security Hub CSPM 控制項，您可以使用 `Implementation.Identifier`中的 欄位 AWS Control Tower。此欄位會映射至 Security Hub CSPM 控制項 ID，並可用於篩選特定控制項 ID。若要擷取 中特定 Security Hub CSPM 控制項 (例如 "CodeBuild.1") 的控制項中繼資料 AWS Control Tower，您可以使用 [ListControls](#) API：

```
aws controlcatalog list-controls --filter '{"Implementations":
{"Identifiers":["CodeBuild.1"],"Types":
["AWS::SecurityHub::SecurityControl"]}]'
```

您無法在 Security Hub CSPM 主控台、Security Hub CSPM API 中檢視或存取此標準，AWS CLI 或是在未先設定 AWS Control Tower 和啟用 Security Hub CSPM 控制項的情況下，AWS Control Tower 使用上述其中一種方法。

此標準僅適用於[AWS 區域AWS Control Tower 提供 的](#)。

在標準中啟用和停用控制項

在透過 啟用 Security Hub CSPM 控制項，AWS Control Tower 並建立服務受管標準：AWS Control Tower 標準之後，您可以在 Security Hub CSPM 中檢視標準及其可用的控制項。

當 Security Hub CSPM 將新控制項新增至服務受管標準：AWS Control Tower 標準時，不會為已啟用標準的客戶自動啟用這些控制項。您應該使用下列其中一種方法 AWS Control Tower，從 啟用和停用標準的控制項：

- AWS Control Tower 主控台
- AWS Control Tower API (呼叫 [EnableControl](#) 和 [DisableControl](#) APIs)
- AWS CLI (執行 [enable-control](#) 和 [disable-control](#) 命令)

當您在 中變更控制項的啟用狀態時 AWS Control Tower，變更也會反映在 Security Hub CSPM 中。

不過，在 Security Hub CSPM 中停用已啟用的控制項 AWS Control Tower 會導致控制偏離。中的控制項狀態 AWS Control Tower 會顯示為 Drifted。您可以使用 [ResetEnabledControl](#) API 重設偏離中的控制項，或在 AWS Control Tower 主控台中選取[重新註冊 OU](#)，或使用上述 AWS Control Tower 其中一種方法在 中停用並重新啟用控制項，以解決此偏離。

在 中完成啟用和停用動作 AWS Control Tower 可協助您避免控制偏離。

當您在 中啟用或停用控制項時 AWS Control Tower，動作會套用至受 管理的帳戶和區域 AWS Control Tower。如果您在 Security Hub CSPM 中啟用和停用控制項（不建議用於此標準），則動作僅適用於目前的帳戶和區域。

Note

[中央組態](#)無法用於管理服務受管標準：AWS Control Tower。您只能使用 AWS Control Tower 服務來啟用和停用此標準中的控制項。

檢視啟用狀態和控制狀態

您可以使用下列其中一種方法來檢視控制項的啟用狀態：

- Security Hub CSPM 主控台、Security Hub CSPM API 或 AWS CLI
- AWS Control Tower 主控台
- AWS Control Tower 用於查看已啟用控制項清單的 API (呼叫 [ListEnabledControls](#) API)
- AWS CLI 查看已啟用控制項的清單 (執行 [list-enabled-controls](#) 命令)

您在 中停用的控制項在 Security Hub CSPM Disabled 中 AWS Control Tower 具有的啟用狀態，除非您在 Security Hub CSPM 中明確啟用該控制項。

Security Hub CSPM 會根據控制調查結果的工作流程狀態和合規狀態來計算控制狀態。如需啟用狀態和控制狀態的詳細資訊，請參閱 [檢閱 Security Hub CSPM 中控制項的詳細資訊](#)。

Security Hub CSPM 會根據控制狀態計算服務受管標準的[安全分數](#)：AWS Control Tower。此分數僅適用於 Security Hub CSPM。此外，您只能在 Security Hub CSPM 中檢視[控制項問題清單](#)。標準安全分數和控制調查結果無法在 中使用 AWS Control Tower。

 Note

當您啟用 Service-Managed Standard：的控制項時 AWS Control Tower，Security Hub CSPM 最多可能需要 18 小時才能產生使用現有 AWS Config 服務連結規則之控制項的調查結果。如果您已在 Security Hub CSPM 中啟用其他標準和控制項，則可能會有現有的服務連結規則。如需詳細資訊，請參閱[執行安全檢查的排程](#)。

刪除標準

您可以使用下列其中一種方法停用所有適用的控制項 AWS Control Tower，在 中刪除此服務受管標準：

- AWS Control Tower 主控台
- AWS Control Tower API（呼叫 [DisableControl](#) API）
- AWS CLI（執行 [disable-control](#) 命令）

停用所有控制項會刪除其中所有受管帳戶和受管區域中的標準 AWS Control Tower。刪除 中的標準會將其從 Security Hub CSPM 主控台的標準頁面 AWS Control Tower 中移除，而且您無法再使用 Security Hub CSPM API 或 存取它 AWS CLI。

 Note

從 Security Hub CSPM 中的標準停用所有控制項並不會停用或刪除標準。

停用 Security Hub CSPM 服務會移除服務受管標準：AWS Control Tower 以及您啟用的任何其他標準。

尋找服務受管標準的欄位格式：AWS Control Tower

當您建立服務受管標準：AWS Control Tower 並為其啟用控制項時，您會開始在 Security Hub CSPM 中接收控制項問題清單。Security Hub CSPM 會在 中報告控制問題清單[AWS 安全調查結果格式 \(ASFF\)](#)。這些是此標準 Amazon Resource Name (ARN) 和 的 ASFF 值GeneratorId：

- 標準 ARN – `arn:aws:us-east-1:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/CodeBuild.1`

如需 Service-Managed Standard：的範例調查結果 AWS Control Tower，請參閱 [控制問題清單的範例](#)。

適用於服務受管標準的控制項：AWS Control Tower

服務受管標準：AWS Control Tower 支援屬於 AWS 基礎安全最佳實務 (FSBP) 標準一部分的控制項子集。選擇控制項以檢視相關資訊，包括失敗問題清單的修復步驟。

若要查看 支援哪些 Security Hub CSPM 控制項 AWS Control Tower，您可以使用下列其中一種方法：

- AWS 控制目錄主控台，您可以在其中篩選 “Control owner = AWS Security Hub”
- AWS Control Catalog API（呼叫 [ListControls](#) API）搭配篩選條件 Implementations 來檢查 Types 是 `AWS::SecurityHub::SecurityControl`
- AWS CLI（執行 [list-controls](#) 命令）搭配的篩選條件 Implementations。CLI 命令範例：

```
aws controlcatalog list-controls --filter '{"Implementations":{"Types":["AWS::SecurityHub::SecurityControl"]}}'
```

透過 Control Tower 標準啟用時，Security Hub CSPM 控制項的區域限制可能不符合基礎控制項的區域限制。

在 Security Hub CSPM 中，如果您的帳戶中關閉 [合併控制調查結果](#)，則產生的調查結果中的 ProductFields.ControlId 欄位會使用標準型控制 ID。標準型控制 ID 的格式為 CT.**ControlId**（例如 CT.CodeBuild.1）。

如需此標準的詳細資訊，請參閱 AWS Control Tower 《使用者指南》中的 [Security Hub CSPM 控制項](#)。

啟用安全標準

當您在 AWS Security Hub CSPM 中啟用安全標準時，Security Hub CSPM 會自動建立並啟用適用於該標準的所有控制項。Security Hub CSPM 也會開始執行安全檢查並產生控制項的問題清單。

若要最佳化問題清單的涵蓋範圍和準確性，請先在中啟用和設定資源記錄，AWS Config 再啟用標準。當您設定資源記錄時，也請務必針對套用標準之控制項檢查的所有資源類型啟用它。否

則，Security Hub CSPM 可能無法評估適當的資源，並為適用於標準的控制項產生準確的調查結果。如需詳細資訊，請參閱[啟用和設定 AWS Config Security Hub CSPM](#)。

啟用標準之後，您可以停用 或稍後重新啟用適用於標準的個別控制項。如果您停用標準控制項，Security Hub CSPM 會停止產生控制項的問題清單。此外，Security Hub CSPM 會在計算標準的安全分數時忽略控制項。安全性分數是通過評估的控制項百分比，相對於適用於標準、已啟用且具有評估資料的控制項總數。

當您啟用標準時，Security Hub CSPM 會產生該標準的初步安全分數，通常在您第一次造訪 Security Hub CSPM 主控台上的摘要或安全標準頁面的 30 分鐘內。只有在您造訪 主控台上的這些頁面時，才會針對啟用的標準產生安全分數。此外，必須在 中設定資源記錄，才能顯示 AWS Config 分數。在中國區域和 中 AWS GovCloud (US) Regions，Security Hub CSPM 最多可能需要 24 小時才能產生標準的初步安全分數。Security Hub CSPM 產生初步分數後，它會每 24 小時更新一次分數。若要判斷上次更新安全分數的時間，您可以參考 Security Hub CSPM 為分數提供的時間戳記。如需詳細資訊，請參閱[計算安全分數](#)。

啟用標準的方式取決於您是否使用[中央組態](#)來管理多個 帳戶和 的 Security Hub CSPM AWS 區域。如果您想要在多帳戶、多區域環境中啟用標準，建議您使用中央組態。如果您將 Security Hub CSPM 與整合，則可以使用中央組態 AWS Organizations。如果您不使用中央組態，則必須在每個帳戶和每個區域中分別啟用每個標準。

主題

- [在多個帳戶和 中啟用標準 AWS 區域](#)
- [在單一帳戶和 中啟用標準 AWS 區域](#)
- [檢查標準的狀態](#)

在多個帳戶和 中啟用標準 AWS 區域

若要跨多個帳戶啟用和設定安全標準 AWS 區域，請使用[中央組態](#)。透過中央組態，委派的 Security Hub CSPM 管理員可以建立啟用一或多個標準的 Security Hub CSPM 組態政策。然後，管理員可以將組態政策與個別帳戶、組織單位 (OUs) 或根帳戶建立關聯。組態政策會影響主要區域，也稱為彙總區域和所有連結的區域。

組態政策提供自訂選項。例如，您可以選擇只為一個 OU 啟用 AWS 基礎安全最佳實務 (FSBP) 標準。對於另一個 OU，您可以選擇同時啟用 FSBP 標準和 Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 標準。如需建立啟用您指定之特定標準的組態政策的詳細資訊，請參閱[建立和關聯組態政策](#)。

如果您使用中央組態，Security Hub CSPM 不會自動在新的或現有的帳戶中啟用任何標準。相反地，Security Hub CSPM 管理員會指定在為其組織建立 Security Hub CSPM 組態政策時，在不同帳戶中啟用哪些標準。Security Hub CSPM 提供建議的組態政策，其中僅啟用 FSBP 標準。如需詳細資訊，請參閱[組態政策的類型](#)。

Note

Security Hub CSPM 管理員可以使用組態政策來啟用[AWS Control Tower 服務受管標準以外](#)的任何標準。若要啟用此標準，管理員必須 AWS Control Tower 直接使用。他們還必須使用 AWS Control Tower 來啟用或停用集中管理帳戶在此標準中的個別控制項。

如果您希望某些帳戶為其自己的帳戶啟用和設定標準，Security Hub CSPM 管理員可以將這些帳戶指定為自我管理帳戶。自我管理帳戶必須在每個區域中分別啟用和設定標準。

在單一帳戶和 中啟用標準 AWS 區域

如果您不使用中央組態或擁有自我管理帳戶，則無法使用組態政策在多個帳戶或 中集中啟用安全標準 AWS 區域。不過，您可以在單一帳戶和區域中啟用標準。您可以使用 Security Hub CSPM 主控台或 Security Hub CSPM API 來執行此操作。

Security Hub CSPM console

請依照下列步驟，使用 Security Hub CSPM 主控台啟用一個帳戶和區域中的標準。

在一個帳戶和區域中啟用標準

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 使用頁面右上角的 AWS 區域 選取器，選擇您要啟用標準的區域。
3. 在導覽窗格中，選擇安全標準。安全標準頁面列出 Security Hub CSPM 目前支援的所有標準。如果您已啟用標準，則標準的 區段會包含目前的安全分數和標準的其他詳細資訊。
4. 在您要啟用的標準區段中，選擇啟用標準。

若要在其他區域中啟用標準，請在每個其他區域中重複上述步驟。

Security Hub CSPM API

若要在單一帳戶和區域中以程式設計方式啟用標準，請使用 [BatchEnableStandards](#) 操作。或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [batch-enable-standards](#) 命令。

在您的請求中，使用 `StandardsArn` 參數來指定您要啟用之標準的 Amazon Resource Name (ARN)。同時指定您的請求套用的區域。例如，下列命令會啟用 AWS 基礎安全最佳實務 (FSBP) 標準：

```
$ aws securityhub batch-enable-standards \
--standards-subscription-requests '{"StandardsArn":"arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0"}' \
--region us-east-1
```

其中 `arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0` 是美國東部（維吉尼亞北部）區域中 FSBP 標準的 ARN，而 `us-east-1` 是要在其中啟用它的區域。

若要取得標準的 ARN，請使用 [DescribeStandards](#) 操作，或者，如果您使用的是 AWS CLI，請執行 [describe-standards](#) 命令。

若要先檢閱目前在帳戶中啟用的標準清單，您可以使用 [GetEnabledStandards](#) 操作。如果您使用的是 AWS CLI，您可以執行 [get-enabled-standards](#) 命令來擷取此清單。

啟用標準之後，Security Hub CSPM 會開始執行任務，以在帳戶和指定的區域中啟用標準。這包括建立適用於標準的所有控制項。若要監控這些任務的狀態，您可以檢查帳戶和區域的標準狀態。

檢查標準的狀態

當您為帳戶啟用安全標準時，Security Hub CSPM 會開始建立適用於帳戶中標準的所有控制項。Security Hub CSPM 也會執行其他任務，以啟用帳戶的標準，例如產生標準的初步安全分數。當 Security Hub CSPM 執行這些任務時，標準的狀態 `Pending` 適用於帳戶。然後，標準的狀態會通過其他狀態，您可以監控和檢查這些狀態。

Note

標準個別控制項的變更不會影響標準的整體狀態。例如，如果您啟用先前停用的控制項，您的變更不會影響標準的狀態。同樣地，如果您變更已啟用控制項的參數值，您的變更不會影響標準的狀態。

若要使用 Security Hub CSPM 主控台檢查標準的狀態，請在導覽窗格中選擇安全標準。安全標準頁面列出 Security Hub CSPM 目前支援的所有標準。如果 Security Hub CSPM 目前正在執行啟用標準的任

務，則標準的 區段表示 Security Hub CSPM 仍在產生標準的安全分數。如果啟用標準，則標準的 區段會包含目前的分數。選擇檢視結果以檢閱其他詳細資訊，包括適用於標準之個別控制項的狀態。如需詳細資訊，請參閱[執行安全檢查的排程](#)。

若要使用 Security Hub CSPM API 以程式設計方式檢查標準的狀態，請使用 [GetEnabledStandards](#) 操作。在您的請求中，選擇性地使用 `StandardsSubscriptionArns` 參數來指定您要檢查其狀態的標準 Amazon Resource Name (ARN)。如果您使用的是 AWS Command Line Interface (AWS CLI)，您可以執行 [get-enabled-standards](#) 命令來檢查標準的狀態。若要指定要檢查的標準 ARN，請使用 `standards-subscription-arns` 參數。若要決定要指定的 ARN，您可以使用 [DescribeStandards](#) 操作，或針對 AWS CLI 執行 [describe-standards](#) 命令。

如果您的請求成功，Security Hub CSPM 會以 物件陣列回應 `StandardsSubscription`。標準訂閱是 Security Hub CSPM 為帳戶啟用標準時，在帳戶中建立 AWS 的資源。每個 `StandardsSubscription` 物件都會提供有關帳戶目前已啟用或正在啟用或停用之標準的詳細資訊。在每個物件中，`StandardsStatus` 欄位會指定帳戶的 標準目前狀態。

標準 (`StandardsStatus`) 的狀態可以是下列其中一項。

PENDING

Security Hub CSPM 目前正在執行任務，以啟用帳戶的 標準。這包括建立適用於標準的控制項，並為標準產生初步安全分數。Security Hub CSPM 可能需要幾分鐘的時間來完成所有任務。如果已為帳戶啟用標準，且 Security Hub CSPM 目前正在將新控制項新增至標準，則標準也可以具有此狀態。

如果標準具有此狀態，您可能無法擷取適用於標準之個別控制項的詳細資訊。此外，您可能無法設定或停用標準的個別控制項。例如，如果您嘗試使用 [UpdateStandardsControl](#) 操作停用控制項，則會發生錯誤。

若要判斷您是否可以設定或以其他方式管理 標準的個別控制項，請參閱 `StandardsControlsUpdatable` 欄位的值。如果此欄位的值為 `READY_FOR_UPDATES`，您可以開始管理標準的個別控制項。否則，請等待 Security Hub CSPM 完成其他處理任務以啟用標準。

READY

帳戶目前已啟用標準。Security Hub CSPM 可以執行安全檢查，並針對適用於標準且目前啟用的所有控制項產生調查結果。Security Hub CSPM 也可以計算標準的安全分數。

如果標準具有此狀態，您可以擷取適用於標準之個別控制項的詳細資訊。此外，您可以設定、停用或重新啟用控制項。您也可以停用標準。

INCOMPLETE

Security Hub CSPM 無法完全為帳戶啟用標準。Security Hub CSPM 無法執行安全檢查，並針對適用於標準且目前已啟用的所有控制項產生調查結果。此外，Security Hub CSPM 無法計算標準的安全分數。

若要判斷未完全啟用標準的原因，請參閱 `StandardsStatusReason` 陣列中的資訊。此陣列會指定導致 Security Hub CSPM 無法啟用標準的問題。如果發生內部錯誤，請嘗試再次為帳戶啟用標準。對於其他類型的問題，[請檢查您的 AWS Config 設定](#)。您也可以[停用您不想檢查的個別控制項](#)，或完全停用標準。

DELETING

Security Hub CSPM 目前正在處理停用帳戶標準的請求。這包括停用適用於標準的控制項，以及移除相關聯的安全分數。Security Hub CSPM 可能需要幾分鐘的時間才能完成處理請求。

如果標準具有此狀態，則您無法重新啟用標準，或嘗試再次為帳戶停用該標準。Security Hub CSPM 必須先完成處理目前的請求。此外，您無法擷取適用於標準或管理控制項之個別控制項的詳細資訊。

FAILED

Security Hub CSPM 無法停用帳戶的標準。當 Security Hub CSPM 嘗試停用標準時發生一或多個錯誤。此外，Security Hub CSPM 無法計算標準的安全分數。

若要判斷未完全停用標準的原因，請參閱 `StandardsStatusReason` 陣列中的資訊。此陣列會指定防止 Security Hub CSPM 停用標準的問題。

如果標準具有此狀態，則您無法擷取適用於標準或管理控制項之個別控制項的詳細資訊。不過，您可以重新啟用帳戶的標準。如果您解決導致 Security Hub CSPM 無法停用標準的問題，您也可以嘗試再次停用標準。

如果標準的狀態為 `READY`，Security Hub CSPM 會執行安全檢查，並針對適用於標準且目前啟用的所有控制項產生問題清單。對於其他狀態，Security Hub CSPM 可能會執行檢查，並產生某些但並非所有已啟用控制項的問題清單。最多可能需要 24 小時才能產生或更新控制調查結果。如需詳細資訊，請參閱[執行安全檢查的排程](#)。

檢閱安全標準的詳細資訊

在 AWS Security Hub CSPM 中啟用安全標準之後，您可以使用主控台來檢閱標準的詳細資訊。在主控台上，標準的詳細資訊頁面包含下列資訊：

- 標準目前的安全分數。
- 適用於標準的控制表。
- 適用於標準之控制項的彙總統計資料。
- 適用於標準之控制項狀態的視覺化摘要。
- 已啟用並套用到標準之控制項的安全檢查視覺化摘要。如果您與 整合 AWS Organizations，在至少一個組織帳戶中啟用的控制項會被視為已啟用。

若要檢閱這些詳細資訊，請在主控台的導覽窗格中選擇安全標準。然後，在標準的 區段中，選擇檢視結果。若要進行更深入的分析，您可以篩選和排序資料，並向下切入以檢閱適用於標準之個別控制項的詳細資訊。

主題

- [了解標準安全分數](#)
- [檢閱標準的控制項](#)

了解標準安全分數

在 AWS Security Hub CSPM 主控台上，標準的詳細資訊頁面會顯示標準的安全分數。分數是通過評估的控制項百分比，相對於適用於標準、已啟用且具有評估資料的控制項總數。在分數下是一個圖表，摘要針對標準啟用的控制項進行安全檢查。這包括通過和失敗的安全檢查數量。對於管理員帳戶，標準分數和圖表會跨管理員帳戶和所有成員帳戶彙總。若要檢閱具有特定嚴重性之控制項的失敗安全檢查，請選擇嚴重性。

當您啟用標準時，Security Hub CSPM 會產生該標準的初步安全分數，通常在您第一次造訪摘要頁面或 Security Hub CSPM 主控台上的安全標準頁面後 30 分鐘內。只會針對您造訪這些頁面時啟用的標準產生分數。此外，必須設定 AWS Config 資源記錄，才能顯示分數。在中國區域和 中 AWS GovCloud (US) Regions，Security Hub CSPM 最多可能需要 24 小時才能產生初步分數。Security Hub CSPM 為標準產生初步分數後，它會每 24 小時更新一次分數。如需詳細資訊，請參閱[計算安全分數](#)。

除非您設定彙總區域，AWS 區域 否則安全標準詳細資訊頁面上的所有資料都專屬於目前的。如果您設定彙總區域，安全分數會跨區域套用，並包含所有連結區域的調查結果。此外，控制項的合規狀態會反映連結區域的調查結果，而安全檢查的數量包括連結區域的調查結果。

檢閱標準的控制項

當您使用 AWS Security Hub CSPM 主控台檢閱您啟用之標準的詳細資訊時，您可以檢閱適用於標準的安全控制表。對於每個控制項，資料表包含下列資訊：

- 控制項 ID 和標題。
- 控制項的狀態。如需詳細資訊，請參閱[評估合規狀態和控制狀態](#)。
- 指派給控制項的嚴重性。
- 失敗的檢查數量和檢查總數。如果適用，失敗檢查欄位也會指定狀態為未知的調查結果數量。
- 控制項是否支援自訂參數。如需詳細資訊，請參閱[了解 Security Hub CSPM 中的控制參數](#)。

Security Hub CSPM 每 24 小時更新一次控制狀態和安全檢查計數。頁面頂端的時間戳記指出 Security Hub CSPM 最近更新此資料的時間。

對於管理員帳戶，控制項狀態和安全檢查數量會在管理員帳戶和所有成員帳戶中彙總。已啟用控制項的計數包含針對管理員帳戶或至少一個成員帳戶中的標準啟用的控制項。停用控制項的計數包含針對管理員帳戶和所有成員帳戶中的標準停用的控制項。

您可以篩選適用於標準的控制項資料表。使用資料表旁的依選項篩選，您可以選擇僅檢視啟用或停用的標準控制項。如果您只顯示已啟用的控制項，您可以進一步依控制項狀態篩選資料表。然後，您可以專注於具有特定控制狀態的控制項。除了依選項篩選之外，您可以在篩選控制項方塊中輸入篩選條件條件。例如，您可以依控制項 ID 或標題進行篩選。

選擇您偏好的存取方法。然後依照步驟來檢閱適用於您啟用之標準的控制項。

Security Hub CSPM console

若要檢閱已啟用標準的控制項

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中選擇安全標準。
3. 在標準區段中，選擇檢視結果。

頁面底部的資料表會列出適用於標準的所有控制項。您可以篩選和排序資料表。您也可以將資料表的目前頁面下載為 CSV 檔案。若要這樣做，請選擇資料表上方的下載。如果您篩選資料表，下載的檔案只會包含符合您目前篩選條件設定的控制項。

Security Hub CSPM API

若要檢閱已啟用標準的控制項

1. 使用 Security Hub CSPM API [ListSecurityControlDefinitions](#) 的操作。如果您使用的是 AWS CLI，請執行 [list-security-control-definitions](#) 命令。

指定您要檢閱控制項之標準的 Amazon Resource Name (ARN)。若要取得標準的 ARNs，請使用 [DescribeStandards](#) 操作或執行 [describe-standards](#) 命令。如果您未指定標準的 ARN，Security Hub CSPM 會傳回所有安全控制 IDs。

2. 使用 Security Hub CSPM API [ListStandardsControlAssociations](#) 的操作，或執行 [list-standards-control-associations](#) 命令。此操作會告訴您在哪些標準中啟用了控制項。

透過提供安全控制 ID 或 ARN 來識別控制項。分頁參數是選用的。

下列範例會告訴您在哪些標準中啟用 Config.1 控制項。

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

關閉自動啟用的安全標準

如果您的組織不使用中央組態，則會使用稱為本機組態的組態類型。使用本機組態，AWS Security Hub CSPM 可以在帳戶加入您的組織時自動為新成員帳戶啟用預設安全標準。套用至這些預設標準的所有控制項也會自動啟用。

目前，預設安全標準是 AWS 基礎安全最佳實務標準和網際網路安全中心 (CIS) AWS 基準 1.2.0 版標準。如需這些標準的資訊，請參閱 [Security Hub CSPM 的標準參考](#)。

如果您偏好手動啟用新成員帳戶的安全標準，您可以關閉預設標準的自動啟用。只有在與整合 AWS Organizations 並使用本機組態時，才能執行此操作。如果您使用中央組態，您可以改為建立啟用預設標準的組態政策，並將政策與根建立關聯。然後，所有組織帳戶和 OUs 都會繼承此組態政策，除非它們與不同的政策相關聯或自我管理。如果您未與整合 AWS Organizations，您可以在最初啟用 Security Hub CSPM 或更新版本時停用預設標準。若要了解作法，請參閱 [停用標準](#)。

若要關閉新成員帳戶預設標準的自動啟用，您可以使用 Security Hub CSPM 主控台或 Security Hub CSPM API。

Security Hub CSPM console

請依照下列步驟，使用 Security Hub CSPM 主控台關閉預設標準的自動啟用。

關閉預設標準的自動啟用

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用管理員帳戶的登入資料登入。

2. 在導覽窗格中的設定下，選擇組態。
3. 在概觀區段中，選擇編輯。
4. 在新帳戶設定下，清除啟用預設安全標準核取方塊。
5. 選擇確認。

Security Hub CSPM API

若要以程式設計方式關閉預設標準的自動啟用，請從 Security Hub CSPM 管理員帳戶使用 Security Hub CSPM API [UpdateOrganizationConfiguration](#) 的操作。在您的請求中，NONE 為 `AutoEnableStandards` 參數指定。

如果您使用的是 AWS CLI，請執行 [update-organization-configuration](#) 命令來關閉預設標準的自動啟用。針對 `auto-enable-standards` 參數，請指定 NONE。例如，下列命令會自動為新成員帳戶啟用 Security Hub CSPM，並關閉帳戶預設標準的自動啟用。

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-standards NONE
```

停用安全標準

當您在 AWS Security Hub CSPM 中停用安全標準時，會發生下列情況：

- 套用至標準的所有控制項都會停用，除非它們與目前啟用的另一個標準相關聯。
- 不再執行已停用控制項的安全檢查，也不會為已停用的控制項產生其他問題清單。
- 停用控制項的現有問題清單會在大約 3-5 天後自動封存。
- AWS Config 刪除 Security Hub CSPM 為已停用控制項建立的規則。

刪除適當的 AWS Config 規則通常會在停用標準的幾分鐘內發生。不過，這可能需要更長的時間。如果第一個請求無法刪除規則，Security Hub CSPM 會每 12 小時重試一次。不過，如果您停用 Security Hub CSPM 或未啟用任何其他標準，Security Hub CSPM 將無法重試，這表示它無法刪除規則。如果發生這種情況，而且您需要刪除規則，請聯絡 AWS 支援。

主題

- [在多個帳戶和 中停用標準 AWS 區域](#)
- [在單一帳戶和 中停用標準 AWS 區域](#)

在多個帳戶和 中停用標準 AWS 區域

若要停用多個帳戶和 之間的安全標準 AWS 區域，請使用[中央組態](#)。透過中央組態，委派的 Security Hub CSPM 管理員可以建立停用一或多個標準的 Security Hub CSPM 組態政策。然後，管理員可以將組態政策與個別帳戶、組織單位 (OUs) 或根帳戶建立關聯。組態政策會影響主要區域，也稱為彙總區域和所有連結的區域。

組態政策提供自訂選項。例如，您可以選擇在一個 OU 中停用支付卡產業資料安全標準 (PCI DSS)。對於另一個 OU，您可以選擇停用 PCI DSS 和國家標準技術研究所 (NIST) SP 800-53 修訂版 5 標準。如需有關建立啟用或停用您指定之個別標準的組態政策的詳細資訊，請參閱 [建立和關聯組態政策](#)。

Note

Security Hub CSPM 管理員可以使用組態政策來停用[AWS Control Tower 服務受管標準以外的任何標準](#)。若要停用此標準，管理員必須 AWS Control Tower 直接使用。他們還必須使用 AWS Control Tower 來停用或啟用集中管理帳戶在此標準中的個別控制項。

如果您希望某些帳戶為自己的帳戶設定或停用標準，Security Hub CSPM 管理員可以將這些帳戶指定為自我管理帳戶。自我管理帳戶必須在每個區域中分別停用標準。

在單一帳戶和 中停用標準 AWS 區域

如果您不使用中央組態或擁有自我管理帳戶，則無法使用組態政策來集中停用多個帳戶或 中的安全標準 AWS 區域。不過，您可以在單一帳戶和區域中停用標準。您可以使用 Security Hub CSPM 主控台或 Security Hub CSPM API 來執行此操作。

Security Hub CSPM console

請依照下列步驟，使用 Security Hub CSPM 主控台停用一個帳戶和區域中的標準。

停用一個帳戶和區域中的標準

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 使用頁面右上角的 AWS 區域 選取器，選擇您要停用標準的區域。
3. 在導覽窗格中，選擇安全標準。
4. 在您要停用的標準區段中，選擇停用標準。

若要在其他區域中停用標準，請在每個其他區域中重複上述步驟。

Security Hub CSPM API

若要在單一帳戶和區域中以程式設計方式停用標準，請使用 [BatchDisableStandards](#) 操作。或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [batch-disable-standards](#) 命令。

在您的請求中，使用 `StandardsSubscriptionArns` 參數來指定您要停用之標準的 Amazon Resource Name (ARN)。如果您使用的是 AWS CLI，請使用 `standards-subscription-arns` 參數來指定 ARN。同時指定您的請求套用的區域。例如，下列命令會停用 帳戶 (123456789012) AWS 的基礎安全最佳實務 (FSBP) 標準：

```
$ aws securityhub batch-disable-standards \
--standards-subscription-arns "arn:aws:securityhub:us-
east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0" \
--region us-east-1
```

其中 `arn#aws#securityhub#us-east-1#123456789012#subscription/aws-foundational-security-best-practices/v/1.0.0` 是美國東部（維吉尼亞北部）區域中帳戶的 FSBP 標準的 ARN，而 `us-east-1` 是要在其中停用它的區域。

若要取得標準的 ARN，您可以使用 [GetEnabledStandards](#) 操作。此操作會擷取目前在您帳戶中啟用之標準的相關資訊。如果您使用的是 AWS CLI，您可以執行 [get-enabled-standards](#) 命令來擷取此資訊。

停用標準之後，Security Hub CSPM 會開始執行任務，以停用帳戶和指定區域中的標準。這包括停用適用於標準的所有控制項。若要監控這些任務的狀態，您可以[檢查帳戶和區域的標準狀態](#)。

了解 Security Hub CSPM 中的安全控制

在 AWS Security Hub CSPM 中，安全控制也稱為控制項，是一種安全標準中的保護措施，可協助組織保護資訊的機密性、完整性和可用性。在 Security Hub CSPM 中，控制項與特定 AWS 資源相關。

當您在一或多個標準中啟用控制項時，Security Hub CSPM 會開始對其執行安全檢查。安全檢查會產生 Security Hub CSPM 調查結果。當您停用控制項時，Security Hub CSPM 會停止對其執行安全檢查，而且不會再產生問題清單。

您可以個別啟用或停用單一帳戶和的控制項 AWS 區域。為了節省時間並減少多帳戶環境中的組態偏離，我們建議您使用[中央組態](#)來啟用或停用控制項。透過中央組態，委派的 Security Hub CSPM 管理員可以建立政策，指定如何在多個帳戶和區域中設定控制項。如需啟用和停用控制項的詳細資訊，請參閱 [在 Security Hub CSPM 中啟用控制項](#)。

合併控制項檢視

Security Hub CSPM 主控台的控制項頁面會顯示目前中可用的所有控制項 AWS 區域（您可以透過造訪安全標準頁面並選擇啟用的標準，在標準內容中檢視控制項）。Security Hub CSPM 指派控制跨標準一致的安全控制 ID、標題和描述。控制項 IDs 包括相關 AWS 服務和唯一數字（例如 CodeBuild.3）。

下列資訊可在 [Security Hub CSPM 主控台](#) 的控制頁面上取得：

- 整體安全分數，根據傳遞控制項與具有資料之已啟用控制項總數的比例
- 所有支援的 Security Hub CSPM 控制項的控制狀態明細
- 通過和失敗的安全檢查總數。
- 針對不同嚴重性控制項的失敗安全檢查數量，以及檢視這些失敗檢查詳細資訊的連結。
- Security Hub CSPM 控制項的清單，其中包含可檢視特定控制項子集的篩選條件。

在控制項頁面中，您可以選擇控制項以檢視其詳細資訊，並對控制項產生的調查結果採取動作。在此頁面上，您也可以目前的 AWS 帳戶和中啟用或停用安全控制 AWS 區域。控制頁面的啟用和停用動作會跨標準套用。如需詳細資訊，請參閱[在 Security Hub CSPM 中啟用控制項](#)。

對於管理員帳戶，控制項頁面會反映成員帳戶之間的控制項狀態。如果至少一個成員帳戶中的控制項檢查失敗，則控制項狀態為失敗。如果您已設定[彙總區域](#)，則控制項頁面會反映所有連結區域的控制項狀態。如果至少一個連結區域中的控制項檢查失敗，則控制項狀態為失敗。

合併控制項檢視會導致變更，以控制 AWS 安全性調查結果格式 (ASFF) 中可能影響工作流程的調查結果欄位。如需詳細資訊，請參閱[合併控制項檢視 – ASFF 變更](#)。

控制項的摘要安全分數

控制頁面會顯示 0-100% 的摘要安全分數。摘要安全分數是根據通過的控制項與具有跨標準資料的已啟用控制項總數的比例來計算。

Note

若要檢視控制項的整體安全分數，您必須新增許可，以 **BatchGetControlEvaluations** 呼叫您用來存取 Security Hub CSPM 的 IAM 角色。檢視特定標準的安全性分數不需要此許可。

當您啟用 Security Hub CSPM 時，Security Hub CSPM 會在您第一次造訪 Security Hub CSPM 主控台的摘要頁面或安全標準頁面後 30 分鐘內計算初始安全分數。在中國區域和中，首次產生安全分數最多可能需要 24 小時 AWS GovCloud (US) Regions。

除了整體安全分數之外，Security Hub CSPM 還會在您第一次造訪摘要頁面或安全標準頁面後 30 分鐘內計算每個已啟用標準的標準安全分數。若要檢視目前啟用的標準清單，請使用 [GetEnabledStandards](#) API 操作。

AWS Config 必須啟用資源記錄，才能顯示分數。如需 Security Hub CSPM 如何計算安全分數的資訊，請參閱 [計算安全分數](#)。

第一次產生分數後，Security Hub CSPM 會每 24 小時更新一次安全分數。Security Hub CSPM 會顯示時間戳記，指出上次更新安全分數的時間。

如果您已設定彙總區域，則整體安全分數會反映連結區域之間的控制問題清單。

Security Hub CSPM 的控制項參考

此控制項參考提供可用的 AWS Security Hub CSPM 控制項資料表，其中包含每個控制項的詳細資訊連結。在表格中，控制項會依控制項 ID 的字母順序列出。此處僅包含 Security Hub CSPM 作用中使用的控制項。已淘汰的控制項會從資料表中排除。

資料表提供每個控制項的下列資訊：

- 安全控制 ID – 此 ID 適用於所有標準，並指出控制項相關的 AWS 服務和資源。Security Hub CSPM 主控台會顯示安全控制 IDs，無論您的帳戶中是否開啟或關閉 [合併控制調查結果](#)。不過，只有在您的帳戶中開啟合併控制調查結果時，Security Hub CSPM 調查結果才會參考安全控制 IDs。如果您的帳戶中關閉了合併控制調查結果，則某些控制 IDs 會因控制調查結果中的標準而有所不同。如需標準特定控制 IDs 與安全控制 IDs 的映射，請參閱 [合併如何影響控制 IDs 和標題](#)。

如果您想要為安全控制設定[自動化](#)，建議您根據控制 ID 而非標題或描述進行篩選。雖然 Security Hub CSPM 可能會偶爾更新控制項標題或描述，但控制項 IDs 會保持不變。

控制項 IDs 可能會略過數字。這些是未來控制的預留位置。

- **安全控制標題** – 此標題適用於所有標準。Security Hub CSPM 主控台會顯示安全控制標題，無論您的帳戶中是否開啟或關閉合併控制問題清單。不過，只有在您的帳戶中開啟合併控制調查結果時，Security Hub CSPM 調查結果才會參考安全控制標題。如果您的帳戶中關閉了合併控制調查結果，則某些控制標題會因控制調查結果中的標準而有所不同。如需標準特定控制 IDs 與安全控制 IDs 的映射，請參閱 [合併如何影響控制 IDs 和標題](#)。
- **適用標準** – 指出適用於控制項的標準。選擇控制項，以檢閱第三方合規架構的特定需求。
- **嚴重性** – 控制項的嚴重性從安全角度識別其重要性。如需 Security Hub CSPM 如何判斷控制嚴重性的資訊，請參閱 [控制問題清單的嚴重性等級](#)。
- **支援自訂參數** – 指出控制項是否支援一或多個參數的自訂值。選擇控制項以檢閱參數詳細資訊。如需詳細資訊，請參閱 [了解 Security Hub CSPM 中的控制參數](#)。
- **排程類型** – 指出何時評估控制項。如需詳細資訊，請參閱 [執行安全檢查的排程](#)。

選擇控制項以檢閱其他詳細資訊。控制項會依安全控制項 ID 的字母順序列出。

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Account.1	應提供的安全聯絡資訊 AWS 帳戶	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	媒體	⊗ 否	定期
帳戶。2	AWS 帳戶應該是 AWS Organizations 組織的一部分	NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ACM.1	匯入和 ACM 發行的憑證應在指定的期間之後續約	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2、PCI DSS v4.0.1	媒體	✔ 是	變更已觸發和定期
ACM.2	ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度	AWS 基礎安全最佳實務 1.0.0 版、PCI DSS 4.0.1 版	HIGH (高)	✘ 否	變更已觸發
ACM.3	ACM 憑證應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Amplify.1	Amplify 應用程式應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Amplify.2	Amplify 分支應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
APIGateway.y.1	應啟用 API Gateway REST 和 WebSocket API 執行記錄	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	✔ 是	變更已觸發
APIGateway.y.2	API Gateway REST API 階段應設定為使用 SSL 憑證進行後端身分驗證	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	媒體	✘ 否	變更已觸發
APIGateway.y.3	API Gateway REST API 階段應該已啟用 AWS X-Ray 追蹤	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	✘ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
APIGateway.y.4	API Gateway 應與 WAF Web ACL 建立關聯	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	⊗ 否	變更已觸發
APIGateway.y.5	API Gateway REST API 快取資料應靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	⊗ 否	變更已觸發
APIGateway.y.8	API Gateway 路由應指定授權類型	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	✔ 是	定期
APIGateway.y.9	應該為 API Gateway V2 階段設定存取記錄	AWS 基礎安全最佳實務 1.0.0 版、NIST SP 800-53 第 5 版、PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
APIGateway.y.10	API Gateway V2 整合應使用 HTTPS 進行私有連線	AWS 基礎安全最佳實務 1.0.0 版	中	⊗ 否	變更已觸發
APIGateway.y.11	API Gateway 網域名稱應使用建議的安全政策	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
AppConfig.1	AWS AppConfig 應用程式應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
AppConfig.2	AWS AppConfig 組態設定檔應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
AppConfig.3	AWS AppConfig 環境應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
AppConfig.4	AWS AppConfig 延伸關聯應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
AppFlow.1	Amazon AppFlow 流程應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
AppRunner.1	App Runner 服務應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
AppRunner.2	App Runner VPC 連接器應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
AppSync.2	AWS AppSync 應該啟用欄位層級記錄	AWS 基礎安全最佳實務 1.0.0 版、PCI DSS 4.0.1 版	中	☑ 是	變更已觸發
AppSync.4	AWS AppSync GraphQL APIs 應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
AppSync.5	AWS AppSync GraphQL APIs 不應使用 API 金鑰進行身分驗證	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	☒ 否	變更已觸發
Athena.2	Athena 資料目錄應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
Athena.3	Athena 工作群組應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
Athena.4	Athena 工作群組應該已啟用記錄	AWS 基礎安全最佳實務	中	☒ 否	變更已觸發
AutoScaling.1	與負載平衡器相關聯的 Auto Scaling 群組應使用 ELB 運作狀態檢查	AWS 基礎安全最佳實務，PCI DSS v3.2.1，NIST SP 800-53 修訂版 5	低	☒ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
AutoScaling.2	Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✔ 是	變更已觸發
AutoScaling.3	Auto Scaling 群組啟動組態應該將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 (IMDSv2)	AWS 基礎安全最佳實務 1.0.0 版、NIST SP 800-53 第 5 版、PCI DSS 4.0.1 版	HIGH (高)	✘ 否	變更已觸發
AutoScaling.5	使用 Auto Scaling 群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址	AWS 基礎安全最佳實務 1.0.0 版、NIST SP 800-53 第 5 版、PCI DSS 4.0.1 版	HIGH (高)	✘ 否	變更已觸發
AutoScaling.6	Auto Scaling 群組應在多個可用區域中使用多個執行個體類型	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	✘ 否	變更已觸發
AutoScaling.9	EC2 Auto Scaling 群組應使用 EC2 啟動範本	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	✘ 否	變更已觸發
AutoScaling.10	EC2 Auto Scaling 群組應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
備份。1	AWS Backup 復原點應靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	✘ 否	變更已觸發
備份。2	AWS Backup 復原點應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
備份。3	AWS Backup 保存庫應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
備份。4	AWS Backup 報告計畫應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
備份。5	AWS Backup 備份計畫應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Batch.1	批次任務佇列應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Batch.2	批次排程政策應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Batch.3	批次運算環境應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Batch.4	受管批次運算環境中的運算資源屬性應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
BedrockAgentCore.1	Bedrock AgentCore 執行時間應使用 VPC 網路模式設定	AWS 基礎安全最佳實務	HIGH (高)	✘ 否	變更已觸發
BedrockAgentCore.2	Bedrock AgentCore Gateways 應要求傳入請求的授權	AWS 基礎安全最佳實務	HIGH (高)	✘ 否	變更已觸發
BedrockAgentCore.3	Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密	NIST SP 800-53 修訂版 5	媒體	✘ 否	變更已觸發
BedrockAgentCore.4	Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密	NIST SP 800-53 修訂版 5	媒體	✘ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
BedrockAgentCore.5	Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式	AWS 基礎安全最佳實務	HIGH (高)	⊗ 否	變更已觸發
BedrockAgentCore.6	Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄	AWS 基礎安全最佳實務	媒體	⊗ 否	變更已觸發
CloudFormation.2	CloudFormation 堆疊應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
CloudFormation.3	CloudFormation 堆疊應該啟用終止保護	AWS 基礎安全最佳實務	媒體	⊗ 否	變更已觸發
CloudFormation.4	CloudFormation 堆疊應該具有相關聯的服務角色	AWS 基礎安全最佳實務	媒體	⊗ 否	變更已觸發
CloudFront.t.1	CloudFront 分佈應該設定預設根物件	AWS 基礎安全最佳實務 1.0.0 版、NIST SP 800-53 第 5 版、PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	變更已觸發
CloudFront.t.3	CloudFront 分佈應該需要傳輸中加密	AWS 基礎安全最佳實務 1.0.0 版、NIST SP 800-53 第 5 版、PCI DSS 4.0.1 版	媒體	⊗ 否	變更已觸發
CloudFront.t.4	CloudFront 分佈應設定原始伺服器容錯移轉	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發
CloudFront.t.5	CloudFront 分佈應該已啟用記錄	AWS 基礎安全最佳實務 1.0.0 版、NIST SP 800-53 第 5 版、PCI DSS 4.0.1 版	媒體	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudFront.t.6	CloudFront 分佈應該啟用 WAF	AWS 基礎安全最佳實務 1.0.0 版、NIST SP 800-53 第 5 版、PCI DSS 4.0.1 版	媒體	⊗ 否	變更已觸發
CloudFront.t.7	CloudFront 分佈應使用自訂 SSL/TLS 憑證	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	低	⊗ 否	變更已觸發
CloudFront.t.8	CloudFront 分佈應使用 SNI 來提供 HTTPS 請求	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發
CloudFront.t.9	CloudFront 分佈應該加密到自訂原始伺服器的流量	AWS 基礎安全最佳實務 1.0.0 版、NIST SP 800-53 第 5 版、PCI DSS 4.0.1 版	媒體	⊗ 否	變更已觸發
CloudFront.t.10	CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2、PCI DSS v4.0.1	媒體	⊗ 否	變更已觸發
CloudFront.t.12	CloudFront 分佈不應指向不存在的 S3 原始伺服器	AWS 基礎安全最佳實務 1.0.0 版、NIST SP 800-53 第 5 版、PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期
CloudFront.t.13	CloudFront 分佈應使用原始存取控制	AWS 基礎安全最佳實務 1.0.0 版	媒體	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudFront.14	應標記 CloudFront 分佈	AWS 資源標記標準	低	✔ 是	變更已觸發
CloudFront.15	CloudFront 分佈應使用建議的 TLS 安全政策	AWS 基礎安全最佳實務 1.0.0 版	媒體	✘ 否	變更已觸發
CloudFront.16	CloudFront 分佈應該使用 Lambda 函數 URL 原始伺服器的原始存取控制	AWS 基礎安全最佳實務 1.0.0 版	媒體	✘ 否	變更已觸發
CloudFront.17	CloudFront 分佈應該針對簽章URLs 和 Cookie 使用信任的金鑰群組	AWS 基礎安全最佳實務 1.0.0 版	媒體	✘ 否	變更已觸發
CloudTrail.1	CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域線索	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5	HIGH (高)	✘ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudTrail I.2	CloudTrail 應該啟用靜態加密	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0 AWS Foundations 安全最佳實務 v1.0.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1、PCI DSS v4.0.1	媒體	⊗ 否	定期
CloudTrail I.3	至少應啟用一個 CloudTrail 追蹤	NIST SP 800-171 第 2 版，PCI DSS 4.0.1 版，PCI DSS 3.2.1 版	HIGH (高)	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudTrail I.4	應啟用 CloudTrail 日誌檔案驗證	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1、PCI DSS v3.2.1	低	⊗ 否	定期
CloudTrail I.5	CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1	媒體	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudTrail I.6	確保不公開存取用於儲存 CloudTrail 日誌的 S3 儲存貯體	CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0、PCI DSS v4.0.1	關鍵	⊗ 否	變更已觸發和定期
CloudTrail I.7	確保 CloudTrail S3 儲存貯體已啟用 S3 儲存貯體存取日誌記錄	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.2.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v3.0.0、PCI DSS v4.0.1	低	⊗ 否	定期
CloudTrail I.9	CloudTrail 追蹤應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
CloudTrail I.10	CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys	NIST SP 800-53 修訂版 5	中	☑ 是	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudWatch h.1	應該存在日誌指標篩選條件和警示，以使用「根」使用者	CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1	低	⊗ 否	定期
CloudWatch h.2	確保未經授權的 API 呼叫中存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.2.0 版，NIST SP 800-171 修訂版 2	低	⊗ 否	定期
CloudWatch h.3	確保不使用 MFA 的管理主控台登入存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.2.0 版	低	⊗ 否	定期
CloudWatch h.4	確保 IAM 政策變更存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.4.0 版、CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	低	⊗ 否	定期
CloudWatch h.5	確保 CloudTrail 組態變更存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.4.0 版、CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	低	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudWatch h.6	確保 AWS 管理主控台驗證失敗時存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.4.0 版、CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	低	⊗ 否	定期
CloudWatch h.7	確保停用或排定刪除客戶建立的 CMK 存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.4.0 版、CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	低	⊗ 否	定期
CloudWatch h.8	確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.4.0 版、CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	低	⊗ 否	定期
CloudWatch h.9	確保 AWS Config 組態變更存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.4.0 版、CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	低	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudWatch h.10	確保安全群組變更存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.4.0 版、CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	低	⊗ 否	定期
CloudWatch h.11	確保網路存取控制清單 (NACL) 變更存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.4.0 版、CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	低	⊗ 否	定期
CloudWatch h.12	確保網路閘道變更存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.4.0 版、CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	低	⊗ 否	定期
CloudWatch h.13	確保路由表變更存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.4.0 版、CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	低	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CloudWatch.h.14	確保 VPC 變更存在日誌指標篩選條件和警示	CIS AWS Foundations Benchmark 1.4.0 版、CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	低	⊗ 否	定期
CloudWatch.h.15	CloudWatch 警示應該已設定指定的動作	NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2	HIGH (高)	✔ 是	變更已觸發
CloudWatch.h.16	CloudWatch 日誌群組應保留一段指定的時間	NIST SP 800-53 修訂版 5	中	✔ 是	定期
CloudWatch.h.17	應啟用 CloudWatch 警示動作	NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	變更已觸發
CodeArtifact.act.1	CodeArtifact 儲存庫應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
CodeBuild.1	CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 3.2.1 版，PCI DSS 4.0.1 版	關鍵	⊗ 否	變更已觸發
CodeBuild.2	CodeBuild 專案環境變數不應包含純文字登入資料	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 3.2.1 版，PCI DSS 4.0.1 版	關鍵	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
CodeBuild.3	CodeBuild S3 日誌應加密	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版，	低	⊗ 否	變更已觸發
CodeBuild.4	CodeBuild 專案環境應具有記錄組態	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
CodeBuild.7	CodeBuild 報告群組匯出應靜態加密	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
CodeGuruProfiler.1	CodeGuru Profiler 分析群組應加上標籤	AWS 資源標記標準	低	⊙ 是	變更已觸發
CodeGuruReviewer.1	CodeGuru Reviewer 儲存庫關聯應加上標籤	AWS 資源標記標準	低	⊙ 是	變更已觸發
Cognito.1	Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護	AWS 基礎安全最佳實務	中	⊙ 是	變更已觸發
Cognito.2	Cognito 身分集區不應允許未驗證的身分	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
Cognito.3	Cognito 使用者集區的密碼政策應該具有強大的組態	AWS 基礎安全最佳實務	中	⊙ 是	變更已觸發
Cognito.4	Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Cognito.5	應為 Cognito 使用者集區啟用 MFA	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
Cognito.6	Cognito 使用者集區應啟用刪除保護	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
Config.1	AWS Config 應啟用並使用服務連結角色進行資源記錄	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1	關鍵	✔ 是	定期
Connect.1	Connect Customer Profiles 物件類型應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Connect.2	Connect Customer 執行個體應該啟用 CloudWatch 記錄	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
DataFirehose.1	Firehose 交付串流應靜態加密	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
DataSync.1	DataSync 任務應該已啟用記錄	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
DataSync.2	DataSync 任務應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
Detective.1	Detective 行為圖表應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
DMS.1	Database Migration Service 複寫執行個體不應為公有	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 3.2.1 版，PCI DSS 4.0.1 版	關鍵	⊗ 否	定期
DMS.2	DMS 憑證應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
DMS.3	DMS 事件訂閱應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
DMS.4	DMS 複寫執行個體應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
DMS.5	DMS 複寫子網路群組應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
DMS.6	DMS 複寫執行個體應啟用自動次要版本升級	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
DMS.7	目標資料庫的 DMS 複寫任務應該已啟用記錄	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
DMS.8	來源資料庫的 DMS 複寫任務應該已啟用記錄	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
DMS.9	DMS 端點應使用 SSL	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
DMS.10	Neptune 資料庫的 DMS 端點應啟用 IAM 授權	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
DMS.11	MongoDB 的 DMS 端點應該啟用身分驗證機制	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
DMS.12	Redis OSS 的 DMS 端點應該已啟用 TLS	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
DMS.13	DMS 複寫執行個體應設定為使用多個可用區域	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
DocumentDB.1	Amazon DocumentDB 叢集應靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
DocumentDB B.2	Amazon DocumentDB 叢集應具有足夠的備份保留期	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	✔ 是	變更已觸發
DocumentDB B.3	Amazon DocumentDB 手動叢集快照不應公開	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	關鍵	✘ 否	變更已觸發
DocumentDB B.4	Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	✘ 否	變更已觸發
DocumentDB B.5	Amazon DocumentDB 叢集應該啟用刪除保護	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
DocumentDB B.6	Amazon DocumentDB 叢集應在傳輸中加密	AWS 基礎安全最佳實務	中	✘ 否	定期
DynamoDB 1	DynamoDB 資料表應隨著需求自動擴展容量	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✔ 是	定期
DynamoDB 2	DynamoDB 資料表應該啟用point-in-time復原	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
DynamoDB 3	DynamoDB Accelerator (DAX) 叢集應靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	定期
DynamoDB 4	DynamoDB 資料表應存在於備份計畫中	NIST SP 800-53 修訂版 5	中	✔ 是	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
DynamoDB 5	DynamoDB 資料表應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
DynamoDB 6	DynamoDB 資料表應該已啟用刪除保護	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
DynamoDB 7	DynamoDB Accelerator 叢集應在傳輸中加密	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	✘ 否	定期
EC2.1	EBS 快照不應可公開還原	AWS 基礎安全最佳實務 1.0.0 版、PCI DSS 3.2.1 版、NIST SP 800-53 第 5 版	關鍵	✘ 否	定期
EC2.2	VPC 預設安全群組不應允許傳入或傳出流量	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices v1.0.0、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	HIGH (高)	✘ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.3	連接的 EBS 磁碟區應該靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
EC2.4	停止的 EC2 執行個體應該在指定的時段之後移除	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✔ 是	定期
EC2.6	應在所有 VPC 中啟用 VPCs 流程記錄	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices v1.0.0、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	中	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.7	應啟用 EBS 預設加密	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、AWS Foundational Security Best Practices v1.0.0、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	中	⊗ 否	定期
EC2.8	EC2 執行個體應使用執行個體中繼資料服務第 2 版 (IMDSv2)	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	HIGH (高)	⊗ 否	變更已觸發
EC2.9	EC2 執行個體不應具有公有 IPv4 地址	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	變更已觸發
EC2.10	Amazon EC2 應設定為使用為 Amazon EC2 服務建立的 VPC 端點	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	中	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.12	應該移除未使用的 EC2 EIPs	PCI DSS v3.2.1、NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發
EC2.13	安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 22	CIS AWS Foundations Benchmark 1.2.0 版、PCI DSS 3.2.1 版、PCI DSS 4.0.1 版、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	HIGH (高)	⊗ 否	變更已觸發和定期
EC2.14	安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389	CIS AWS Foundations Benchmark 1.2.0 版、PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	變更已觸發和定期
EC2.15	EC2 子網路不應自動指派公有 IP 地址	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版，	中	⊗ 否	變更已觸發
EC2.16	應該移除未使用的網路存取控制清單	AWS 基礎安全最佳實務、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2、PCI DSS 4.0.1、	低	⊗ 否	變更已觸發
EC2.17	EC2 執行個體不應使用多個 ENIs	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.18	安全群組應僅允許授權連接埠的無限制傳入流量	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	HIGH (高)	✔ 是	變更已觸發
EC2.19	安全群組不應允許無限制存取高風險的連接埠	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2	關鍵	✘ 否	變更已觸發和定期
EC2.20	用於 an AWS Site-to-Site VPN 連線的兩個 VPN 通道都應啟動	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	中	✘ 否	變更已觸發
EC2.21	網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	中	✘ 否	變更已觸發
EC2.22	應該移除未使用的 EC2 安全群組		中	✘ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.23	EC2 Transit Gateways 不應自動接受 VPC 連接請求	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	變更已觸發
EC2.24	不應使用 EC2 全虛擬執行個體類型	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
EC2.25	EC2 啟動範本不應將公IPs 指派給網路介面	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	變更已觸發
EC2.28	EBS 磁碟區應位於備份計畫中	NIST SP 800-53 修訂版 5	低	☑ 是	定期
EC2.33	EC2 傳輸閘道附件應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
EC2.34	EC2 傳輸閘道路由表應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
EC2.35	EC2 網路介面應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
EC2.36	EC2 客戶閘道應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
EC2.37	EC2 彈性 IP 地址應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
EC2.38	應標記 EC2 執行個體	AWS 資源標記標準	低	☑ 是	變更已觸發
EC2.39	EC2 網際網路閘道應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.40	EC2 NAT 閘道應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.41	EC2 網路 ACLs 應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.42	EC2 路由表應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.43	EC2 安全群組應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.44	EC2 子網路應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.45	EC2 磁碟區應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.46	Amazon VPCs 應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.47	Amazon VPC 端點服務應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.48	Amazon VPC 流程日誌應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.49	Amazon VPC 對等互連連線應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.50	EC2 VPN 閘道應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.51	EC2 Client VPN 端點應該啟用用戶端連線記錄	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2，PCI DSS 4.0.1	低	⊗ 否	變更已觸發
EC2.52	EC2 傳輸閘道應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.53	EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、PCI DSS v4.0.1	HIGH (高)	⊗ 否	定期
EC2.54	EC2 安全群組不應允許從 :::/0 傳入遠端伺服器管理連接埠	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、PCI DSS v4.0.1	HIGH (高)	⊗ 否	定期
EC2.55	VPCs應使用 ECR API 的介面端點進行設定	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	媒體	✔ 是	定期
EC2.56	VPCs應使用 Docker 登錄檔的介面端點進行設定	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	媒體	✔ 是	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.57	VPCs應使用 Systems Manager 的介面端點進行設定	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	媒體	✔ 是	定期
EC2.58	VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	媒體	✔ 是	定期
EC2.60	VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	媒體	✔ 是	定期
EC2.170	EC2 啟動範本應使用執行個體中繼資料服務第 2 版 (IMDSv2)	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	低	✘ 否	變更已觸發
EC2.171	EC2 VPN 連線應該已啟用記錄	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	媒體	✘ 否	變更已觸發
EC2.172	EC2 VPC 封鎖公開存取設定應封鎖網際網路閘道流量	AWS 基礎安全最佳實務	媒體	✔ 是	變更已觸發
EC2.173	具有啟動參數的 EC2 Spot Fleet 請求應為連接的 EBS 磁碟區啟用加密	AWS 基礎安全最佳實務	媒體	✘ 否	變更已觸發
EC2.174	EC2 DHCP 選項集應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.175	EC2 啟動範本應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EC2.176	EC2 字首清單應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.177	EC2 流量鏡像工作階段應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.178	EC2 流量鏡像篩選條件應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.179	EC2 流量鏡像目標應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EC2.180	EC2 網路介面應啟用來源/目的地檢查	AWS 基礎安全最佳實務 1.0.0 版	媒體	✘ 否	變更已觸發
EC2.181	EC2 啟動範本應為連接的 EBS 磁碟區啟用加密	AWS 基礎安全最佳實務 1.0.0 版	媒體	✘ 否	變更已觸發
EC2.182	EBS 快照不應公開存取	AWS 基礎安全最佳實務	HIGH (高)	✘ 否	變更已觸發
EC2.183	EC2 VPN 連線應使用 IKEv2 通訊協定	AWS 基礎安全最佳實務	媒體	✘ 否	變更已觸發
ECR.1	ECR 私有儲存庫應設定映像掃描	AWS 基礎安全最佳實務 1.0.0 版、NIST SP 800-53 第 5 版、PCI DSS 4.0.1 版	HIGH (高)	✘ 否	定期
ECR.2	ECR 私有儲存庫應設定標籤不可變性	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	✘ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ECR.3	ECR 儲存庫應至少設定一個生命週期政策	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	⊗ 否	變更已觸發
ECR.4	ECR 公有儲存庫應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
ECR.5	ECR 儲存庫應使用客戶受管加密 AWS KMS keys	NIST SP 800-53 修訂版 5	媒體	✔ 是	變更已觸發
ECS.2	ECS 服務不應自動為其指派公有 IP 地址	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	變更已觸發
ECS.3	ECS 任務定義不應共用主機的程序命名空間	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	變更已觸發
ECS.4	ECS 容器應以非特殊權限執行	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	變更已觸發
ECS.5	ECS 容器應僅限於對根檔案系統的唯讀存取	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	變更已觸發
ECS.8	秘密不應做為容器環境變數傳遞	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	變更已觸發
ECS.9	ECS 任務定義應具有記錄組態	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ECS.10	ECS Fargate 服務應在最新的 Fargate 平台版本上執行	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	媒體	⊗ 否	變更已觸發
ECS.12	ECS 叢集應使用 Container Insights	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	⊗ 否	變更已觸發
ECS.13	ECS 服務應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
ECS.14	ECS 叢集應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
ECS.15	ECS 任務定義應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
ECS.16	ECS 任務集不應自動指派公有 IP 地址	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	變更已觸發
ECS.17	ECS 任務定義不應使用主機網路模式	NIST SP 800-53 修訂版 5	媒體	⊗ 否	變更已觸發
ECS.18	ECS 任務定義應針對 EFS 磁碟區使用傳輸中加密	AWS 基礎安全最佳實務	媒體	⊗ 否	變更已觸發
ECS.19	ECS 容量提供者應該啟用受管終止保護	AWS 基礎安全最佳實務	媒體	⊗ 否	變更已觸發
ECS.20	ECS 任務定義應在 Linux 容器定義中設定非根使用者	AWS 基礎安全最佳實務	媒體	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ECS.21	ECS 任務定義應在 Windows 容器定義中設定非管理員使用者	AWS 基礎安全最佳實務	媒體	⊗ 否	變更已觸發
EFS.1	彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	媒體	⊗ 否	定期
EFS.2	Amazon EFS 磁碟區應處於備份計劃中	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	⊗ 否	定期
EFS.3	EFS 存取點應強制執行根目錄	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	媒體	⊗ 否	變更已觸發
EFS.4	EFS 存取點應強制執行使用者身分	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
EFS.5	EFS 存取點應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EFS.6	EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯	AWS 基礎安全最佳實務	中	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EFS.7	EFS 檔案系統應該啟用自動備份	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
EFS.8	EFS 檔案系統應靜態加密	CIS AWS Foundations Benchmark v5.0.0，AWS 基礎安全最佳實務	中	✔ 是	變更已觸發
EKS.1	不應公開存取 EKS 叢集端點	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期
EKS.2	EKS 叢集應在支援的 Kubernetes 版本上執行	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	變更已觸發
EKS.3	EKS 叢集應使用加密的 Kubernetes 秘密	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	定期
EKS.6	EKS 叢集應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EKS.7	EKS 身分提供者組態應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
EKS.8	EKS 叢集應該啟用稽核記錄	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EKS.9	EKS 節點群組應在支援的 Kubernetes 版本上執行	AWS 基礎安全最佳實務	HIGH (高)	⊗ 否	變更已觸發
ElastiCache.1	ElastiCache (Redis OSS) 叢集應該啟用自動備份	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	✔ 是	定期
ElastiCache.2	ElastiCache 叢集應該啟用自動次要版本升級	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期
ElastiCache.3	ElastiCache 複寫群組應該啟用自動容錯移轉	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	定期
ElastiCache.4	ElastiCache 複寫群組應該靜態 encrypted-at-rest	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	定期
ElastiCache.5	ElastiCache 複寫群組應該在 encrypted-in-transit	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	定期
ElastiCache.6	舊版的 ElastiCache (Redis OSS) 複寫群組應該已啟用 Redis OSS AUTH	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	定期
ElastiCache.7	ElastiCache 叢集不應使用預設子網路群組	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ElasticBeanstalk.1	Elastic Beanstalk 環境應啟用增強型運作狀態報告	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發
ElasticBeanstalk.2	應啟用 Elastic Beanstalk 受管平台更新	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	HIGH (高)	✔ 是	變更已觸發
ElasticBeanstalk.3	Elastic Beanstalk 應該將日誌串流到 CloudWatch	AWS 基礎安全最佳實務，PCI DSS v4.0.1	HIGH (高)	✔ 是	變更已觸發
ELB.1	Application Load Balancer 應設定為將所有 HTTP 請求重新導向至 HTTPS	AWS 基礎安全最佳實務 1.0.0 版、PCI DSS 3.2.1 版、NIST SP 800-53 第 5 版	中	⊗ 否	定期
ELB.2	具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用提供的憑證 AWS Certificate Manager	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	中	⊗ 否	變更已觸發
ELB.3	Classic Load Balancer 接聽程式應設定為 HTTPS 或 TLS 終止	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2，PCI DSS 4.0.1	中	⊗ 否	變更已觸發
ELB.4	Application Load Balancer 應設定為捨棄 http 標頭	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ELB.5	應啟用應用程式和 Classic Load Balancer 記錄	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
ELB.6	應用程式、閘道和 Network Load Balancer 應啟用刪除保護	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
ELB.7	Classic Load Balancer 應啟用連線耗盡	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發
ELB.8	具有 SSL 接聽程式的 Classic Load Balancer 應使用具有強大組態的預先定義安全政策	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
ELB.9	Classic Load Balancer 應啟用跨區域負載平衡	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
ELB.10	Classic Load Balancer 應跨越多個可用區域	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✔ 是	變更已觸發
ELB.12	Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
ELB.13	應用程式、網路和閘道負載平衡器應跨越多個可用區域	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✔ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ELB.14	Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
ELB.16	Application Load Balancer 應與 AWS WAF Web ACL 建立關聯	NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
ELB.17	具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
ELB.18	應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料	AWS 基礎安全最佳實務 1.0.0 版	中	⊗ 否	變更已觸發
ELB.21	應用程式和 Network Load Balancer 目標群組應使用加密的運作狀態檢查通訊協定	AWS 基礎安全最佳實務 1.0.0 版	中	⊗ 否	變更已觸發
ELB.22	ELB 目標群組應使用加密的傳輸通訊協定	AWS 基礎安全最佳實務 1.0.0 版	中	⊗ 否	變更已觸發
EMR.1	Amazon EMR 叢集主節點不應具有公有 IP 地址	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
EMR.2	應啟用 Amazon EMR 封鎖公開存取設定	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	關鍵	⊗ 否	定期
EMR.3	Amazon EMR 安全組態應靜態加密	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
EMR.4	Amazon EMR 安全組態應在傳輸中加密	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
ES.1	Elasticsearch 網域應該啟用靜態加密	AWS 基礎安全最佳實務 1.0.0 版、PCI DSS 3.2.1 版、NIST SP 800-53 第 5 版	中	⊗ 否	定期
ES.2	Elasticsearch 網域不應可公開存取	AWS 基礎安全最佳實務、PCI DSS v3.2.1、PCI DSS v4.0.1、NIST SP 800-53 Rev. 5	關鍵	⊗ 否	定期
ES.3	Elasticsearch 網域應該加密節點之間傳送的資料	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版，	中	⊗ 否	變更已觸發
ES.4	應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
ES.5	Elasticsearch 網域應該啟用稽核記錄	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
ES.6	Elasticsearch 網域應該至少具有三個資料節點	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
ES.7	Elasticsearch 網域應該至少設定三個專用主節點	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
ES.8	應使用最新的 TLS 安全政策加密與 Elasticsearch 網域的連線	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
ES.9	應標記 Elasticsearch 網域	AWS 資源標記標準	低	☑ 是	變更已觸發
EventBridge.2	應標記 EventBridge 事件匯流排	AWS 資源標記標準	低	☑ 是	變更已觸發
EventBridge.3	EventBridge 自訂事件匯流排應該連接以資源為基礎的政策	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	低	⊗ 否	變更已觸發
EventBridge.4	EventBridge 全域端點應該已啟用事件複寫	NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
FraudDetector.1	Amazon Fraud Detector 實體類型應該加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
FraudDetector.2	Amazon Fraud Detector 標籤應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
FraudDetector.3	Amazon Fraud Detector 結果應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
FraudDetector.4	Amazon Fraud Detector 變數應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
FSx.1	FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	✘ 否	定期
FSx.2	FSx for Lustre 檔案系統應設定為將標籤複製到備份	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	低	✘ 否	定期
FSx.3	FSx for OpenZFS 檔案系統應設定為異地同步備份部署	AWS 基礎安全最佳實務	中	✘ 否	定期
FSx.4	FSx for NetApp ONTAP 檔案系統應設定為異地同步備份部署	AWS 基礎安全最佳實務	中	✔ 是	定期
FSx.5	FSx for Windows File Server 檔案系統應設定為異地同步備份部署	AWS 基礎安全最佳實務	中	✘ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Glue.1	AWS Glue 任務應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Glue.3	AWS Glue 機器學習轉換應該靜態加密	AWS 基礎安全最佳實務	中	✘ 否	變更已觸發
Glue.4	AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
GlobalAccelerator.1	Global Accelerator 加速器應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
GuardDuty.1	GuardDuty 應啟用	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2，PCI DSS 3.2.1 版，PCI DSS 4.0.1 版	HIGH (高)	✘ 否	定期
GuardDuty.2	GuardDuty 篩選條件應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
GuardDuty.3	GuardDuty IPSets 應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
GuardDuty.4	GuardDuty 偵測器應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
GuardDuty.5	應啟用 GuardDuty EKS 稽核日誌監控	AWS 基礎安全最佳實務	HIGH (高)	✘ 否	定期
GuardDuty.6	應啟用 GuardDuty Lambda 保護	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	HIGH (高)	✘ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
GuardDuty .7	應啟用 GuardDuty EKS 執行期監控	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期
GuardDuty .8	應啟用 EC2 的 GuardDuty 惡意軟體防護	AWS 基礎安全最佳實務	HIGH (高)	⊗ 否	定期
GuardDuty .9	應啟用 GuardDuty RDS 保護	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期
GuardDuty .10	應啟用 GuardDuty S3 保護	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期
GuardDuty .11	應啟用 GuardDuty 執行期監控	AWS 基礎安全最佳實務	HIGH (高)	⊗ 否	定期
GuardDuty .12	應啟用 GuardDuty ECS 執行期監控	AWS 基礎安全最佳實務	媒體	⊗ 否	定期
GuardDuty .13	應啟用 GuardDuty EC2 執行期監控	AWS 基礎安全最佳實務	媒體	⊗ 否	定期
IAM.1	IAM 政策不應允許完整的「*」管理權限	CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices v1.0.0、PCI DSS v3.2.1、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	HIGH (高)	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.2	IAM 使用者不應連接 IAM 政策	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices v1.0.0、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2	低	⊗ 否	變更已觸發
IAM.3	IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	媒體	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.4	IAM 根使用者存取金鑰不應存在	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices v1.0.0、PCI DSS v3.2.1、NIST SP 800-53 Rev. 5	關鍵	⊗ 否	定期
IAM.5	應為具有主控台密碼的所有 IAM 使用者啟用 MFA	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	媒體	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.6	應為根使用者啟用硬體 MFA	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1	關鍵	⊗ 否	定期
IAM.7	IAM 使用者的密碼政策應具有強大的組態	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2，PCI DSS 4.0.1	媒體	☑ 是	定期
IAM.8	應該移除未使用的 IAM 使用者登入資料	CIS AWS Foundations Benchmark v1.2.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1、PCI DSS v4.0.1	媒體	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.9	應為根使用者啟用 MFA	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1	關鍵	⊗ 否	定期
IAM.10	IAM 使用者的密碼政策應具有強大的組態	NIST SP 800-171 第 2 版，PCI DSS 3.2.1 版	媒體	⊗ 否	定期
IAM.11	確保 IAM 密碼政策至少需要一個大寫字母	CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 第 2 版、PCI DSS 4.0.1 版	媒體	⊗ 否	定期
IAM.12	確保 IAM 密碼政策至少需要一個小寫字母	CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 第 2 版、PCI DSS 4.0.1 版	媒體	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.13	確保 IAM 密碼政策至少需要一個符號	CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 修訂版 2	媒體	⊗ 否	定期
IAM.14	確保 IAM 密碼政策至少需要一個數字	CIS AWS Foundations Benchmark 1.2.0 版、NIST SP 800-171 第 2 版、PCI DSS 4.0.1 版	媒體	⊗ 否	定期
IAM.15	確保 IAM 密碼政策要求密碼長度下限為 14 或更高	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2	中	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.16	確保 IAM 密碼政策防止重複使用密碼	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	低	⊗ 否	定期
IAM.17	確保 IAM 密碼政策在 90 天內過期密碼	CIS AWS Foundations Benchmark 1.2.0 版、PCI DSS 4.0.1 版	低	⊗ 否	定期
IAM.18	確保已建立支援角色來使用 管理事件 AWS 支援	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-171 Rev. 2、PCI DSS v4.0.1	低	⊗ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.19	應為所有 IAM 使用者啟用 MFA	NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2、PCI DSS 3.2.1、PCI DSS 4.0.1	中	⊗ 否	定期
IAM.21	您建立的 IAM 客戶受管政策不應允許服務的萬用字元動作	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	低	⊗ 否	變更已觸發
IAM.22	應移除未使用 45 天的 IAM 使用者登入資料	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-171 Rev. 2	中	⊗ 否	定期
IAM.23	IAM Access Analyzer 分析器應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IAM.24	IAM 角色應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IAM.25	IAM 使用者應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IAM.26	應該移除在 IAM 中管理的過期 SSL/TLS 憑證	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0	中	⊗ 否	定期
IAM.27	IAM 身分不應連接 AWSCloudShellFullAccess 政策	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0	中	⊗ 否	變更已觸發
IAM.28	應啟用 IAM Access Analyzer 外部存取分析器	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0	HIGH (高)	⊗ 否	定期
Inspector .1	應啟用 Amazon Inspector EC2 掃描	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期
Inspector .2	應啟用 Amazon Inspector ECR 掃描	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期
Inspector .3	應啟用 Amazon Inspector Lambda 程式碼掃描	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期
Inspector .4	應啟用 Amazon Inspector Lambda 標準掃描	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期
IoT.1	AWS IoT Device Defender 安全設定檔應加上標籤	AWS 資源標記標準	低	✅ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IoT.2	AWS IoT Core 應標記緩解動作	AWS 資源標記標準	低	☑ 是	變更已觸發
IoT.3	AWS IoT Core 維度應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IoT.4	AWS IoT Core 授權方應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IoT.5	AWS IoT Core 角色別名應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IoT.6	AWS IoT Core 政策應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IoTEvents.1	AWS IoT Events 輸入應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IoTEvents.2	AWS IoT Events 偵測器模型應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IoTEvents.3	AWS IoT Events 警示模型應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IoTSiteWise.1	AWS IoT SiteWise 資產模型應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IoTSiteWise.2	AWS IoT SiteWise 儀表板應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IoTSiteWise.3	AWS IoT SiteWise 閘道應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
IoTSiteWise.4	AWS IoT SiteWise 入口網站應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
IoTSiteWise.5	AWS IoT SiteWise 專案應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
IoTtwinmaker.1	AWS IoT TwinMaker 同步任務應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
IoTtwinmaker.2	AWS IoT TwinMaker 工作區應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
IoTtwinmaker.3	AWS IoT TwinMaker 場景應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
IoTtwinmaker.4	AWS IoT TwinMaker 實體應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
IoTWireless.1	AWS IoT Wireless 多點傳送群組應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
IoTWireless.2	AWS IoT Wireless 服務設定檔應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
IoTWireless.3	AWS IoT Wireless FUOTA 任務應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
IVS.1	IVS 播放金鑰對應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
IVS.2	IVS 記錄組態應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
IVS.3	IVS 頻道應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
鍵空間。1	Amazon Keyspaces 金鑰空間應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Kinesis.1	Kinesis 串流應靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
Kinesis.2	Kinesis 串流應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Kinesis.3	Kinesis 串流應具有足夠的資料保留期	AWS 基礎安全最佳實務	中	✔ 是	變更已觸發
KMS.1	IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
KMS.2	IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
KMS.3	AWS KMS keys 不應意外刪除	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	關鍵	✘ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
KMS.4	AWS KMS key 應該啟用輪換	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、CIS AWS Foundations Benchmark v1.2.0、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1	中	⊗ 否	定期
KMS.5	不應公開存取 KMS 金鑰	AWS 基礎安全最佳實務	關鍵	⊗ 否	變更已觸發
Lambda.1	Lambda 函數政策應禁止公開存取	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 3.2.1 版，PCI DSS 4.0.1 版	關鍵	⊗ 否	變更已觸發
Lambda.2	Lambda 函數應使用支援的執行時間	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
Lambda.3	Lambda 函數應該位於 VPC 中	PCI DSS v3.2.1、NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Lambda.5	VPC Lambda 函數應該在多個可用區域中操作	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	☑ 是	變更已觸發
Lambda.6	Lambda 函數應該加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
Lambda.7	Lambda 函數應該啟用 AWS X-Ray 主動追蹤	NIST SP 800-53 修訂版 5	低	☒ 否	變更已觸發
Macie.1	應啟用 Amazon Macie	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	☒ 否	定期
Macie.2	應啟用 Macie 自動化敏感資料探索	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	☒ 否	定期
MSK.1	MSK 叢集應該在代理程式節點之間傳輸時加密	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	☒ 否	變更已觸發
MSK.2	MSK 叢集應該已設定增強型監控	NIST SP 800-53 修訂版 5	低	☒ 否	變更已觸發
MSK.3	MSK Connect 連接器應該在傳輸中加密	AWS 基礎安全最佳實務，PCI DSS v4.0.1	中	☒ 否	變更已觸發
MSK.4	MSK 叢集應該停用公有存取	AWS 基礎安全最佳實務	關鍵	☒ 否	變更已觸發
MSK.5	MSK 連接器應該已啟用記錄	AWS 基礎安全最佳實務	中	☒ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
MSK.6	MSK 叢集應停用未驗證的存取	AWS 基礎安全最佳實務	中	否	變更已觸發
MQ.2	ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	否	變更已觸發
MQ.4	Amazon MQ 代理程式應加上標籤	AWS 資源標記標準	低	是	變更已觸發
MQ.5	ActiveMQ 代理程式應使用作用中/待命部署模式	NIST SP 800-53 修訂版 5	低	否	變更已觸發
MQ.6	RabbitMQ 代理程式應使用叢集部署模式	NIST SP 800-53 修訂版 5	低	否	變更已觸發
Neptune.1	Neptune 資料庫叢集應靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	否	變更已觸發
Neptune.2	Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	否	變更已觸發
Neptune.3	Neptune 資料庫叢集快照不應公開	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	關鍵	否	變更已觸發
Neptune.4	Neptune 資料庫叢集應該啟用刪除保護	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Neptune.5	Neptune 資料庫叢集應該啟用自動備份	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	☑ 是	變更已觸發
Neptune.6	Neptune 資料庫叢集快照應靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	☒ 否	變更已觸發
Neptune.7	Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	☒ 否	變更已觸發
Neptune.8	Neptune 資料庫叢集應設定為將標籤複製到快照	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	☒ 否	變更已觸發
Neptune.9	Neptune 資料庫叢集應該跨多個可用區域部署	NIST SP 800-53 修訂版 5	中	☒ 否	變更已觸發
NetworkFirewall.1	網路防火牆防火牆應部署在多個可用區域	NIST SP 800-53 修訂版 5	中	☒ 否	變更已觸發
NetworkFirewall.2	應啟用 Network Firewall 記錄	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	中	☒ 否	定期
NetworkFirewall.3	Network Firewall 政策應至少有一個相關聯的規則群組	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	中	☒ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
NetworkFirewall.4	Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
NetworkFirewall.5	Network Firewall 政策的預設無狀態動作應為捨棄或轉送分段封包	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	中	⊗ 否	變更已觸發
NetworkFirewall.6	無狀態網路防火牆規則群組不應為空	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	中	⊗ 否	變更已觸發
NetworkFirewall.7	應標記 Network Firewall 防火牆	AWS 資源標記標準	低	✔ 是	變更已觸發
NetworkFirewall.8	應標記 Network Firewall 防火牆政策	AWS 資源標記標準	低	✔ 是	變更已觸發
NetworkFirewall.9	Network Firewall 防火牆應該啟用刪除保護	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
NetworkFirewall.10	Network Firewall 防火牆應該啟用子網路變更保護	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
OpenSearch.1	OpenSearch 網域應該啟用靜態加密	AWS 基礎安全最佳實務 1.0.0 版、PCI DSS 3.2.1 版、NIST SP 800-53 第 5 版	中	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Opensearch h.2	OpenSearch 網域不應可公開存取	AWS 基礎安全最佳實務 1.0.0 版、PCI DSS 3.2.1 版、NIST SP 800-53 第 5 版	關鍵	⊗ 否	變更已觸發
Opensearch h.3	OpenSearch 網域應該加密節點之間傳送的資料	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
Opensearch h.4	應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
Opensearch h.5	OpenSearch 網域應該啟用稽核記錄	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
Opensearch h.6	OpenSearch 網域應至少具有三個資料節點	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
Opensearch h.7	OpenSearch 網域應該啟用精細存取控制	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	變更已觸發
Opensearch h.8	應使用最新的 TLS 安全政策加密與 OpenSearch 網域的連線	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
Opensearch h.9	OpenSearch 網域應加上標籤	AWS 資源標記標準	低	✅ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Opensearch h.10	OpenSearch 網域應該已安裝最新的軟體更新	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
Opensearch h.11	OpenSearch 網域應至少具有三個專用主節點	NIST SP 800-53 修訂版 5	低	⊗ 否	定期
PCA.1	AWS 私有 CA 應停用根憑證授權單位	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	⊗ 否	定期
PCA.2	AWS 私有 CA 憑證授權單位應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
RDS.1	RDS 快照應為私有	AWS 基礎安全最佳實務 1.0.0 版、PCI DSS 3.2.1 版、NIST SP 800-53 第 5 版	關鍵	⊗ 否	變更已觸發
RDS.2	RDS 資料庫執行個體應禁止公開存取，由 PubliclyAccessible 組態決定	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1	關鍵	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.3	RDS 資料庫執行個體應啟用靜態加密	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices v1.0.0、NIST SP 800-53 Rev. 5	中	⊗ 否	變更已觸發
RDS.4	RDS 叢集快照和資料庫快照應靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
RDS.5	RDS 資料庫執行個體應該設定多個可用區域	CIS AWS Foundations Benchmark v5.0.0、AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
RDS.6	應為 RDS 資料庫執行個體設定增強型監控	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	✔ 是	變更已觸發
RDS.7	RDS 叢集應該已啟用刪除保護	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
RDS.8	RDS 資料庫執行個體應該已啟用刪除保護	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.9	RDS 資料庫執行個體應將日誌發佈至 CloudWatch Logs	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
RDS.10	應為 RDS 執行個體設定 IAM 身分驗證	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
RDS.11	RDS 執行個體應該啟用自動備份	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✔ 是	變更已觸發
RDS.12	應為 RDS 叢集設定 IAM 身分驗證	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
RDS.13	應啟用 RDS 自動次要版本升級	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	HIGH (高)	⊗ 否	變更已觸發
RDS.14	Amazon Aurora 叢集應該已啟用恢復	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✔ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.15	應為多個可用區域設定 RDS 資料庫叢集	CIS AWS Foundations Benchmark v5.0.0、AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
RDS.16	Aurora 資料庫叢集應設定為將標籤複製到資料庫快照	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發
RDS.17	RDS 資料庫執行個體應設定為將標籤複製到快照	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發
RDS.18	RDS 執行個體應該部署在 VPC 中		HIGH (高)	⊗ 否	變更已觸發
RDS.19	應為關鍵叢集事件設定現有的 RDS 事件通知訂閱	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發
RDS.20	應為關鍵資料庫執行個體事件設定現有的 RDS 事件通知訂閱	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	低	⊗ 否	變更已觸發
RDS.21	應為關鍵資料庫參數群組事件設定 RDS 事件通知訂閱	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	低	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.22	應為關鍵資料庫安全群組事件設定 RDS 事件通知訂閱	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	低	⊗ 否	變更已觸發
RDS.23	RDS 執行個體不應使用資料庫引擎預設連接埠	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發
RDS.24	RDS 資料庫叢集應使用自訂管理員使用者名稱	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
RDS.25	RDS 資料庫執行個體應使用自訂管理員使用者名稱	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
RDS.26	RDS 資料庫執行個體應受備份計劃保護	NIST SP 800-53 修訂版 5	中	☑ 是	定期
RDS.27	RDS 資料庫叢集應靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
RDS.28	RDS 資料庫叢集應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
RDS.29	RDS 資料庫叢集快照應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發
RDS.30	RDS 資料庫執行個體應加上標籤	AWS 資源標記標準	低	☑ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.31	RDS 資料庫安全群組應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
RDS.32	RDS 資料庫快照應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
RDS.33	RDS 資料庫子網路群組應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
RDS.34	Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	✘ 否	變更已觸發
RDS.35	RDS 資料庫叢集應該啟用自動次要版本升級	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	✘ 否	變更已觸發
RDS.36	RDS for PostgreSQL 資料庫執行個體應將日誌發佈至 CloudWatch Logs	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	中	✔ 是	變更已觸發
RDS.37	Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs	AWS 基礎安全最佳實務，PCI DSS 4.0.1 版	中	✘ 否	變更已觸發
RDS.38	RDS for PostgreSQL 資料庫執行個體應在傳輸中加密	AWS 基礎安全最佳實務	中	✘ 否	定期
RDS.39	RDS for MySQL 資料庫執行個體應在傳輸中加密	AWS 基礎安全最佳實務	中	✘ 否	定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.40	RDS for SQL Server 資料庫執行個體應將日誌發佈至 CloudWatch Logs	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	✔ 是	變更已觸發
RDS.41	RDS for SQL Server 資料庫執行個體應在傳輸中加密	AWS 基礎安全最佳實務	中	✘ 否	定期
RDS.42	RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	✔ 是	定期
RDS.43	RDS 資料庫代理應該需要連線的 TLS 加密	AWS 基礎安全最佳實務	中	✘ 否	定期
RDS.44	RDS for MariaDB 資料庫執行個體應在傳輸中加密	AWS 基礎安全最佳實務	中	✘ 否	定期
RDS.45	Aurora MySQL 資料庫叢集應該啟用稽核記錄	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	✘ 否	定期
RDS.46	RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中	AWS 基礎安全最佳實務	HIGH (高)	✘ 否	定期
RDS.47	RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照	AWS 基礎安全最佳實務	低	✘ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
RDS.48	RDS for MySQL 資料庫叢集應設定為將標籤複製到資料庫快照	AWS 基礎安全最佳實務	低	⊗ 否	變更已觸發
RDS.50	RDS 資料庫叢集應設定足夠的備份保留期	AWS 基礎安全最佳實務 1.0.0 版	中	⊗ 是	變更已觸發
RDS.51	RDS 全域叢集應在支援的 Aurora MySQL 版本上執行	AWS 基礎安全最佳實務	HIGH (高)	⊗ 否	變更已觸發
Redshift.1	Amazon Redshift 叢集應禁止公開存取	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 3.2.1 版，PCI DSS 4.0.1 版	關鍵	⊗ 否	變更已觸發
Redshift.2	與 Amazon Redshift 叢集的連線應在傳輸中加密	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
Redshift.3	Amazon Redshift 叢集應該啟用自動快照	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✔ 是	變更已觸發
Redshift.4	Amazon Redshift 叢集應該啟用稽核記錄	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
Redshift.6	Amazon Redshift 應該已啟用主要版本的自動升級	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Redshift. 7	Redshift 叢集應使用增強型 VPC 路由	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
Redshift. 8	Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
Redshift. 10	Redshift 叢集應靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
Redshift. 11	應標記 Redshift 叢集	AWS 資源標記標準	低	☑ 是	變更已觸發
Redshift. 12	應標記 Redshift 事件訂閱通知	AWS 資源標記標準	低	☑ 是	變更已觸發
Redshift. 13	應標記 Redshift 叢集快照	AWS 資源標記標準	低	☑ 是	變更已觸發
Redshift. 14	應標記 Redshift 叢集子網路群組	AWS 資源標記標準	低	☑ 是	變更已觸發
Redshift. 15	Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠	AWS 基礎安全最佳實務，PCI DSS v4.0.1	HIGH (高)	⊗ 否	定期
Redshift. 16	Redshift 叢集子網路群組應具有來自多個可用區域的子網路	NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
Redshift. 17	應標記 Redshift 叢集參數群組	AWS 資源標記標準	低	☑ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Redshift.18	Redshift 叢集應該啟用異地同步備份部署	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
RedshiftServerless.1	Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由	AWS 基礎安全最佳實務	HIGH (高)	⊗ 否	定期
RedshiftServerless.2	使用 SSL 時，需要連線至 Redshift Serverless 工作群組	AWS 基礎安全最佳實務	中	⊗ 否	定期
RedshiftServerless.3	Redshift Serverless 工作群組應禁止公開存取	AWS 基礎安全最佳實務	HIGH (高)	⊗ 否	定期
RedshiftServerless.4	Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys	NIST SP 800-53 修訂版 5	中	✔ 是	定期
RedshiftServerless.5	Redshift Serverless 命名空間不應使用預設的管理員使用者名稱	AWS 基礎安全最佳實務	中	⊗ 否	定期
RedshiftServerless.6	Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs	AWS 基礎安全最佳實務	中	⊗ 否	定期
Route53.1	Route 53 運作狀態檢查應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Route53.2	Route 53 公有託管區域應記錄 DNS 查詢	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
S3.1	S3 一般用途儲存貯體應啟用封鎖公開存取設定	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v3.2.1、PCI DSS v4.0.1	中	⊗ 否	定期
S3.2	S3 一般用途儲存貯體應封鎖公開讀取存取	AWS 基礎安全最佳實務，PCI DSS 3.2.1 版，NIST SP 800-53 修訂版 5	關鍵	⊗ 否	變更已觸發和定期
S3.3	S3 一般用途儲存貯體應封鎖公有寫入存取	AWS 基礎安全最佳實務，PCI DSS 3.2.1 版，NIST SP 800-53 修訂版 5	關鍵	⊗ 否	變更已觸發和定期

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
S3.5	S3 一般用途儲存貯體應要求請求使用 SSL	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、NIST SP 800-171 Rev. 2、PCI DSS v3.2.1、PCI DSS v4.0.1	中	⊗ 否	變更已觸發
S3.6	S3 一般用途儲存貯體政策應限制對其他的存取 AWS 帳戶	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2	HIGH (高)	⊗ 否	變更已觸發
S3.7	S3 一般用途儲存貯體應使用跨區域複寫	PCI DSS v3.2.1、NIST SP 800-53 修訂版 5	低	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
S3.8	S3 一般用途儲存貯體應封鎖公開存取	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、AWS Foundational Security Best Practices、NIST SP 800-53 Rev. 5、PCI DSS v4.0.1	HIGH (高)	⊗ 否	變更已觸發
S3.9	S3 一般用途儲存貯體應啟用伺服器存取記錄	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發
S3.10	已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態	NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
S3.11	S3 一般用途儲存貯體應啟用事件通知	NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2	中	☑ 是	變更已觸發
S3.12	ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
S3.13	S3 一般用途儲存貯體應具有生命週期組態	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	低	☑ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
S3.14	S3 一般用途儲存貯體應該已啟用版本控制	NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2	低	⊗ 否	變更已觸發
S3.15	S3 一般用途儲存貯體應該已啟用物件鎖定	NIST SP 800-53 修訂版 5，PCI DSS 4.0.1 版	中	✔ 是	變更已觸發
S3.17	S3 一般用途儲存貯體應使用 靜態加密 AWS KMS keys	NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2、PCI DSS 4.0.1	中	⊗ 否	變更已觸發
S3.19	S3 存取點應該啟用封鎖公開存取設定	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	關鍵	⊗ 否	變更已觸發
S3.20	S3 一般用途儲存貯體應啟用 MFA 刪除	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、CIS AWS Foundations Benchmark v1.4.0、NIST SP 800-53 Rev. 5	低	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
S3.22	S3 一般用途儲存貯體應記錄物件層級寫入事件	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、PCI DSS v4.0.1	中	⊗ 否	定期
S3.23	S3 一般用途儲存貯體應記錄物件層級讀取事件	CIS AWS Foundations Benchmark v5.0.0、CIS AWS Foundations Benchmark v3.0.0、PCI DSS v4.0.1	中	⊗ 否	定期
S3.24	S3 多區域存取點應啟用封鎖公開存取設定	AWS 基礎安全最佳實務，PCI DSS v4.0.1	HIGH (高)	⊗ 否	變更已觸發
S3.25	S3 目錄儲存貯體應該具有生命週期組態	AWS 基礎安全最佳實務	低	✔ 是	變更已觸發
SageMaker .1	Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 3.2.1 版，PCI DSS 4.0.1 版	HIGH (高)	⊗ 否	定期
SageMaker .2	SageMaker 筆記本執行個體應該在自訂 VPC 中啟動	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	變更已觸發
SageMaker .3	使用者不應擁有 SageMaker 筆記本執行個體的根存取權	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	HIGH (高)	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
SageMaker .4	SageMaker 端點生產變體的初始執行個體計數應大於 1	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	否	定期
SageMaker .5	SageMaker 模型應該啟用網路隔離	AWS 基礎安全最佳實務	中	否	變更已觸發
SageMaker .6	SageMaker 應用程式映像組態應加上標籤	AWS 資源標記標準	低	是	變更已觸發
SageMaker .7	SageMaker 映像應加上標籤	AWS 資源標記標準	低	是	變更已觸發
SageMaker .8	SageMaker 筆記本執行個體應在支援的平台上執行	AWS 基礎安全最佳實務	中	否	定期
SageMaker .9	SageMaker 資料品質任務定義應該啟用容器間流量加密	AWS 基礎安全最佳實務 1.0.0 版	中	否	變更已觸發
SageMaker .10	SageMaker 模型可解釋性任務定義應該啟用容器間流量加密	AWS 基礎安全最佳實務 1.0.0 版	中	否	變更已觸發
SageMaker .11	SageMaker 資料品質任務定義應該啟用網路隔離	AWS 基礎安全最佳實務 1.0.0 版	中	否	變更已觸發
SageMaker .12	SageMaker 模型偏差任務定義應該啟用網路隔離	AWS 基礎安全最佳實務 1.0.0 版	中	否	變更已觸發
SageMaker .13	SageMaker 模型品質任務定義應該啟用容器間流量加密	AWS 基礎安全最佳實務 1.0.0 版	中	否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
SageMaker .14	SageMaker 監控排程應該啟用網路隔離	AWS 基礎安全最佳實務 1.0.0 版	中	⊗ 否	變更已觸發
SageMaker .15	SageMaker 模型偏差任務定義應該啟用容器間流量加密	AWS 基礎安全最佳實務 1.0.0 版	中	⊗ 否	變更已觸發
SageMaker .16	SageMaker 模型應該在 VPC 中針對主要容器使用私有登錄檔	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
SageMaker .17	SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
SageMaker .18	使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密	NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
SageMaker .19	SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
SecretsManager.1	Secrets Manager 秘密應該啟用自動輪換	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	✔ 是	變更已觸發
SecretsManager.2	設定自動輪換的 Secrets Manager 秘密應能成功輪換	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
SecretsManager.3	移除未使用的 Secrets Manager 秘密	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	✔ 是	定期
SecretsManager.4	Secrets Manager 秘密應在指定的天數內輪換	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	✔ 是	定期
SecretsManager.5	Secrets Manager 秘密應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
ServiceCatalog.1	Service Catalog 產品組合應僅在 AWS 組織內共用	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	✘ 否	定期
SES.1	SES 聯絡人清單應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
SES.2	SES 組態集應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
SES.3	SES 組態集應啟用 TLS 以傳送電子郵件	AWS 基礎安全最佳實務	中	✘ 否	變更已觸發
SNS.1	SNS 主題應使用 靜態加密 AWS KMS	NIST SP 800-53 修訂版 5，NIST SP 800-171 修訂版 2	中	✘ 否	變更已觸發
SNS.3	SNS 主題應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
SNS.4	SNS 主題存取政策不應允許公開存取	AWS 基礎安全最佳實務	關鍵	✘ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
SQS.1	Amazon SQS 佇列應靜態加密	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
SQS.2	SQS 佇列應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
SQS.3	SQS 佇列存取政策不應允許公開存取	AWS 基礎安全最佳實務	關鍵	⊗ 否	變更已觸發
SSM.1	EC2 執行個體應該由管理 AWS Systems Manager	AWS 基礎安全最佳實務 1.0.0 版、PCI DSS 3.2.1 版、NIST SP 800-53 第 5 版	中	⊗ 否	變更已觸發
SSM.2	Systems Manager 管理的 EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2、PCI DSS v3.2.1、PCI DSS v4.0.1	HIGH (高)	⊗ 否	變更已觸發
SSM.3	Systems Manager 管理的 EC2 執行個體應具有 COMPLIANT 的關聯合規狀態	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、PCI DSS v3.2.1、PCI DSS v4.0.1	低	⊗ 否	變更已觸發
SSM.4	SSM 文件不應公開	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	關鍵	⊗ 否	定期
SSM.5	SSM 文件應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
SSM.6	SSM Automation 應該啟用 CloudWatch 記錄	AWS 基礎安全最佳實務 1.0.0 版	中	⊗ 否	定期
SSM.7	SSM 文件應該啟用封鎖公開共用設定	AWS 基礎安全最佳實務 1.0.0 版	關鍵	⊗ 否	定期
StepFunctions.1	Step Functions 狀態機器應該已開啟記錄	AWS 基礎安全最佳實務 1.0.0 版、PCI DSS 4.0.1 版	中	✔ 是	變更已觸發
StepFunctions.2	應標記 Step Functions 活動	AWS 資源標記標準	低	✔ 是	變更已觸發
Transfer.1	Transfer Family 工作流程應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Transfer.2	Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	⊗ 否	定期
Transfer.3	Transfer Family 連接器應該已啟用記錄	AWS 基礎安全最佳實務，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
Transfer.4	Transfer Family 協議應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Transfer.5	Transfer Family 憑證應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
Transfer.6	Transfer Family 連接器應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
Transfer.7	Transfer 系列設定檔應加上標籤	AWS 資源標記標準	低	✔ 是	變更已觸發
WAF.1	AWS 應啟用 WAF Classic Global Web ACL 記錄	AWS 基礎安全最佳實務，NIST SP 800-53 第 5 版，PCI DSS 4.0.1 版	中	✘ 否	定期
WAF.2	AWS WAF Classic Regional 規則應至少有一個條件	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
WAF.3	AWS WAF Classic Regional 規則群組應至少有一個規則	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
WAF.4	AWS WAF Classic Regional Web ACLs 應該至少有一個規則或規則群組	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
WAF.6	AWS WAF Classic 全域規則應至少有一個條件	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
WAF.7	AWS WAF Classic 全域規則群組應至少有一個規則	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發
WAF.8	AWS WAF Classic 全域 Web ACLs 應至少有一個規則或規則群組	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	✘ 否	變更已觸發

安全控制 ID	安全控制標題	適用標準	嚴重性	支援自訂參數	排程類型
WAF.10	AWS WAF Web ACLs 應該至少有一個規則或規則群組	AWS 基礎安全最佳實務 1.0.0 版，NIST SP 800-53 修訂版 5	中	⊗ 否	變更已觸發
WAF.11	AWS 應啟用 WAF Web ACL 記錄	NIST SP 800-53 修訂版 5，PCI DSS 4.0.1 版	低	⊗ 否	定期
WAF.12	AWS WAF 規則應該啟用 CloudWatch 指標	AWS 基礎安全最佳實務 v1.0.0、NIST SP 800-53 修訂版 5、NIST SP 800-171 修訂版 2	中	⊗ 否	變更已觸發
Workspace s.1	WorkSpaces 使用者磁碟區應靜態加密	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發
Workspace s.2	WorkSpaces 根磁碟區應靜態加密	AWS 基礎安全最佳實務	中	⊗ 否	變更已觸發

Security Hub CSPM 控制項的變更日誌

下列變更日誌會追蹤現有 AWS Security Hub CSPM 控制項的重大變更，這可能會導致控制項的整體狀態及其調查結果的合規狀態發生變更。如需 Security Hub CSPM 如何評估控制狀態的資訊，請參閱 [評估合規狀態和控制狀態](#)。變更在此日誌中的項目後可能需要幾天的時間，才能影響所有可用的 AWS 區域控制項。

此日誌會追蹤 2023 年 4 月以來發生的變更。選擇控制項來檢閱其其他詳細資訊。標題變更會在控制項的詳細說明中記下 90 天。

變更日期	控制項 ID 和標題	變更描述
2026 年 5 月 4 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每

變更日期	控制項 ID 和標題	變更描述
		種語言中支援執行時間設定的預期值。Security Hub CSPM 現在支援 <code>ruby4.0</code> 做為參數，不再包含 <code>nodejs20.x</code> ，因為 AWS Lambda 已取代此執行時間。
2026 年 4 月 27 日	【EC2.4】已停止的 EC2 執行個體應在指定的期間之後移除	Security Hub CSPM 將此控制項的備份規則從 <code>ec2-stopped-instance</code> 變更為自訂 Security Hub CSPM 規則， <code>ec2-stopped-instance-days-check</code> ，以簡化評估邏輯。
2026 年 4 月 7 日	【EC2.1】Amazon EBS 快照不應設定為可公開還原	Security Hub CSPM 變更了此控制項的標題和描述。新的標題和描述會更準確地反映控制項會檢查 Amazon EBS 快照是否設定為可公開還原。先前，此控制項的標題為：Amazon EBS 快照不應可公開還原。

變更日期	控制項 ID 和標題	變更描述
2026 年 4 月 7 日	【EC2.182】 應為 Amazon EBS 快照啟用封鎖公開存取設定	Security Hub CSPM 變更了此控制項的標題和描述。新的標題和描述會更準確地反映控制項會檢查是否已為 Amazon EBS 快照啟用帳戶層級封鎖公開存取。先前，此控制項的標題為：不應公開存取 Amazon EBS 快照。
2026 年 4 月 6 日	【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策	Security Hub CSPM 已更新此控制項的參數值，以反映建議的安全性政策。
2026 年 4 月 3 日	【Cognito.3】 Cognito 使用者集區的密碼政策應具有強大的組態	Security Hub CSPM 擴展了此控制項之 temporary Password Validity 參數的支援值範圍。您現在可以指定介於 1-365 天之間的值。先前，範圍為 7-365 天。

變更日期	控制項 ID 和標題	變更描述
2026 年 4 月 3 日	【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行	此控制項會檢查 Amazon EKS 叢集是否在支援的 Kubernetes 版本上執行。Security Hub CSPM 將此控制項的參數值從 變更為 1.32 1.33。Amazon EKS 中 Kubernetes 1.32 版的標準支援已於 2026 年 3 月 23 日結束。
2026 年 4 月 3 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	支援執行時間的 Lambda.2 參數不再包含，ruby3.2 因為 Lambda 已取代此執行時間。
2026 年 3 月 24 日	【RDS.50】 RDS 資料庫叢集應設定足夠的備份保留期間	Security Hub CSPM 已更新控制項標題，以反映控制項會檢查所有 RDS 資料庫叢集。

變更日期	控制項 ID 和標題	變更描述
2026 年 3 月 24 日	【ECS.5】 ECS 任務定義應將容器設定為僅限對根檔案系統的唯一讀存取	Security Hub CSPM 已更新控制項標題和描述，以反映控制項檢查 ECS 任務定義。Security Hub CSPM 也更新了控制項，不為runtimePlatform 設定為指定WINDOWS_SERVER 作業系統系列的任務定義產生調查結果。
2026 年 3 月 9 日	【AppSync.1】 AWS AppSync API 快取應靜態加密	Security Hub CSPM 已淘汰此控制項，並將其從 AWS 基礎安全最佳實務 (FSBP) 標準 中移除。AWS AppSync 現在為所有目前和未來的 API 快取提供預設加密。
2026 年 3 月 9 日	【AppSync.6】 AWS AppSync API 快取應在傳輸中加密	Security Hub CSPM 已淘汰此控制項，並將其從 AWS 基礎安全最佳實務 (FSBP) 標準 中移除。AWS AppSync 現在為所有目前和未來的 API 快取提供預設加密。

變更日期	控制項 ID 和標題	變更描述
2026 年 3 月 4 日	【ECS.1】 Amazon ECS 任務定義應具有安全的聯網模式和使用使用者定義	Security Hub CSPM 已淘汰此控制項，並將其從 AWS 基礎安全最佳實務 (FSBP) 標準 和 NIST SP 800-53 修訂版 5 標準 中移除。
2026 年 2 月 5 日	【AppSync.1】 AWS AppSync API 快取應靜態加密	Security Hub CSPM 將於 2026 年 3 月 9 日淘汰此控制項，並從所有適用的 Security Hub CSPM 標準中移除。AWS AppSync 正在為所有目前和未來的 API 快取提供預設加密。
2026 年 2 月 5 日	【AppSync.6】 AWS AppSync API 快取應在傳輸中加密	Security Hub CSPM 將於 2026 年 3 月 9 日淘汰此控制項，並從所有適用的 Security Hub CSPM 標準中移除。AWS AppSync 正在為所有目前和未來的 API 快取提供預設加密。
2026 年 1 月 16 日	【ECS.1】 Amazon ECS 任務定義應具有安全的聯網模式和使用使用者定義	Security Hub CSPM 已通知 2026 年 2 月 16 日之後，將會淘汰此控制項，並從所有適用的 Security Hub CSPM 標準中移除。

變更日期	控制項 ID 和標題	變更描述
2026 年 1 月 12 日	【Redshift.4】 Amazon Redshift 叢集應該啟用稽核記錄	Security Hub CSPM 已更新此控制項以移除 loggingEnabled 參數。
2026 年 1 月 12 日	【MQ.3】 Amazon MQ 代理程式應該啟用自動次要版本升級	Security Hub CSPM 已淘汰控制項，並從所有適用標準中移除控制項。Security Hub CSPM 由於 Amazon MQ 要求自動次要版本升級而淘汰控制項。 先前，控制項適用於AWS 基礎安全最佳實務 (FSBP) 標準、NIST SP 800-53 修訂版 5 標準和 PCI DSS 4.0.1 版標準。
2026 年 1 月 12 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	此控制項會檢查 AWS Lambda 函數的執行時間設定是否符合每種語言中支援執行時間的預期值。Security Hub CSPM 現在支援 dotnet10 做為此控制項的參數值。AWS Lambda 新增對此執行時間的支援。

變更日期	控制項 ID 和標題	變更描述
2025 年 12 月 15 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	此控制項會檢查 AWS Lambda 函數的執行時間設定是否符合每種語言中支援執行時間的預期值。Security Hub CSPM 不再支援 python3.9 做為此 control 的參數值。AWS Lambda 不再支援此執行時間。
2025 年 12 月 12 日	【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行	此控制項會檢查 Amazon EKS 叢集是否在支援的 Kubernetes 版本上執行。Security Hub CSPM 將此控制項的參數值從變更為 1.31 1.32。Amazon EKS 中 Kubernetes 1.31 版的標準支援已於 2025 年 11 月 26 日結束。
2025 年 11 月 21 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	此控制項會檢查 AWS Lambda 函數的執行時間設定是否符合每種語言中支援執行時間的預期值。Security Hub CSPM 現在支援 nodejs24.x 和 python3.14 做為此控制項的參數值。AWS Lambda 已新增這些執行時間的支援。

變更日期	控制項 ID 和標題	變更描述
2025 年 11 月 14 日	【EC2.15】 Amazon EC2 子網路不應自動指派公有 IP 地址	Security Hub CSPM 已更新此控制項的描述和原理。 先前，控制項只會使用 MapPublicIpOnLaunch 旗標在 Amazon VPC 子網路中檢查 IPv4 公有 IP 自動指派。此控制項現在會檢查 IPv4 和 IPv6 公有 IP 自動指派。已更新控制項的描述和原理，以反映這些變更。
2025 年 11 月 14 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	此控制項會檢查 AWS Lambda 函數的執行時間設定是否符合每種語言中支援執行時間的預期值。Security Hub CSPM 現在支援 java25 做為此控制項的參數值。AWS Lambda 新增了對此執行時間的支援。
2025 年 11 月 13 日	【SNS.4】 SNS 主題存取政策不應允許公開存取	Security Hub CSPM 將此控制項的嚴重性從 變更為 HIGH CRITICAL。允許公開存取 Amazon SNS 主題會造成重大的安全風險。

變更日期	控制項 ID 和標題	變更描述
2025 年 11 月 13 日	【SQS.3】 SQS 佇列存取政策不應允許公開存取	Security Hub CSPM 將此控制項的嚴重性從 變更為 HIGH CRITICAL。允許公開存取 Amazon SQS 佇列會造成重大的安全風險。
2025 年 11 月 13 日	【GuardDuty.7】 應啟用 GuardDuty EKS 執行期監控	Security Hub CSPM 將此控制項的嚴重性從 變更為 MEDIUM HIGH。這種類型的執行期監控可為 Amazon EKS 資源提供增強型威脅偵測。
2025 年 11 月 13 日	【MQ.3】 Amazon MQ 代理程式應該啟用自動次要版本升級	Security Hub CSPM 將此控制項的嚴重性從 變更為 LOW MEDIUM。次要版本升級包括維護 Amazon MQ 代理程式安全性所需的安全修補程式。
2025 年 11 月 13 日	【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新	Security Hub CSPM 將此控制項的嚴重性從 變更為 LOW MEDIUM。軟體更新包括維護 OpenSearch 網域安全所需的安全修補程式。

變更日期	控制項 ID 和標題	變更描述
2025 年 11 月 13 日	【RDS.7】 RDS 叢集應該啟用刪除保護	Security Hub CSPM 將此控制項的嚴重性從 變更為 LOW MEDIUM。刪除保護有助於防止意外刪除 Amazon RDS 資料庫，以及未經授權的實體刪除 RDS 資料庫。
2025 年 11 月 13 日	【CloudTrail.5】 CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合	Security Hub CSPM 將此控制項的嚴重性從 變更為 LOW MEDIUM。Amazon CloudWatch Logs 中的 AWS CloudTrail 記錄資料可用於稽核活動、警示和其他重要的安全操作。
2025 年 11 月 13 日	【ServiceCatalog.1】 Service Catalog 產品組合只能在 AWS 組織內共用	Security Hub CSPM 將此控制項的嚴重性從 變更為 HIGH MEDIUM。與特定帳戶共用 AWS Service Catalog 產品組合可能是有意的，不一定表示產品組合可公開存取。

變更日期	控制項 ID 和標題	變更描述
2025 年 11 月 13 日	【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證	Security Hub CSPM 將此控制項的嚴重性從 變更為 MEDIUM LOW。Amazon CloudFront 分佈的預設cloudfront.net 網域名稱是隨機產生的，可降低安全風險。
2025 年 11 月 13 日	【ELB.7】 Classic Load Balancer 應啟用連線耗盡	Security Hub CSPM 將此控制項的嚴重性從 變更為 MEDIUM LOW。在多執行個體部署中，其他運作狀態良好的執行個體可以在執行個體終止時處理使用者工作階段，而不會耗盡連線，進而降低營運影響和可用性風險。
2025 年 11 月 13 日	【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱	Security Hub CSPM 已更新此控制項，以移除選用validAdminUserNames 參數。
2025 年 10 月 23 日	【ElastiCache.1】 ElastiCache (Redis OSS) 叢集應該啟用自動備份	Security Hub CSPM 已還原 2025 年 10 月 14 日對此控制項的標題、描述和規則所做的變更。

變更日期	控制項 ID 和標題	變更描述
2025 年 10 月 22 日	【CloudFront.1】CloudFront 分佈應設定預設根物件	Security Hub CSPM 已更新此控制項，而不會為使用自訂原始伺服器的 Amazon CloudFront 分佈產生問題清單。
2025 年 10 月 16 日	【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策	此控制項會檢查 Amazon CloudFront 分佈是否設定為使用建議的 TLS 安全政策。Security Hub CSPM 現在支援 TLSv1.2_2025 和 TLSv1.3_2025 做為此控制項的參數值。

變更日期	控制項 ID 和標題	變更描述
2025 年 10 月 14 日	【ElastiCache.1】ElastiCache (Redis OSS) 叢集應該啟用自動備份	Security Hub CSPM 已變更此控制項的標題、描述和規則。 先前，控制項會使用 elasticache-redis-cluster-automatic-backup-check 規則檢查 Redis OSS 叢集和所有複寫群組。控制項的標題為：ElastiCache (Redis OSS) 叢集應該啟用自動備份。 除了 Redis OSS 叢集和所有複寫群組之外，此控制項現在會使用已啟用 elasticache-automatic-backup-check-enabled 規則來檢查 Valkey 叢集。新的標題和描述反映控制項會檢查這兩種類型的叢集。

變更日期	控制項 ID 和標題	變更描述
2025 年 10 月 5 日	【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新	如果 Amazon OpenSearch Service 網域沒有可用的軟體更新，且更新狀態不符合資格，則此控制項的規則已更新，也會產生PASSED問題清單。先前，只有在 OpenSearch 網域沒有可用的軟體更新且更新狀態完成時，此控制項才會產生PASSED調查結果。
2025 年 9 月 24 日	【Redshift.9】 Redshift 叢集不應使用預設資料庫名稱 【RedshiftServerless.7】 Redshift Serverless 命名空間不應使用預設資料庫名稱	Security Hub CSPM 已淘汰這些控制項，並將其從所有適用標準中移除。Security Hub CSPM 已淘汰這些控制項，因為 Amazon Redshift 固有限制導致無法有效修復控制項的問題 FAILED清單。 先前，適用於AWS 基礎安全最佳實務 (FSBP) 標準和NIST SP 800-53 修訂版 5 標準的控制項。Redshift.9 控制項也套用至AWS Control Tower 服務受管標準。

變更日期	控制項 ID 和標題	變更描述
2025 年 9 月 9 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	此控制項會檢查 AWS Lambda 函數的執行時間設定是否符合每種語言中支援執行時間的預期值。Security Hub CSPM 不再支援 nodejs18.x 做為此控制項的參數值。AWS Lambda 不再支援 Node.js 18 執行時間。
2025 年 8 月 13 日	【SageMaker.5】 SageMaker 模型應該啟用網路隔離	Security Hub CSPM 變更了此控制項的標題和描述。新的標題和描述更準確地反映控制項會檢查 Amazon SageMaker AI 託管模型EnableNetworkIsolation 參數的設定。先前，此控制項的標題為：SageMaker models should block inbound traffic。

變更日期	控制項 ID 和標題	變更描述
2025 年 8 月 13 日	【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯	Security Hub CSPM 變更了此控制項的標題和描述。新的標題和描述更精確地反映控制項執行之檢查的範圍和性質。先前，此控制項的標題為：EFS mount targets should not be associated with a public subnet。
2025 年 7 月 24 日	【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行	此控制項會檢查 Amazon EKS 叢集是否在支援的 Kubernetes 版本上執行。Security Hub CSPM 將此控制項的參數值從 變更為 1.30 1.31。Amazon EKS 中 Kubernetes 1.30 版的標準支援已於 2025 年 7 月 23 日結束。

變更日期	控制項 ID 和標題	變更描述
2025 年 7 月 23 日	【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密	Security Hub CSPM 已變更此控制項的標題。新標題更準確地反映控制項只會檢查指定啟動參數的 Amazon EC2 Spot Fleet 請求。先前，此控制項的標題為：EC2 Spot Fleet requests should enable encryption for attached EBS volumes。
2025 年 6 月 30 日	【IAM.13】 確保 IAM 密碼政策至少需要一個符號	Security Hub CSPM 從 PCI DSS v4.0.1 標準 中移除此控制項。PCI DSS 4.0.1 版並未明確要求在密碼中使用符號。
2025 年 6 月 30 日	【IAM.17】 確保 IAM 密碼政策在 90 天內過期密碼	Security Hub CSPM 從 NIST SP 800-171 修訂版 2 標準 中移除此控制項。NIST SP 800-171 修訂版 2 未明確要求密碼過期期間為 90 天或更少。

變更日期	控制項 ID 和標題	變更描述
2025 年 6 月 30 日	【RDS.16】 Aurora 資料庫叢集應設定為將標籤複製到資料庫快照	Security Hub CSPM 已變更此控制項的標題。新標題更準確地反映控制項只會檢查 Amazon Aurora 資料庫叢集。先前，此控制項的標題為：RDS DB clusters should be configured to copy tags to snapshots。
2025 年 6 月 30 日	【SageMaker.8】 SageMaker 筆記本執行個體應在支援的平台上執行	此控制項會根據筆記本執行個體指定的平台識別符，檢查 Amazon SageMaker AI 筆記本執行個體是否設定為在支援的平台上執行。Security Hub CSPM 不再支援 notebook-a12-v1 和 notebook-a12-v2 做為此控制項的參數值。在這些平台上執行的筆記本執行個體已於 2025 年 6 月 30 日終止支援。

變更日期	控制項 ID 和標題	變更描述
2025 年 5 月 30 日	【IAM.10】 IAM 使用者的密碼政策應具有強大的組態	Security Hub CSPM 從 PCI DSS v4.0.1 標準 中移除此控制項。此控制項會檢查 IAM 使用者的帳戶密碼政策是否符合最低要求，包括至少 7 個字元的密碼長度。PCI DSS v4.0.1 現在需要密碼至少 8 個字元。控制項會繼續套用至具有不同密碼要求的 PCI DSS v3.2.1 標準。 若要根據 PCI DSS v4.0.1 要求評估帳戶密碼政策，您可以使用 IAM.7 控制項。此控制項需要密碼至少 8 個字元。它也支援密碼長度和其他參數的自訂值。IAM.7 控制項是 Security Hub CSPM 中 PCI DSS v4.0.1 標準的一部分。
2025 年 5 月 8 日	【RDS.46】 RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中	Security Hub CSPM 完全復原了 RDS.46 控制項的版本。AWS 區域先前，此控制項支援 AWS 基礎安全最佳實務 (FSBP) 標準。

變更日期	控制項 ID 和標題	變更描述
2025 年 4 月 7 日	【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策	此控制項會檢查 Application Load Balancer 的 HTTPS 接聽程式或 Network Load Balancer 的 TLS 接聽程式是否設定為使用建議的安全政策來加密傳輸中的資料。Security Hub CSPM 現在支援此控制項的兩個額外參數值：ELBSecurityPolicy-TLS13-1-2-Res-2021-06 和 ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04。
2025 年 3 月 27 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	此控制項會檢查 AWS Lambda 函數的執行時間設定是否符合每種語言中支援執行時間的預期值。Security Hub CSPM 現在支援 ruby3.4 做為此控制項的參數值。AWS Lambda 新增對此執行時間的支援。

變更日期	控制項 ID 和標題	變更描述
2025 年 3 月 26 日	【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行	此控制項會檢查 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集是否在支援的 Kubernetes 版本上執行。針對 <code>oldestVersionSupported</code> 參數，Security Hub CSPM 會將值從 變更 為 1.29 1.30。最舊支援的 Kubernetes 版本現在為 1.30。
2025 年 3 月 10 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	此控制項會檢查 AWS Lambda 函數的執行時間設定是否符合每種語言中支援執行時間的預期值。Security Hub CSPM 不再支援 dotnet6 和 python3.8 做為此 control 的參數值。AWS Lambda 不再支援這些執行時間。

變更日期	控制項 ID 和標題	變更描述
2025 年 3 月 7 日	【RDS.18】 RDS 執行個體應部署在 VPC 中	Security Hub CSPM 已從 AWS 基礎安全最佳實務標準移除此控制項，並自動檢查 NIST SP 800-53 修訂版 5 要求。由於 Amazon EC2-Class ic 網路已淘汰，因此 Amazon Relationa l Database Service (Amazon RDS) 執行個體無法再部署在 VPC 外部。控制項會繼續成為 AWS Control Tower 服務受管標準 的一部分。
2025 年 1 月 10 日	【Glue.2】 AWS Glue 任務應該已啟用記錄	Security Hub CSPM 已淘汰此控制項，並將其從所有標準中移除。
2024 年 12 月 20 日	EC2.61 到 EC2.169	Security Hub CSPM 透過 EC2.169 控制項復原 EC2.61 的版本。

變更日期	控制項 ID 和標題	變更描述
2024 年 12 月 12 日	【RDS.23】 RDS 執行個體不應使用資料庫引擎預設連接埠	RDS.23 會檢查 Amazon Relational Database Service (Amazon RDS) 叢集或執行個體是否使用資料庫引擎預設連接埠以外的連接埠。我們更新控制項，讓基礎 AWS Config 規則 NOT_APPLICABLE 針對屬於叢集的 RDS 執行個體傳回的結果。
2024 年 12 月 2 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 現在支援 nodejs22.x 做為參數。
2024 年 11 月 26 日	【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行	此控制項會檢查 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集是否在支援的 Kubernetes 版本上執行。最舊支援的版本現在是 1.29。

變更日期	控制項 ID 和標題	變更描述
2024 年 11 月 20 日	【Config.1】 AWS Config 應啟用並使用服務連結角色進行資源記錄	Config.1 會檢查 AWS Config 是否已啟用、是否使用服務連結角色，以及記錄已啟用控制項的資源。Security Hub CSPM 將此控制項的嚴重性從 提高MEDIUM為 CRITICAL。Security Hub CSPM 也為失敗的 Config.1 問題清單新增了新的狀態碼和狀態原因。這些變更反映 Config.1 對 Security Hub CSPM 控制項操作的重要性。如果您已停用 AWS Config 或 資源錄製，則可能會收到不正確的控制問題清單。 若要接收 Config.1 的問題PASSED清單，請開啟對應至已啟用 Security Hub CSPM 控制項之資源的資源記錄，並停用組織中不需要的控制項。如需 AWS Config 設定 Security Hub CSPM 的說明，請參閱 啟用和設定 AWS Config Security Hub CSPM。如需 Security Hub CSPM 控制項及其對

變更日期	控制項 ID 和標題	變更描述
		應資源的清單，請參閱 控制問題清單所需的 AWS Config 資源 。
2024 年 11 月 12 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 現在支援 python3.13 做為參數。
2024 年 10 月 11 日	ElastiCache 控制項	已變更 ElastiCache.3, ElastiCache.4, ElastiCache.5, 和 ElastiCache.7. 標題不再提及 Redis OSS，因為控制項也適用於 ElastiCache for Valkey。
2024 年 9 月 27 日	【ELB.4】 Application Load Balancer 應設定為捨棄無效的 http 標頭	從 Application Load Balancer 變更的控制標題應設定為捨棄 http 標頭至 Application Load Balancer 應設定為捨棄無效的 http 標頭。

變更日期	控制項 ID 和標題	變更描述
2024 年 8 月 19 日	DMS.12 和 ElastiCache 控制項的標題變更	透過 ElastiCache.7 變更 DMS.12 和 ElastiCache.1 ElastiCache.7. 我們變更了這些標題，以反映 Amazon ElastiCache (Redis OSS) 服務中的名稱變更。
2024 年 8 月 15 日	【Config.1】AWS Config 應啟用並使用服務連結角色進行資源記錄	Config.1 會檢查 AWS Config 是否已啟用、是否使用服務連結角色，以及記錄已啟用控制項的資源。Security Hub CSPM 新增了名為的自訂控制參數includeConfigServiceLinkedRoleCheck。透過將此參數設定為false，您可以選擇不檢查是否 AWS Config 使用服務連結角色。
2024 年 7 月 31 日	【IoT.1】AWS IoT Device Defender 安全設定檔應加上標籤	從AWS IoT Core 安全性描述檔變更的控制標題應標記為AWS IoT Device Defender 安全性描述檔應標記。

變更日期	控制項 ID 和標題	變更描述
2024 年 7 月 29 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 不再支援 nodejs16.x 做為參數。
2024 年 7 月 29 日	【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行	此控制項會檢查 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集是否在支援的 Kubernetes 版本上執行。最舊支援的版本是 1.28。
2024 年 6 月 25 日	【Config.1】 AWS Config 應啟用並使用服務連結角色進行資源記錄	此控制項會檢查 AWS Config 是否已啟用、是否使用服務連結角色，以及記錄已啟用控制項的資源。Security Hub CSPM 已更新控制項標題，以反映控制項評估的內容。

變更日期	控制項 ID 和標題	變更描述
2024 年 6 月 14 日	【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs	此控制項會檢查 Amazon Aurora MySQL 資料庫叢集是否已設定為將稽核日誌發佈至 Amazon CloudWatch Logs。Security Hub CSPM 已更新控制項，因此不會產生 Aurora Serverless v1 資料庫叢集的問題清單。
2024 年 6 月 11 日	【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行	此控制項會檢查 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集是否在支援的 Kubernetes 版本上執行。最舊支援的版本為 1.27。

變更日期	控制項 ID 和標題	變更描述
2024 年 6 月 10 日	【Config.1】 AWS Config 應啟用並使用服務連結角色進行資源記錄	此控制項會檢查 AWS Config 是否已啟用，以及是否開啟 AWS Config 資源記錄。先前，只有在您為所有資源設定記錄時，控制項才會產生 PASSED 調查結果。Security Hub CSPM 已更新控制項，以在啟用控制項所需的資源開啟記錄時產生 PASSED 問題清單。控制項也已更新，以檢查是否使用 AWS Config 服務連結角色，這可提供記錄必要資源的許可。

變更日期	控制項 ID 和標題	變更描述
2024 年 5 月 8 日	【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除	此控制項會檢查 Amazon S3 一般用途版本控制的儲存貯體是否已啟用多重要素驗證 (MFA) 刪除。在過去，控制項會針對具有生命週期組態的儲存貯體產生 FAILED 問題清單。不過，無法在具有生命週期組態的儲存貯體上啟用具有版本控制的 MFA 刪除。Security Hub CSPM 已更新控制項，對具有生命週期組態的儲存貯體不會產生問題清單。控制項描述已更新，以反映目前的行為。
2024 年 5 月 2 日	【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行	Security Hub CSPM 更新了 Amazon EKS 叢集可執行的最舊支援 Kubernetes 版本，以產生傳遞的問題清單。目前最舊支援的版本是 Kubernetes 1.26。

變更日期	控制項 ID 和標題	變更描述
2024 年 4 月 30 日	【CloudTrail.3】至少應啟用一個 CloudTrail 追蹤	應將 CloudTrail 的控制標題變更為至少應啟用一個 CloudTrail 追蹤。如果 AWS 帳戶至少已啟用一個 CloudTrail 追蹤，則此控制項目前會產生 PASSED 問題清單。已變更標題和描述，以準確反映目前的行為。
2024 年 4 月 29 日	【AutoScaling.1】與負載平衡器相關聯的 Auto Scaling 群組應使用 ELB 運作狀態檢查	與 Classic Load Balancer 相關聯的 Auto Scaling 群組變更控制標題應使用負載平衡器運作狀態檢查，而與負載平衡器相關聯的 Auto Scaling 群組應使用 ELB 運作狀態檢查。此控制項目前評估 Application、Gateway、Network 和 Classic Load Balancer。已變更標題和描述，以準確反映目前的行為。

變更日期	控制項 ID 和標題	變更描述
2024 年 4 月 19 日	【CloudTrail.1】CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤	控制項會檢查 AWS CloudTrail 是否已啟用並設定至少一個包含讀取和寫入管理事件的多區域線索。在過去，當帳戶已啟用 CloudTrail 並設定至少一個多區域追蹤時，即使沒有追蹤擷取讀取和寫入管理事件，控制項也會錯誤地產生PASSED調查結果。控制項現在只會在啟用 CloudTrail 並設定至少一個擷取讀取和寫入管理事件的多區域線索時產生PASSED調查結果。
2024 年 4 月 10 日	【Athena.1】 Athena 工作群組應靜態加密	Security Hub CSPM 已淘汰此控制項，並將其從所有標準中移除。Athena 工作群組會將日誌傳送至 Amazon Simple Storage Service (Amazon S3) 儲存貯體。Amazon S3 現在可在新的和現有的 S3 儲存貯體上使用 S3 受管金鑰 (SS3-S3) 提供預設加密。

變更日期	控制項 ID 和標題	變更描述
2024 年 4 月 10 日	【AutoScaling.4】Auto Scaling 群組啟動組態的中繼資料回應跳轉限制不應大於 1	Security Hub CSPM 已淘汰此控制項，並將其從所有標準中移除。Amazon Elastic Compute Cloud (Amazon EC2) 執行個體的中繼資料回應跳轉限制取決於工作負載。
2024 年 4 月 10 日	【CloudFormation.1】CloudFormation 堆疊應與 Simple Notification Service (SNS) 整合	Security Hub CSPM 已淘汰此控制項，並將其從所有標準中移除。將 AWS CloudFormation 堆疊與 Amazon SNS 主題整合不再是安全最佳實務。雖然整合重要的 CloudFormation 堆疊與 SNS 主題可能很有用，但並非所有堆疊都需要。
2024 年 4 月 10 日	【CodeBuild.5】CodeBuild 專案環境不應啟用特權模式	Security Hub CSPM 已淘汰此控制項，並將其從所有標準中移除。在 CodeBuild 專案中啟用特權模式不會對客戶環境造成額外的風險。

變更日期	控制項 ID 和標題	變更描述
2024 年 4 月 10 日	【IAM.20】 避免使用根使用者	Security Hub CSPM 已淘汰此控制項，並將其從所有標準中移除。此控制項的目的涵蓋於另一個控制項 【CloudWatch.1】 應該存在日誌指標篩選條件和警示以使用「根」使用者。
2024 年 4 月 10 日	【SNS.2】 應針對傳送至主題的通知訊息啟用傳遞狀態記錄	Security Hub CSPM 已淘汰此控制項，並將其從所有標準中移除。記錄 SNS 主題的交付狀態不再是安全最佳實務。雖然重要 SNS 主題的記錄傳遞狀態可能很有用，但並非所有主題都需要這樣做。

變更日期	控制項 ID 和標題	變更描述
2024 年 4 月 10 日	【S3.10】 已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態	Security Hub CSPM 已從 AWS 基礎安全最佳實務和服務受管標準中移除此控制項：AWS Control Tower。此控制項的目的涵蓋於另外兩個控制項： 【S3.13】 S3 一般用途儲存貯體應該具有生命週期組態 和 【S3.14】 S3 一般用途儲存貯體應該已啟用版本控制 。此控制項仍然是 NIST SP 800-53 修訂版 5 的一部分。
2024 年 4 月 10 日	【S3.11】 S3 一般用途儲存貯體應啟用事件通知	Security Hub CSPM 已從 AWS 基礎安全最佳實務和服務受管標準中移除此控制項：AWS Control Tower。雖然在某些情況下 S3 儲存貯體的事件通知很有用，但這不是通用的安全最佳實務。此控制項仍然是 NIST SP 800-53 修訂版 5 的一部分。

變更日期	控制項 ID 和標題	變更描述
2024 年 4 月 10 日	【SNS.1】 SNS 主題應使用 進行靜態加密 AWS KMS	Security Hub CSPM 已從 AWS 基礎安全最佳實務和服務受管標準中移除此控制項：AWS Control Tower。根據預設，SNS 會使用磁碟加密來加密靜態主題。如需詳細資訊，請參閱 資料加密 。不再建議使用 AWS KMS 加密主題做為安全最佳實務。此控制項仍然是 NIST SP 800-53 修訂版 5 的一部分。
2024 年 4 月 8 日	【ELB.6】 應用程式、閘道和 Network Load Balancer 應啟用刪除保護	從 Application Load Balancer 刪除保護變更的控制標題應啟用至 Application、Gateway 和 Network Load Balancer 應啟用刪除保護。此控制項目前評估 Application、Gateway 和 Network Load Balancer。已變更標題和描述，以準確反映目前的行為。

變更日期	控制項 ID 和標題	變更描述
2024 年 3 月 22 日	【Opensearch.8】應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線	從連線至 OpenSearch 網域變更的控制標題應使用 TLS 1.2 加密為連線至 OpenSearch 網域，應使用最新的 TLS 安全政策加密。先前，控制項只會檢查 OpenSearch 網域的連線是否使用 TLS 1.2。如果使用最新的 TLS 安全政策加密 OpenSearch 網域，控制項現在會產生 PASSED 問題清單。控制項標題和描述已更新，以反映目前的行為。

變更日期	控制項 ID 和標題	變更描述
2024 年 3 月 22 日	【ES.8】 應使用最新的 TLS 安全政策加密與 Elasticsearch 網域的連線	從連線至 Elasticsearch 網域變更的控制標題應使用 TLS 1.2 加密為連線至 Elasticsearch 網域，應使用最新的 TLS 安全政策加密。先前，控制項只會檢查與 Elasticsearch 網域的連線是否使用 TLS 1.2。如果使用最新的 TLS 安全政策加密 Elasticsearch 網域，控制項現在會產生問題 PASSED 清單。控制項標題和描述已更新，以反映目前的行為。
2024 年 3 月 12 日	【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定	從 S3 封鎖公開存取設定變更為 S3 一般用途儲存貯體的標題應該啟用封鎖公開存取設定。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。

變更日期	控制項 ID 和標題	變更描述
2024 年 3 月 12 日	【S3.2】 S3 一般用途儲存貯體應封鎖公開讀取存取	從 S3 儲存貯體變更標題應禁止公開讀取存取 S3 一般用途儲存貯體應封鎖公開讀取存取。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。
2024 年 3 月 12 日	【S3.3】 S3 一般用途儲存貯體應封鎖公有寫入存取	從 S3 儲存貯體變更的標題應禁止公開寫入存取 S3 一般用途儲存貯體應封鎖公開寫入存取。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。
2024 年 3 月 12 日	【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL	從 S3 儲存貯體變更的標題應要求請求使用 Secure Socket Layer 到 S3 一般用途儲存貯體應要求請求使用 SSL。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。

變更日期	控制項 ID 和標題	變更描述
2024 年 3 月 12 日	【S3.6】 S3 一般用途儲存貯體政策應限制對其他的存取 AWS 帳戶	從授予其他儲存貯體政策 AWS 帳戶 中其他的 S3 許可變更的標題，應限制為 S3 一般用途儲存貯體政策應限制對其他的存取 AWS 帳戶。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。
2024 年 3 月 12 日	【S3.7】 S3 一般用途儲存貯體應使用跨區域複寫	從 S3 儲存貯體變更的標題應啟用跨區域複寫至 S3 一般用途儲存貯體應使用跨區域複寫。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。
2024 年 3 月 12 日	【S3.7】 S3 一般用途儲存貯體應使用跨區域複寫	從 S3 儲存貯體變更的標題應啟用跨區域複寫至 S3 一般用途儲存貯體應使用跨區域複寫。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。

變更日期	控制項 ID 和標題	變更描述
2024 年 3 月 12 日	【S3.8】 S3 一般用途儲存貯體應封鎖公開存取	應該在儲存貯體層級將 S3 封鎖公開存取設定的標題變更為 S3 一般用途儲存貯體應該封鎖公開存取。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。
2024 年 3 月 12 日	【S3.9】 S3 一般用途儲存貯體應啟用伺服器存取記錄	應將 S3 儲存貯體伺服器存取記錄的變更標題啟用至 S3 一般用途儲存貯體的伺服器存取記錄。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。
2024 年 3 月 12 日	【S3.10】 已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態	從已啟用版本控制的 S3 儲存貯體變更的標題，應該將生命週期政策設定為已啟用版本控制的 S3 一般用途儲存貯體，應該具有生命週期組態。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。

變更日期	控制項 ID 和標題	變更描述
2024 年 3 月 12 日	【S3.11】 S3 一般用途儲存貯體應啟用事件通知	從 S3 儲存貯體變更的標題應啟用 S3 一般用途儲存貯體的事件通知應啟用事件通知S3。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。
2024 年 3 月 12 日	【S3.12】 ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取	從 S3 存取控制清單 (ACLs) 變更的標題不應用於管理使用者對 ACL 的存取，不應用於管理使用者對 S3 一般用途儲存貯體的存取 ACLs。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。
2024 年 3 月 12 日	【S3.13】 S3 一般用途儲存貯體應具有生命週期組態	從 S3 儲存貯體變更的標題應該將生命週期政策設定為 S3 一般用途儲存貯體應該具有生命週期組態。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。

變更日期	控制項 ID 和標題	變更描述
2024 年 3 月 12 日	【S3.14】 S3 一般用途儲存貯體應該已啟用版本控制	從 S3 儲存貯體變更的標題應該使用版本控制到 S3 一般用途儲存貯體應該已啟用版本控制。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。
2024 年 3 月 12 日	【S3.15】 S3 一般用途儲存貯體應啟用物件鎖定	從 S3 儲存貯體變更的標題應設定為使用物件鎖定至 S3 一般用途儲存貯體時，應啟用物件鎖定。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。
2024 年 3 月 12 日	【S3.17】 S3 一般用途儲存貯體應使用 靜態加密 AWS KMS keys	從 S3 儲存貯體變更的標題應使用 靜態加密 AWS KMS keys 為 S3 一般用途儲存貯體應使用 靜態加密 AWS KMS keys。Security Hub CSPM 已將標題變更為考量新的 S3 儲存貯體類型。

變更日期	控制項 ID 和標題	變更描述
2024 年 3 月 7 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 現在支援 nodejs20.x 和 ruby3.3 做為參數。
2024 年 2 月 22 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 現在支援 dotnet8 做為參數。
2024 年 2 月 5 日	【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行	Security Hub CSPM 更新了 Amazon EKS 叢集可執行的最舊支援 Kubernetes 版本，以產生傳遞的問題清單。目前最舊支援的版本是 Kubernetes 1.25。

變更日期	控制項 ID 和標題	變更描述
2024 年 1 月 10 日	【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料	從 CodeBuild GitHub 或 Bitbucket 來源儲存庫 URLs 變更的標題應使用 OAuth 至 CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感憑證。Security Hub CSPM 已移除提及 OAuth，因為其他連線方法也可能是安全的。Security Hub CSPM 已移除提及 GitHub，因為在 GitHub 來源儲存庫 URLs 中無法再擁有個人存取字符或使用者名稱和密碼。
2024 年 1 月 8 日	【Lambda.2】Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 不再支援 go1.x 和 java8 做為參數，因為這些是淘汰的執行時間。

變更日期	控制項 ID 和標題	變更描述
2023 年 12 月 29 日	【RDS.8】 RDS 資料庫執行個體應啟用刪除保護	RDS.8 會檢查使用其中一個受支援資料庫引擎的 Amazon RDS 資料庫執行個體是否已啟用刪除保護。Security Hub CSPM 現在支援 custom-oracle-ee、oracle-ee-cdb 和 oracle-se2-cdb 做為資料庫引擎。
2023 年 12 月 22 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 現在支援 java21 和 python3.12 做為參數。Security Hub CSPM 不再支援 ruby2.7 做為參數。
2023 年 12 月 15 日	【CloudFront.1】 CloudFront 分佈應設定預設根物件	CloudFront.1 會檢查 Amazon CloudFront 分佈是否已設定預設根物件。Security Hub CSPM 將此控制項的嚴重性從 CRITICAL 降低為 HIGH，因為新增預設根物件是取決於使用者應用程式和特定需求的建議。

變更日期	控制項 ID 和標題	變更描述
2023 年 12 月 5 日	【EC2.13】安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 22	從安全群組變更控制標題不應允許從 0.0.0.0/0 傳入連接埠 22 到安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 22。
2023 年 12 月 5 日	【EC2.14】安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389	變更控制標題自 確保沒有安全群組允許從 0.0.0.0/0 傳入連接埠 3389 到安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389。
2023 年 12 月 5 日	【RDS.9】RDS 資料庫執行個體應將日誌發佈至 CloudWatch Logs	從資料庫記錄變更的控制標題應啟用至 RDS 資料庫執行個體，並將日誌發佈至 CloudWatch Logs。Security Hub CSPM 已識別此控制項只會檢查日誌是否發佈至 Amazon CloudWatch Logs，而不會檢查是否啟用 RDS 日誌。如果 RDS 資料庫執行個體設定為將日誌發佈至 CloudWatch Logs，控制項會產生PASSED調查結果。控制項標題已更新，以反映目前的行為。

變更日期	控制項 ID 和標題	變更描述
2023 年 12 月 5 日	【EKS.8】 EKS 叢集應該啟用稽核記錄	此控制項會檢查 Amazon EKS 叢集是否已啟用稽核記錄。Security Hub CSPM 用來評估此控制項的 AWS Config 規則從 變更為 eks-cluster-logging-enabled eks-cluster-log-enabled 。
2023 年 11 月 17 日	【EC2.19】 安全群組不應允許無限制存取高風險的連接埠	EC2.19 會檢查安全群組的無限制傳入流量是否可供被視為高風險的指定連接埠存取。Security Hub CSPM 更新了此控制項，以便在做為安全群組規則的來源提供受管字首清單時將其納入考量。如果字首清單包含字串 '0.0.0.0/0' 或 ':::0'，則控制項會產生 FAILED 調查結果。
2023 年 11 月 16 日	【CloudWatch.15】 CloudWatch 警示應已設定指定的動作	從 CloudWatch 警示變更控制標題時，應針對 ALARM 狀態設定動作至 CloudWatch 警示時，應已設定指定的動作。

變更日期	控制項 ID 和標題	變更描述
2023 年 11 月 16 日	【CloudWatch.16】 CloudWatch 日誌群組應保留一段指定的時間	從 CloudWatch 日誌群組變更的控制標題應保留至少 1 年，而 CloudWatch 日誌群組應保留一段指定的時間。
2023 年 11 月 16 日	【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作	將控制標題從 VPC Lambda 函數變更為 VPC Lambda 函數應在多個可用區域中操作。
2023 年 11 月 16 日	【AppSync.2】 AWS AppSync 應該啟用欄位層級記錄	從 變更的控制標題AWS AppSync 應開啟請求層級和欄位層級記錄，AWS AppSync 且應啟用欄位層級記錄。
2023 年 11 月 16 日	【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址	從 Amazon Elastic MapReduce 叢集主節點變更的控制標題不應具有 Amazon EMR 叢集主節點的公有 IP 地址，也不應具有公有 IP 地址。
2023 年 11 月 16 日	【Opensearch.2】 不應公開存取 OpenSearch 網域	從 OpenSearch 網域變更的控制標題應位於 VPC 中，不應公開存取 OpenSearch 網域。

變更日期	控制項 ID 和標題	變更描述
2023 年 11 月 16 日	【ES.2】不應公開存取 Elasticsearch 網域	從 Elasticsearch 網域變更的控制標題應位於 VPC 中，不應公開存取 Elasticsearch 網域。
2023 年 10 月 31 日	【ES.4】應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤	ES.4 會檢查 Elasticsearch 網域是否設定為將錯誤日誌傳送至 Amazon CloudWatch Logs。控制項先前為 Elasticsearch 網域產生了一個 PASSED 調查結果，該網域已將任何日誌設定為傳送至 CloudWatch Logs。Security Hub CSPM 已更新控制項，僅針對設定為將錯誤日誌傳送至 CloudWatch Logs 的 Elasticsearch 網域產生 PASSED 調查結果。控制項也已更新，將不支援錯誤日誌的 Elasticsearch 版本排除在評估之外。

變更日期	控制項 ID 和標題	變更描述
2023 年 10 月 16 日	【EC2.13】安全群組不應允許從 0.0.0.0/0 或 : : /0 傳入連接埠 22	EC2.13 會檢查安全群組是否允許不受限制的連接埠 22 傳入存取。Security Hub CSPM 更新了此控制項，以便在做為安全群組規則的來源提供受管字首清單時將其納入考量。如果字首清單包含字串 '0.0.0.0/0' 或 ': : /0'，則控制項會產生 FAILED 調查結果。
2023 年 10 月 16 日	【EC2.14】安全群組不應允許從 0.0.0.0/0 或 : : /0 傳入連接埠 3389	EC2.14 會檢查安全群組是否允許不受限制的連接埠 3389 傳入存取。Security Hub CSPM 更新了此控制項，以便在做為安全群組規則的來源提供受管字首清單時將其納入考量。如果字首清單包含字串 '0.0.0.0/0' 或 ': : /0'，則控制項會產生 FAILED 調查結果。

變更日期	控制項 ID 和標題	變更描述
2023 年 10 月 16 日	【EC2.18】安全群組應僅允許授權連接埠不受限制的傳入流量	EC2.18 會檢查使用中的安全群組是否允許不受限制的傳入流量。Security Hub CSPM 更新了此控制項，以便在做為安全群組規則的來源提供受管字首清單時將其納入考量。如果字首清單包含字串 '0.0.0.0/0' 或 ': : /0'，則控制項會產生 FAILED 調查結果。
2023 年 10 月 16 日	【Lambda.2】Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 現在支援 python3.11 做為參數。
2023 年 10 月 4 日	【S3.7】S3 一般用途儲存貯體應使用跨區域複寫	Security Hub CSPM 新增了值 <code>ReplicationType</code> 為的參數 <code>CROSS-REGION</code> ，以確保 S3 儲存貯體已啟用跨區域複寫，而不是啟用相同區域複寫。

變更日期	控制項 ID 和標題	變更描述
2023 年 9 月 27 日	【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行	Security Hub CSPM 更新了 Amazon EKS 叢集可執行的最舊支援 Kubernetes 版本，以產生傳遞的問題清單。目前最舊支援的版本是 Kubernetes 1.24。
2023 年 9 月 20 日	【CloudFront.2】 CloudFront 分佈應啟用原始存取身分	Security Hub CSPM 已淘汰此控制項，並將其從所有標準中移除。反之，請參閱 【CloudFront.13】 CloudFront 分佈應使用原始存取控制 。原始存取控制是目前的安全最佳實務。此控制項將在 90 天內從文件中移除。

變更日期	控制項 ID 和標題	變更描述
2023 年 9 月 20 日	【EC2.22】應移除未使用的 Amazon EC2 安全群組	Security Hub CSPM 已從 AWS 基礎安全最佳實務 (FSBP) 和國家標準技術研究所 (NIST) SP 800-53 修訂版 5 中移除此控制。它仍然是服務受管標準的一部分：AWS Control Tower。如果安全群組連接到 EC2 執行個體或彈性網路介面，此控制項會產生傳遞的問題清單。不過，對於某些使用案例，未連接的安全群組不會構成安全風險。您可以使用其他 EC2 控制項，例如 EC2.2、EC2.13、EC2.14、EC2.18 和 EC2.19，來監控您的安全群組。
2023 年 9 月 20 日	【EC2.29】應在 VPC 中啟動 EC2 執行個體	Security Hub CSPM 已淘汰此控制項，並將其從所有標準中移除。Amazon EC2 已將 EC2-Classic 執行個體遷移至 VPC。此控制項將在 90 天內從文件中移除。

變更日期	控制項 ID 和標題	變更描述
2023 年 9 月 20 日	[S3.4] S3 儲存貯體應啟用伺服器端加密	Security Hub CSPM 已淘汰此控制項，並將其從所有標準中移除。Amazon S3 現在可在新的和現有的 S3 儲存貯體上使用 S3 受管金鑰 (SS3-S3) 提供預設加密。使用 SS3-S3 或 SS3-KMS 伺服器端加密的現有儲存貯體的加密設定保持不變。此控制項將在 90 天內從文件中移除。
2023 年 9 月 14 日	【EC2.2】 VPC 預設安全群組不應允許傳入或傳出流量	來自 VPC 預設安全群組的變更控制標題不應允許傳入和傳出至 VPC 預設安全群組的流量不應允許傳入或傳出流量。
2023 年 9 月 14 日	【IAM.9】 應為根使用者啟用 MFA	應為根使用者啟用從虛擬 MFA 到 MFA 的變更控制標題。
2023 年 9 月 14 日	【RDS.19】 應為關鍵叢集事件設定現有的 RDS 事件通知訂閱	應將關鍵叢集事件的事件 RDS 事件通知訂閱變更控制標題，設定為關鍵叢集事件的現有 RDS 事件通知訂閱。

變更日期	控制項 ID 和標題	變更描述
2023 年 9 月 14 日	<u>【RDS.20】 應為關鍵資料庫執行個體事件設定現有的 RDS 事件通知訂閱</u>	應將關鍵資料庫執行個體事件的 RDS 事件通知訂閱變更控制標題，設定為關鍵資料庫執行個體事件的現有 RDS 事件通知訂閱。
2023 年 9 月 14 日	<u>【WAF.2】 AWS WAF 傳統區域規則應至少有一個條件</u>	從 WAF 區域規則變更控制標題時，至少應有一個條件變更為 AWS WAF 傳統區域規則時，至少應有一個條件。
2023 年 9 月 14 日	<u>【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則</u>	將控制項標題從 WAF 區域規則群組變更為 Classic 區域規則群組時，AWS WAF 至少應有一個規則。
2023 年 9 月 14 日	<u>【WAF.4】 AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組</u>	從 WAF 區域 Web ACL 變更的控制項標題應至少有一個規則或規則群組，變更為 AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組。

變更日期	控制項 ID 和標題	變更描述
2023 年 9 月 14 日	【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件	從 WAF 全域規則變更控制標題應至少有一個條件變更為 AWS WAF Classic 全域規則應至少有一個條件。
2023 年 9 月 14 日	【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則	將控制項標題從 WAF 全域規則群組變更為 Classic 全域規則群組時，應至少 AWS WAF 有一個規則。
2023 年 9 月 14 日	【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組	從 WAF 全域 Web ACL 變更的控制項標題應具有至少一個規則或規則群組，而 AWS WAF Classic 全域 Web ACLs 應具有至少一個規則或規則群組。
2023 年 9 月 14 日	【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組	從 WAFv2 Web ACL 變更的控制標題應該至少有一個規則或規則群組到 AWS WAF Web ACLs 應該至少有一個規則或規則群組。
2023 年 9 月 14 日	【WAF.11】 應該啟用 AWS WAF Web ACL 記錄	AWS WAF 應該啟用從 v2 Web ACL 記錄到 AWS WAF Web ACL 記錄的變更控制標題。

變更日期	控制項 ID 和標題	變更描述
2023 年 7 月 20 日	[S3.4] S3 儲存貯體應啟用伺服器端加密	S3.4 會檢查 Amazon S3 儲存貯體是否已啟用伺服器端加密，或 S3 儲存貯體政策是否在沒有伺服器端加密的情況下明確拒絕PutObject 請求。Security Hub CSPM 已更新此控制項，以包含使用 KMS 金鑰 (DSSE-KMS) 的雙層伺服器端加密。當 S3 儲存貯體使用 SSE-S3、SSE-KMS 或 DSSE-KMS 加密時，控制項會產生傳遞的問題清單。
2023 年 7 月 17 日	【S3.17】 S3 一般用途儲存貯體應使用 靜態加密 AWS KMS keys	S3.17 會檢查 Amazon S3 儲存貯體是否使用加密 AWS KMS key。Security Hub CSPM 已更新此控制項，以包含使用 KMS 金鑰 (DSSE-KMS) 的雙層伺服器端加密。當 S3 儲存貯體使用 SSE-KMS 或 DSSE-KMS 加密時，控制項會產生傳遞的問題清單。

變更日期	控制項 ID 和標題	變更描述
2023 年 6 月 9 日	【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行	EKS.2 會檢查 Amazon EKS 叢集是否在支援的 Kubernetes 版本上執行。最舊的支援版本現在是 1.23。
2023 年 6 月 9 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 現在支援 ruby3.2 做為參數。
2023 年 6 月 5 日	【APIGateway.5】 API Gateway REST API 快取資料應靜態加密	APIGateway.5.checks Amazon API Gateway REST API 階段中的所有方法是否靜態加密。Security Hub CSPM 已更新控制項，只在針對該方法啟用快取時，才能評估特定方法的加密。
2023 年 5 月 18 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 現在支援 java17 做為參數。

變更日期	控制項 ID 和標題	變更描述
2023 年 5 月 18 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 不再支援 nodejs12.x 做為參數。
2023 年 4 月 23 日	【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行	ECS.10 會檢查 Amazon ECS Fargate 服務是否執行最新的 Fargate 平台版本。客戶可以直接透過 ECS 或使用 CodeDeploy 部署 Amazon ECS。Security Hub CSPM 更新了此控制項，以便在您使用 CodeDeploy 部署 ECS Fargate 服務時產生已傳遞的問題清單。
2023 年 4 月 20 日	【S3.6】 S3 一般用途儲存貯體政策應限制對其他的存取 AWS 帳戶	S3.6 會檢查 Amazon Simple Storage Service (Amazon S3) 儲存貯體政策是否防止委託人對 S3 儲存貯體中的資源 AWS 帳戶執行拒絕的動作。Security Hub CSPM 已更新控制項，以說明儲存貯體政策中的條件。

變更日期	控制項 ID 和標題	變更描述
2023 年 4 月 18 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 現在支援 python3.10 做為參數。
2023 年 4 月 18 日	【Lambda.2】 Lambda 函數應使用支援的執行時間	Lambda.2 會檢查執行時間的 AWS Lambda 函數設定是否符合每種語言中支援執行時間設定的預期值。Security Hub CSPM 不再支援 dotnetcore3.1 做為參數。
2023 年 4 月 17 日	【RDS.11】 RDS 執行個體應該啟用自動備份	RDS.11 會檢查 Amazon RDS 執行個體是否已啟用自動備份，且備份保留期間大於或等於七天。Security Hub CSPM 已更新此控制項，以排除僅供讀取複本的評估，因為並非所有引擎都支援在僅供讀取複本上自動備份。此外，RDS 不提供在建立僅供讀取複本時指定備份保留期的選項。依預設，會建立備份保留期為的僅供讀取複本。

的 Security Hub CSPM 控制項 AWS 帳戶

這些 Security Hub CSPM 控制項會評估 AWS 帳戶。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Account.1】 應針對 提供安全性聯絡資訊 AWS 帳戶

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.2、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

類別：識別 > 資源組態

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：[security-account-information-provided](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon Web Services (AWS) 帳戶是否具有安全性聯絡資訊。如果未為帳戶提供安全聯絡資訊，則控制項會失敗。

備用安全聯絡人允許 AWS 與其他人聯絡，以解決您帳戶的問題，以防您無法聯絡。通知可以是來自或其他 AWS 服務 團隊 支援，與您的 AWS 帳戶 用量相關的安全相關主題。

修補

若要將替代聯絡人新增為安全聯絡人 AWS 帳戶，請參閱AWS 《帳戶管理參考指南》中的[更新替代聯絡人 AWS 帳戶](#)。

【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分

類別：保護 > 安全存取控制 > 存取控制

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

嚴重性：高

資源類型：AWS::::Account

AWS Config 規則：[account-part-of-organizations](#)

排程類型：定期

參數：無

此控制項會檢查 AWS 帳戶 是否為透過 管理之組織的一部分 AWS Organizations。如果帳戶不是組織的一部分，則控制項會失敗。

Organizations 可協助您在擴展工作負載時集中管理環境 AWS。您可以使用多個 AWS 帳戶 來隔離具有特定安全需求的工作負載，或遵循 HIPAA 或 PCI 等架構。透過建立組織，您可以單一單位管理多個帳戶，並集中管理其對 AWS 服務資源和區域的存取。

修補

若要建立新組織並自動 AWS 帳戶 新增至組織，請參閱AWS Organizations 《使用者指南》中的[建立組織](#)。若要將帳戶新增至現有組織，請參閱AWS Organizations 《使用者指南》中的[邀請 AWS 帳戶加入您的組織](#)。

的 Security Hub CSPM 控制項 AWS Amplify

這些 Security Hub CSPM 控制項會評估 AWS Amplify 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Amplify.1】 Amplify 應用程式應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Amplify::App

AWS Config 規則：[amplify-app-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Amplify 應用程式是否具有 `requiredKeyTags` 參數指定的標籤索引鍵。如果應用程式沒有任何標籤索引鍵，或沒有 `requiredKeyTags` 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 `requiredKeyTags` 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果應用程式沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 `aws:` 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需有關將標籤新增至 AWS Amplify 應用程式的資訊，請參閱《AWS Amplify 託管使用者指南》中的[資源標記支援](#)。

【Amplify.2】 Amplify 分支應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Amplify::Branch

AWS Config 規則：[amplify-branch-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1-6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Amplify 分支是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果分支沒有任何標籤索引鍵，或沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果分支沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws: 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需將標籤新增至 AWS Amplify 分支的詳細資訊，請參閱 AWS Amplify 《託管使用者指南》中的[資源標記支援](#)。

Amazon API Gateway 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon API Gateway 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【APIGateway.1】應啟用 API Gateway REST 和 WebSocket API 執行記錄

相關要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::ApiGateway::Stage、AWS::ApiGatewayV2::Stage

AWS Config 規則：[api-gw-execution-logging-enabled](#)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
loggingLevel	Logging level (記錄層級)	列舉	ERROR, INFO	No default value

此控制項會檢查 Amazon API Gateway REST 或 WebSocket API 的所有階段是否已啟用記錄。如果 loggingLevel 不是 API 的所有階段 ERROR 或 INFO，則控制項會失敗。除非您提供自訂參數值來指示應啟用特定日誌類型，否則如果記錄層級為 ERROR 或 INFO，Security Hub CSPM 會產生傳遞的問題清單 INFO。

API Gateway REST 或 WebSocket API 階段應該啟用相關日誌。API Gateway REST 和 WebSocket API 執行記錄提供對 API Gateway REST 和 WebSocket API 階段提出請求的詳細記錄。這些階段包括 API 整合後端回應、Lambda 授權方回應，以及 AWS 整合端點 requestId 的。

修補

若要啟用 REST 和 WebSocket API 操作的記錄，請參閱 [API Gateway 開發人員指南中的使用 API Gateway 主控台設定 CloudWatch API 記錄](#)。

【APIGateway.2】API Gateway REST API 階段應設定為使用 SSL 憑證進行後端身分驗證

相關要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-85、NIST.800-53.r5 SI-7 3.13.15

類別：保護 > 資料保護 > data-in-transit 加密

嚴重性：中

資源類型：AWS::ApiGateway::Stage

AWS Config 規則：[api-gw-ssl-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon API Gateway REST API 階段是否已設定 SSL 憑證。後端系統使用這些憑證來驗證傳入請求是否來自 API Gateway。

API Gateway REST API 階段應使用 SSL 憑證設定，以允許後端系統驗證請求是否來自 API Gateway。

修補

如需如何產生和設定 API Gateway REST API SSL 憑證的詳細說明，請參閱 API Gateway 開發人員指南中的[產生和設定後端身分驗證的 SSL 憑證](#)。

【APIGateway.3】API Gateway REST API 階段應該已啟用 AWS X-Ray 追蹤

相關需求：NIST.800-53.r5 CA-7

類別：偵測 > 偵測服務

嚴重性：低

資源類型：AWS::ApiGateway::Stage

AWS Config 規則：[api-gw-xray-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查您的 Amazon API Gateway REST API 階段是否已啟用 AWS X-Ray 主動追蹤。

X-Ray 主動追蹤可更快速回應基礎基礎設施的效能變更。效能變更可能會導致 API 無法使用。X-Ray 主動追蹤提供使用者請求的即時指標，這些請求會流經您的 API Gateway REST API 操作和連線服務。

修補

如需如何為 API Gateway REST API 操作啟用 X-Ray 主動追蹤的詳細指示，請參閱 [《開發人員指南》中的 Amazon API Gateway 主動追蹤支援 AWS X-Ray](#)。AWS X-Ray

【APIGateway.4】API Gateway 應與 WAF Web ACL 建立關聯

相關要求：NIST.800-53.r5 AC-4(21)

類別：保護 > 保護服務

嚴重性：中

資源類型：AWS::ApiGateway::Stage

AWS Config 規則：[api-gw-associated-with-waf](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 API Gateway 階段是否使用 AWS WAF Web 存取控制清單 (ACL)。如果 AWS WAF Web ACL 未連接至 REST API Gateway 階段，則此控制項會失敗。

AWS WAF 是一種 Web 應用程式防火牆，可協助保護 Web 應用程式和 APIs 免受攻擊。它可讓您設定 ACL，這是一組規則，可根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 請求。確保您的 API Gateway 階段與 AWS WAF Web ACL 相關聯，以協助保護其免受惡意攻擊。

修補

如需有關如何使用 API Gateway 主控台將 AWS WAF 區域性 Web ACL 與現有 API Gateway API 階段建立關聯的資訊，請參閱[APIs Gateway 開發人員指南》中的使用 AWS WAF 來保護您的 API](#)。

【APIGateway.5】API Gateway REST API 快取資料應靜態加密

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：AWS::ApiGateway::Stage

AWS Config rule：api-gw-cache-encrypted (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 API Gateway REST API 階段中已啟用快取的所有方法是否已加密。如果 API Gateway REST API 階段中的任何方法設定為快取且未加密快取，則控制項會失敗。Security Hub CSPM 只有在針對該方法啟用快取時，才會評估特定方法的加密。

加密靜態資料可降低未驗證的使用者存取磁碟上儲存的資料的風險 AWS。它新增了另一組存取控制，以限制未經授權的使用者存取資料的能力。例如，需要 API 許可才能解密資料，才能讀取資料。

API Gateway REST API 快取應靜態加密，以增加一層安全性。

修補

若要設定階段的 API 快取，請參閱 [《API Gateway 開發人員指南》中的啟用 Amazon API Gateway 快取](#)。在快取設定中，選擇加密快取資料。

【APIGateway.8】API Gateway 路由應指定授權類型

相關需求：NIST.800-53.r5 AC-3、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::ApiGatewayV2::Route

AWS Config 規則：[api-gwv2-authorization-type-configured](#)

排程類型：定期

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
authorizationType	API 路由的授權類型	列舉	AWS_IAM, CUSTOM, JWT	無預設值

此控制項會檢查 Amazon API Gateway 路由是否具有授權類型。如果 API Gateway 路由沒有任何授權類型，則控制項會失敗。或者，如果您希望控制項僅在路由使用 參數中指定的授權類型時傳遞，您可以提供自訂 `authorizationType` 參數值。

API Gateway 支援多種機制來控制和管理 API 的存取。透過指定授權類型，您可以限制只有授權的使用者或程序才能存取 API。

修補

若要設定 HTTP APIs 的授權類型，請參閱 [《API Gateway 開發人員指南》中的在 API Gateway 中控制和管理對 HTTP API 的存取](#)。若要設定 WebSocket APIs 的授權類型，請參閱 [《API Gateway 開發人員指南》中的在 API Gateway 中控制和管理對 WebSocket API 的存取](#)。

【APIGateway.9】應為 API Gateway V2 階段設定存取記錄

相關要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(7)、PCIIST.100.10.4.2。

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::ApiGatewayV2::Stage

AWS Config 規則：[api-gwv2-access-logs-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon API Gateway V2 階段是否已設定存取記錄。如果未定義存取日誌設定，則此控制項會失敗。

API Gateway 存取日誌提供有關誰存取您的 API 以及發起人如何存取 API 的詳細資訊。這些日誌適用於安全與存取稽核及鑑識調查等應用程式。啟用這些存取日誌以分析流量模式和疑難排解問題。

如需其他最佳實務，請參閱[APIs開發人員指南》中的監控 REST API](#)。

修補

若要設定存取記錄，請參閱 [API Gateway 開發人員指南中的使用 API Gateway 主控台設定 CloudWatch API 記錄](#)。

【APIGateway.10】API Gateway V2 整合應使用 HTTPS 進行私有連線

類別：保護 > 資料保護 > data-in-transit

嚴重性：中

資源類型：AWS::ApiGatewayV2::Integration

AWS Config 規則：[apigatewayv2-integration-private-https-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 API Gateway V2 整合是否已針對私有連線啟用 HTTPS。如果未設定 TLS，則控制項會失敗。

VPC Links 會將 API Gateway 連線至私有資源。當 VPC Links 建立私有連線時，它們本質上不會加密資料。設定 TLS 可確保使用 HTTPS 透過 API Gateway end-to-end 加密。如果沒有 TLS，敏感 API 流量會在私有連線之間未加密。HTTPS 加密透過私有連線保護流量，避免資料攔截、man-in-the-middle 攻擊和憑證暴露。

修補

若要在 API Gateway v2 整合中啟用私有連線的傳輸中加密，請參閱《Amazon API Gateway 開發人員指南》中的[更新私有整合](#)。設定 [TLS 組態](#)，讓私有整合使用 HTTPS 通訊協定。

【APIGateway.11】API Gateway 網域名稱應使用建議的安全政策

類別：保護 > data-in-transit 加密

嚴重性：中

資源類型：AWS::ApiGateway::DomainName

AWS Config 規則：[apigateway-domain-name-tls-check](#)

排程類型：變更已觸發

參數：

- allowedSecurityPolicies: SecurityPolicy_TLS13_1_3_2025_09, SecurityPolicy_TLS13_1_3_FIPS_2025_09, SecurityPolicy_TLS13_1_2_PFS_PQ_2025_09, SecurityPolicy_TLS13_2025_EDGE, SecurityPolicy_TLS12_PFS_2025_EDGE (不可自訂)

此控制項會檢查 API Gateway 網域名稱是否設定為使用建議的安全政策來加密傳輸中的資料。如果 API Gateway 網域名稱未設定為使用建議的安全政策，則控制項會失敗。

安全政策是 API Gateway 所提供的最低 TLS 版本與密碼套件的預先定義組合。當用戶端建立 API 的 TLS 交握或自訂網域名稱時，安全政策會強制執行 API Gateway 接受的 TLS 版本和密碼套件。安全政策可保護您的 API 和自訂網域名稱，使其免於發生網路安全問題，例如在用戶端和伺服器之間竄改和竊聽。使用建議的安全政策有助於確保 API Gateway 網域名稱使用現代、安全的 TLS 組態，以保護用戶端和 API 之間傳輸中的資料。

修補

若要更新 API Gateway 網域名稱的 TLS 安全政策，請參閱《Amazon API Gateway 開發人員指南》中的[如何變更安全政策](#)。

的 Security Hub CSPM 控制項 AWS AppConfig

這些 Security Hub CSPM 控制項會評估 AWS AppConfig 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【AppConfig.1】AWS AppConfig 應用程式應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::AppConfig::Application

AWS Config 規則：appconfig-application-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS AppConfig 應用程式是否具有具有參數 中定義之特定金鑰的標籤 `requiredKeyTags`。如果應用程式沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredKeyTags`。如果 `requiredKeyTags` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果應用程式未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 AWS AppConfig 應用程式，請參閱 AWS AppConfig API 參考[TagResource](#)中的 。

【AppConfig.2】AWS AppConfig 組態設定檔應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::AppConfig::ConfigurationProfile

AWS Config 規則：appconfig-configuration-profile-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS AppConfig 組態描述檔是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果組態描述檔沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果組態設定檔未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 AWS AppConfig 組態設定檔，請參閱 AWS AppConfig API 參考 [TagResource](#) 中的。

【AppConfig.3】AWS AppConfig 環境應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::AppConfig::Environment

AWS Config 規則：appconfig-environment-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS AppConfig 環境是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果環境沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果環境未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 AWS AppConfig 環境，請參閱 AWS AppConfig API 參考 [TagResource](#) 中的。

【AppConfig.4】AWS AppConfig 應標記延伸關聯

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::AppConfig::ExtensionAssociation

AWS Config 規則：appconfig-extension-association-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS AppConfig 延伸關聯是否具有與參數中定義之特定金鑰的標籤 `requiredKeyTags`。如果延伸關聯沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 `requiredKeyTags`。如果 `requiredKeyTags` 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果延伸關聯未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 AWS AppConfig 延伸關聯，請參閱《AWS AppConfig API 參考 [TagResource](#)》中的。

Amazon AppFlow 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 Amazon AppFlow 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【AppFlow.1】Amazon AppFlow 流程應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::AppFlow::Flow

AWS Config 規則：appflow-flow-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon AppFlow 流程是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果流程沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果流程未標記任何索引鍵，則會失敗。系統會 aws: 忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義

許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 Amazon AppFlow 流程，請參閱《[Amazon AppFlow 使用者指南](#)》中的在 [Amazon AppFlow 中建立流程](#)。 AppFlow

的 Security Hub CSPM 控制項 AWS App Runner

這些 AWS Security Hub CSPM 控制項會評估 AWS App Runner 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【AppRunner.1】App Runner 服務應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::AppRunner::Service

AWS Config 規則：[apprunner-service-tagged](#)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS App Runner 服務是否具有具有參數 中定義之特定金鑰的標籤 `requiredKeyTags`。如果 App Runner 服務沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredKeyTags`。如果 `requiredKeyTags` 未提供參數，則控制項只會檢查標籤金鑰是否存在，如果 App Runner 服務未標記任何金鑰，則會失敗。系統會 `aws:` 忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

如需將標籤新增至 AWS App Runner 服務的資訊，請參閱 AWS App Runner API 參考[TagResource](#)中的。

【AppRunner.2】應標記 App Runner VPC 連接器

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::AppRunner::VpcConnector

AWS Config 規則：[apprunner-vpc-connector-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS App Runner VPC 連接器是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果 VPC 連接器沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果 VPC 連接器未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

如需將標籤新增至 AWS App Runner VPC 連接器的詳細資訊，請參閱《AWS App Runner API 參考 [TagResource](#)》中的。

的 Security Hub CSPM 控制項 AWS AppSync

這些 Security Hub CSPM 控制項會評估 AWS AppSync 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【AppSync.1】AWS AppSync API 快取應靜態加密

Important

Security Hub CSPM 已於 2026 年 3 月 9 日淘汰此控制項。如需詳細資訊，請參閱 [Security Hub CSPM 控制項的變更日誌](#)。AWS AppSync now 為所有目前和未來的 API 快取提供預設加密。

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::AppSync::GraphQLApi

AWS Config 規則：[appsync-cache-ct-encryption-at-rest](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS AppSync API 快取是否靜態加密。如果 API 快取未靜態加密，則控制項會失敗。

靜態資料是指存放在持久性、非揮發性儲存體中任何持續時間的資料。加密靜態資料可協助您保護其機密性，進而降低未經授權的使用者可存取資料的風險。

修補

您無法在啟用 AWS AppSync API 的快取之後變更加密設定。反之，您必須刪除快取，並在啟用加密的情況下重新建立快取。如需詳細資訊，請參閱《AWS AppSync 開發人員指南》中的[快取加密](#)。

【AppSync.2】AWS AppSync 應該啟用欄位層級記錄

相關要求：PCI DSS v4.0.1/10.4.2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::AppSync::GraphQLApi

AWS Config 規則：[appsync-logging-enabled](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值	
fieldLoggingLevel	欄位記錄層級	列舉	ERROR, ALL, INFO, DEBUG	No default value	

此控制項會檢查 AWS AppSync API 是否已開啟欄位層級記錄。如果欄位解析程式日誌層級設定為無，則控制項會失敗。除非您提供自訂參數值來指出應該啟用特定日誌類型，否則如果欄位解析程式日誌層級為 ERROR 或 ALL，Security Hub CSPM 會產生傳遞的問題清單。

您可以使用記錄和指標來識別、故障診斷和最佳化您的 GraphQL 查詢。開啟 for AWS AppSync GraphQL 的記錄可協助您取得 API 請求和回應的詳細資訊、識別和回應問題，以及遵守法規要求。

修補

若要開啟的記錄 AWS AppSync，請參閱《AWS AppSync 開發人員指南》中的[設定和組態](#)。

【AppSync.4】AWS AppSync GraphQL APIs 應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::AppSync::GraphQLApi

AWS Config rule：tagged-appsync-graphqlapi (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS AppSync GraphQL API 是否具有具有參數中定義之特定金鑰的標籤 `requiredTagKeys`。如果 GraphQL API 沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果 GraphQL API 未標記任何索引鍵，則會失敗。系統會 `aws:忽略` 自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 AWS AppSync GraphQL API，請參閱《AWS AppSync API 參考 [TagResource](#)》中的。

【AppSync.5】AWS AppSync GraphQL APIs 不應使用 API 金鑰進行身分驗證

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

類別：保護 > 安全存取管理 > 無密碼身分驗證

嚴重性：高

資源類型：AWS::AppSync::GraphQLApi

AWS Config 規則：[appsync-authorization-check](#)

排程類型：已觸發變更

參數：

- AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS (不可自訂)

此控制項會檢查您的應用程式是否使用 API 金鑰與 AWS AppSync GraphQL API 互動。如果使用 API 金鑰驗證 AWS AppSync GraphQL API，則控制項會失敗。

API 金鑰是應用程式中的硬式編碼值，會在您建立未經驗證的 GraphQL 端點時由 AWS AppSync 服務產生。如果此 API 金鑰遭到入侵，您的端點容易受到意外存取的影響。除非您支援可公開存取的應用程式或網站，否則我們不建議使用 API 金鑰進行身分驗證。

修補

若要為您的 AWS AppSync GraphQL API 設定授權選項，請參閱《AWS AppSync 開發人員指南》中的[授權和身分驗證](#)。

【AppSync.6】AWS AppSync API 快取應在傳輸中加密

 Important

Security Hub CSPM 已於 2026 年 3 月 9 日淘汰此控制項。如需詳細資訊，請參閱 [Security Hub CSPM 控制項的變更日誌](#)。AWS AppSync now 為所有目前和未來的 API 快取提供預設加密。

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::AppSync::ApiCache

AWS Config 規則：[appsync-cache-ct-encryption-in-transit](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS AppSync API 快取是否在傳輸中加密。如果 API 快取未在傳輸中加密，則控制項會失敗。

傳輸中的資料是指從一個位置移動到另一個位置的資料，例如叢集中的節點之間，或叢集與您的應用程式之間。資料可能會在網際網路或私有網路中移動。加密傳輸中的資料可降低未經授權的使用者可以竊聽網路流量的風險。

修補

您無法在啟用 AWS AppSync API 的快取之後變更加密設定。反之，您必須刪除快取，並在啟用加密的情況下重新建立快取。如需詳細資訊，請參閱《AWS AppSync 開發人員指南》中的[快取加密](#)。

Amazon Athena 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Athena 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Athena.1】 Athena 工作群組應靜態加密

Important

Security Hub CSPM 已於 2024 年 4 月淘汰此控制項。如需詳細資訊，請參閱[Security Hub CSPM 控制項的變更日誌](#)。

類別：保護 – 資料保護 – 靜態資料加密

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

嚴重性：中

資源類型：AWS::Athena::WorkGroup

AWS Config 規則：[athena-workgroup-encrypted-at-rest](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Athena 工作群組是否靜態加密。如果 Athena 工作群組未靜態加密，則控制項會失敗。

在 Athena 中，您可以建立工作群組，以執行團隊、應用程式或不同工作負載的查詢。每個工作群組都有一個設定，可在所有查詢上啟用加密。您可以選擇搭配 Amazon Simple Storage Service (Amazon S3) 受管金鑰使用伺服器端加密、搭配 AWS Key Management Service (AWS KMS) 金鑰使用伺服器端加密，或搭配客戶受管 KMS 金鑰使用用戶端加密。靜態資料是指在任何期間內存放在持久性、非揮發性儲存體中的任何資料。加密可協助您保護此類資料的機密性，降低未經授權的使用者可存取資料的風險。

修補

若要啟用 Athena 工作群組的靜態加密，請參閱《Amazon Athena 使用者指南》中的[編輯工作群組](#)。在查詢結果組態區段中，選取加密查詢結果。

【Athena.2】應標記 Athena 資料目錄

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Athena::DataCatalog

AWS Config rule：tagged-athena-datacatalog (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1-6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon Athena 資料目錄是否具有具有參數中定義之特定金鑰的標籤requiredTagKeys。如果資料目錄沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果資料目錄未標記任何索引鍵，則會失敗。系統會aws:忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Athena 資料目錄，請參閱《Amazon Athena [Athena 使用者指南](#)》中的[標記 Athena 資源](#)。

【Athena.3】 應標記 Athena 工作群組

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Athena::WorkGroup

AWS Config rule：tagged-athena-workgroup (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	No default value

此控制項會檢查 Amazon Athena 工作群組是否具有具有參數 中定義之特定金鑰的標籤 `requiredTagKeys`。如果工作群組沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果工作群組未標記任何索引鍵，則 控制會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Athena 工作群組，請參閱《Amazon Athena 使用者指南》中的 [在個別工作群組上新增和刪除標籤](#)。

【Athena.4】 Athena 工作群組應該已啟用記錄

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::Athena::WorkGroup

AWS Config 規則：[athena-workgroup-logging-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Athena 工作群組是否已啟用記錄。如果工作群組未啟用記錄，則控制項會失敗。

稽核日誌會追蹤和監控系統活動。它們提供事件的記錄，可協助您偵測安全漏洞、調查事件並遵守法規。稽核日誌也會增強組織的整體責任和透明度。

修補

如需有關啟用 Athena 工作群組記錄的資訊，請參閱《Amazon Athena 使用者指南》中的在 Athena [中啟用 CloudWatch 查詢指標](#)。

的 Security Hub CSPM 控制項 AWS Backup

這些 Security Hub CSPM 控制項會評估 AWS Backup 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Backup.1】 AWS Backup 復原點應靜態加密

相關需求：NIST.800-53.r5 CP-9(8)、NIST.800-53.r5 SI-12

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::Backup::RecoveryPoint

AWS Config 規則：[backup-recovery-point-encrypted](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS Backup 復原點是否靜態加密。如果復原點未靜態加密，則控制項會失敗。

AWS Backup 復原點是指在備份程序中建立的特定資料複本或快照。它代表資料備份並做為還原點的特定時間點，以防原始資料遺失、損毀或無法存取。加密備份復原點可多加一層保護，防止未經授權的存取。加密是保護備份資料的機密性、完整性和安全性的最佳實務。

修補

若要加密 AWS Backup 復原點，請參閱《AWS Backup 開發人員指南》中的[中的備份加密 AWS Backup](#)。

【Backup.2】 AWS Backup 復原點應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Backup::RecoveryPoint

AWS Config rule：tagged-backup-recoverypoint (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Backup 復原點是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果復原點沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果復原點未標記任何索引鍵，則 會失敗。系統會忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

將標籤新增至 AWS Backup 復原點

1. 在 <https://console.aws.amazon.com/backup> 開啟 AWS Backup 主控台。
2. 在導覽窗格中，選擇 Backup plans (備份計劃)。
3. 從清單中選擇備份計劃。
4. 在備份計畫標籤區段中，選擇管理標籤。
5. 輸入標籤的金鑰和值。針對其他鍵/值對選擇新增標籤。
6. 當您完成新增標籤的作業時，請選擇 Save (儲存)。

【Backup.3】 保存 AWS Backup 庫應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Backup::BackupVault

AWS Config rule：tagged-backup-backupvault (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Backup 保存庫是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果復原點沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果復原點未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

將標籤新增至 AWS Backup 保存庫

1. 在 <https://console.aws.amazon.com/backup> 開啟 AWS Backup 主控台。
2. 在導覽窗格中，選擇 Backup vaults (備份文件庫)。
3. 從清單中選擇備份保存庫。
4. 在備份保存庫標籤區段中，選擇管理標籤。
5. 輸入標籤的金鑰和值。針對其他鍵/值對選擇新增標籤。
6. 當您完成新增標籤的作業時，請選擇 Save (儲存)。

【Backup.4】應標記 AWS Backup 報告計劃

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Backup::ReportPlan

AWS Config rule：tagged-backup-reportplan (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Backup 報告計劃是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果報告計畫沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果報告計畫未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

將標籤新增至 AWS Backup 報告計畫

1. 在 <https://console.aws.amazon.com/backup> 開啟 AWS Backup 主控台。
2. 在導覽窗格中，選擇 Backup vaults (備份文件庫)。
3. 從清單中選擇備份保存庫。
4. 在備份保存庫標籤區段中，選擇管理標籤。
5. 選擇 Add new tag (新增標籤)。輸入標籤的金鑰和值。針對其他鍵/值對重複此步驟。

6. 當您完成新增標籤的作業時，請選擇 Save (儲存)。

【Backup.5】 AWS Backup 備份計劃應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Backup::BackupPlan

AWS Config rule：tagged-backup-backupplan (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Backup 備份計劃是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果備份計劃沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果備份計劃未標記任何索引鍵，則 會失敗。系統會 aws: 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

將標籤新增至 AWS Backup 備份計劃

1. 在 <https://console.aws.amazon.com/backup> 開啟 AWS Backup 主控台。
2. 在導覽窗格中，選擇 Backup vaults (備份文件庫)。
3. 從清單中選擇備份保存庫。
4. 在備份保存庫標籤區段中，選擇管理標籤。
5. 選擇 Add new tag (新增標籤)。輸入標籤的金鑰和值。針對其他鍵/值對重複此步驟。
6. 當您完成新增標籤的作業時，請選擇 Save (儲存)。

的 Security Hub CSPM 控制項 AWS Batch

這些 Security Hub CSPM 控制項會評估 AWS Batch 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Batch.1】 批次任務佇列應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Batch::JobQueue

AWS Config 規則：[batch-job-queue-tagged](#)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	無預設值

此控制項會檢查 AWS Batch 任務佇列是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果任務佇列沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果任務佇列未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至批次任務佇列，請參閱 AWS Batch 《使用者指南》中的 [標記您的資源](#)。

【Batch.2】 批次排程政策應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Batch::SchedulingPolicy

AWS Config 規則：[batch-scheduling-policy-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Batch 排程政策是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果排程政策沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果排程政策未標記任何索引鍵，則會失敗。系統會忽略以 aws: 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至批次排程政策，請參閱 AWS Batch 《使用者指南》中的[標記您的資源](#)。

【Batch.3】 批次運算環境應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Batch::ComputeEnvironment

AWS Config 規則：[batch-compute-environment-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Batch 運算環境是否具有具有參數中定義之特定金鑰的標籤requiredKeyTags。如果運算環境沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗requiredKeyTags。如果requiredKeyTags未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果運算環境未標記任何索引鍵，則控制會失敗。系統會aws:忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至批次運算環境，請參閱AWS Batch 《使用者指南》中的[標記您的資源](#)。

【Batch.4】 應標記受管批次運算環境中的運算資源屬性

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Batch::ComputeEnvironment

AWS Config 規則：[batch-managed-compute-env-compute-resources-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查受管 AWS Batch 運算環境中的運算資源屬性是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果運算資源屬性沒有任何標籤索引鍵，或它沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果運算資源屬性沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws: 字首。此控制項不會評估未受管的運算環境，或使用 AWS Fargate 資源的受管環境。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多 存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需有關在受管運算環境中新增標籤以 AWS Batch 運算資源的資訊，請參閱AWS Batch 《使用者指南》中的[標記您的資源](#)。

Amazon Bedrock AgentCore 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Bedrock AgentCore 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定

類別：保護 > 安全存取管理 > 資源不可公開存取

嚴重性：高

資源類型：AWS::BedrockAgentCore::Runtime

AWS Config 規則：[bedrockagentcore-runtime-private-network-required](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Bedrock AgentCore 執行期是否已設定 VPC 網路模式。如果執行時間的網路模式設為 PUBLIC，則控制項會失敗。

將公有網路模式用於 Amazon Bedrock AgentCore 執行時間會直接將執行時間公開到網際網路，增加受攻擊面和未經授權的存取風險。使用 VPC 網路模式設定執行時間可確保執行時間流量限制在您的私有網路中，讓您能夠套用安全群組、網路 ACLs 和 VPC 流程日誌等網路層級安全控制。

修補

若要修復此調查結果，請更新不合規的 Bedrock AgentCore 執行時間，並使用 VPC 網路模式進行設定。如需說明，請參閱 [《Amazon Bedrock AgentCore 開發人員指南》中的設定 VPC 的 Amazon Bedrock AgentCore 執行期和工具](#)。 AgentCore

【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權

類別：保護 > 安全存取管理

嚴重性：高

資源類型：AWS::BedrockAgentCore::Gateway

AWS Config 規則：[bedrockagentcore-gateway-authorizer-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Bedrock AgentCore Gateway 是否需要傳入請求的授權。如果 Bedrock AgentCore Gateway 未設定傳入授權，則控制項會失敗。

在 Amazon Bedrock AgentCore 閘道上設定身分驗證可確保只有授權的用戶端才能將請求傳送至您的 AI 代理器。如果沒有授權方，具有閘道端點網路存取權的任何實體都可以叫用您的代理程式，這可能會導致未經授權的資料存取、資源濫用或意外成本。傳入授權會驗證嘗試透過 AgentCore 閘道存取目標的使用者。

修補

若要設定 Amazon Bedrock AgentCore Gateway 的傳入授權，請參閱《Amazon Bedrock AgentCore 開發人員指南》中的[為您的閘道設定傳入授權](#)。

【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密

相關要求：NIST.800-53.r5 AU-9、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：AWS::BedrockAgentCore::Memory

AWS Config 規則：[bedrock-agentcore-memory-encryption-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Bedrock AgentCore 記憶體是否使用客戶受管 AWS KMS 金鑰進行靜態加密。如果 Bedrock AgentCore 記憶體未使用客戶受管 KMS 金鑰加密，則控制項會失敗。

使用客戶受管 KMS 金鑰來加密 Amazon Bedrock AgentCore 記憶體，可增強預設服務受管金鑰的安全性。客戶受管 KMS 金鑰可讓您完全控制加密金鑰生命週期和存取政策。此外，所有加密金鑰用量都可以透過 記錄和監控，AWS CloudTrail 以確保可稽核性。

修補

若要使用客戶受管 KMS 金鑰加密 Amazon Bedrock AgentCore 記憶體，請參閱《[Amazon Bedrock AgentCore 開發人員指南](#)》中的[加密 Amazon Bedrock AgentCore 記憶體](#)。 AgentCore

【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密

相關要求：NIST.800-53.r5 AU-9、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：AWS::BedrockAgentCore::Gateway

AWS Config 規則：[bedrockagentcore-gateway-encryption-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Bedrock AgentCore Gateway 是否使用客戶受管 AWS KMS 金鑰進行靜態加密。如果 Bedrock AgentCore Gateway 未使用客戶受管 KMS 金鑰加密，則控制項會失敗。

根據預設，Amazon Bedrock AgentCore 會使用 AWS 受管金鑰加密閘道資料。使用客戶受管 KMS 金鑰可讓您完全控制加密金鑰生命週期，包括輪換、存取政策和稽核 AWS CloudTrail。這有助於滿足要求對敏感 AI 工作負載進行客戶控制加密的合規要求。

修補

若要使用客戶受管 KMS 金鑰加密 Bedrock AgentCore Gateway，請參閱《[Amazon Bedrock AgentCore 開發人員指南](#)》中的[使用客戶受管 KMS 金鑰加密](#) AgentCore 閘道。 AgentCore

【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式

類別：保護 > 安全網路組態 > VPC 內的資源

嚴重性：高

資源類型：AWS::BedrockAgentCore::BrowserCustom

AWS Config 規則：[bedrockagentcore-browsercustom-network-mode-not-public](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Bedrock AgentCore 自訂瀏覽器是否已設定為公有網路模式。如果網路模式設為公有，則控制項會失敗。

將 PUBLIC 網路模式用於 Amazon Bedrock AgentCore 自訂瀏覽器會直接將瀏覽器工作階段公開到網際網路，增加攻擊面和未經授權的存取風險。使用 VPC 網路模式設定瀏覽器可確保瀏覽器流量限制在私有網路內，讓您能夠套用安全群組、網路 ACLs 和 VPC 流程日誌等網路層級安全控制。

修補

若要修復此調查結果，請刪除不合規的 Bedrock AgentCore 自訂瀏覽器，然後使用 VPC 網路模式重新建立。如需說明，請參閱 [《Amazon Bedrock AgentCore 開發人員指南》](#) 中的設定 VPC 的 Amazon Bedrock AgentCore 執行期和工具。 AgentCore

【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::BedrockAgentCore::BrowserCustom

AWS Config 規則：[bedrockagentcore-browsercustom-recording-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Bedrock AgentCore 自訂瀏覽器是否已在設定 S3 目的地的情況下啟用工作階段記錄。如果自訂瀏覽器未啟用錄製，或未設定用於儲存錄製的 S3 位置，則控制項會失敗。

Bedrock AgentCore 自訂瀏覽器的工作階段記錄可確保瀏覽器互動的完整可稽核性，以便在自動瀏覽工作階段期間偵測未經授權的存取、資料外洩或惡意活動。

修補

如需如何啟用瀏覽器工作階段錄製的指示，請參閱《Amazon Bedrock AgentCore 開發人員指南》中的[工作階段錄製和重播](#)。

的 Security Hub CSPM 控制項 AWS Certificate Manager

這些 AWS Security Hub CSPM 控制項會評估 AWS Certificate Manager (ACM) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【ACM.1】 匯入和 ACM 發行的憑證應在指定的期間之後續約

相關要求：NIST.800-53.r5 SC-28(3)、NIST.800-53.r5 SC-7(16)、NIST.800-171.r2 3.13.15、PCI DSS v4.0.1/4.2.1

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::ACM::Certificate

AWS Config 規則：[acm-certificate-expiration-check](#)

排程類型：變更已觸發和定期

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
daysToExpiration	必須續約 ACM 憑證的天數	Integer	14 至 365	30

此控制項會檢查 AWS Certificate Manager (ACM) 憑證是否在指定的期間內續約。它會檢查匯入的憑證和 ACM 提供的憑證。如果未在指定的期間內續約憑證，則控制項會失敗。除非您提供續約期間的自訂參數值，否則 Security Hub CSPM 會使用預設值 30 天。

ACM 可以自動續約使用 DNS 驗證的憑證。對於使用電子郵件驗證的憑證，您必須回應網域驗證電子郵件。ACM 不會自動續約您匯入的憑證。您必須手動更新匯入的憑證。

修補

ACM 為 Amazon 發行的 SSL/TLS 憑證提供受管續約。這表示 ACM 會自動續約您的憑證（如果您使用 DNS 驗證），或在憑證過期接近時傳送電子郵件通知給您。這些服務可供公有和私有 ACM 憑證使用。

對於透過電子郵件驗證的網域

當憑證過期後 45 天，ACM 會為每個網域名稱傳送電子郵件給網域擁有者。若要驗證網域並完成續約，您必須回應電子郵件通知。

如需詳細資訊，請參閱 AWS Certificate Manager 《使用者指南》中的 [透過電子郵件驗證的網域續約](#)。

對於 DNS 驗證的網域

ACM 會自動續約使用 DNS 驗證的憑證。在過期前 60 天，ACM 會驗證憑證是否可以續約。

如果無法驗證網域名稱，則 ACM 會傳送通知，告知需要手動驗證。它會在過期前 45 天、30 天、7 天和 1 天傳送這些通知。

如需詳細資訊，請參閱 AWS Certificate Manager 《使用者指南》中的 [DNS 驗證的網域續約](#)。

【ACM.2】 由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度

相關要求：PCI DSS v4.0.1/4.2.1

類別：識別 > 庫存 > 庫存服務

嚴重性：高

資源類型：AWS::ACM::Certificate

AWS Config 規則：[acm-certificate-rsa-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查由管理的 RSA 憑證是否 AWS Certificate Manager 使用至少 2,048 位元的金鑰長度。如果金鑰長度小於 2,048 位元，則控制項會失敗。

加密強度與金鑰大小直接相關。我們建議您使用至少 2,048 位元的金鑰長度來保護您的 AWS 資源，因為運算能力變得較不昂貴，且伺服器變得更先進。

修補

ACM 發行之 RSA 憑證的金鑰長度下限已經是 2,048 位元。如需使用 ACM 發行新 RSA 憑證的說明，請參閱AWS Certificate Manager 《使用者指南》中的[發行和管理憑證](#)。

雖然 ACM 可讓您匯入金鑰長度較短的憑證，但您必須使用至少 2,048 位元的金鑰才能傳遞此控制項。您無法在匯入憑證後變更金鑰長度。相反地，您必須刪除金鑰長度小於 2,048 位元的憑證。如需將憑證匯入 ACM 的詳細資訊，請參閱AWS Certificate Manager 《使用者指南》中的[匯入憑證的先決條件](#)。

【ACM.3】ACM 憑證應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::ACM::Certificate

AWS Config rule：tagged-acm-certificate (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Certificate Manager (ACM) 憑證是否具有具有參數中定義之特定金鑰的標籤requiredTagKeys。如果憑證沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供參數，則控制項只會檢查標籤金鑰是否存在，如果憑證未標記任何金鑰，則會失敗。系統會aws:忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知

的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 ACM 憑證，請參閱 AWS Certificate Manager 《使用者指南》中的[標記 AWS Certificate Manager 憑證](#)。

的 Security Hub CSPM 控制項 CloudFormation

這些 Security Hub CSPM 控制項會評估 AWS CloudFormation 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【CloudFormation.1】CloudFormation 堆疊應與 Simple Notification Service (SNS) 整合

Important

Security Hub CSPM 已於 2024 年 4 月淘汰此控制項。如需詳細資訊，請參閱[Security Hub CSPM 控制項的變更日誌](#)。

相關需求：NIST.800-53.r5 SI-4(12)、NIST.800-53.r5 SI-4(5)

類別：偵測 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：AWS::CloudFormation::Stack

AWS Config 規則：[cloudformation-stack-notification-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Simple Notification Service 通知是否與 CloudFormation 堆疊整合。如果沒有 SNS 通知與其相關聯，則 CloudFormation 堆疊的控制項會失敗。

使用 CloudFormation 堆疊設定 SNS 通知有助於在堆疊發生任何事件或變更時，立即通知利益相關者。

修補

若要整合 CloudFormation 堆疊和 SNS 主題，請參閱AWS CloudFormation 《使用者指南》中的[直接更新堆疊](#)。

【CloudFormation.2】應標記 CloudFormation 堆疊

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::CloudFormation::Stack

AWS Config rule：tagged-cloudformation-stack (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS CloudFormation 堆疊是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果堆疊沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果堆疊未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知

的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 CloudFormation 堆疊，請參閱 AWS CloudFormation API 參考中的 [CreateStack](#)。

【CloudFormation.3】CloudFormation 堆疊應啟用終止保護

類別：保護 > 資料保護 > 資料刪除保護

嚴重性：中

資源類型：AWS::CloudFormation::Stack

AWS Config 規則：[cloudformation-termination-protection-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS CloudFormation 堆疊是否已啟用終止保護。如果 CloudFormation 堆疊上未啟用終止保護，則控制項會失敗。

CloudFormation 有助於以稱為 Stack 的單一單位來管理相關資源。您可以在堆疊上啟用終止保護來防止堆疊遭意外刪除。如果使用者嘗試刪除啟用終止保護的堆疊，則刪除會失敗，且堆疊及其狀態保持不變。除了 DELETE_IN_PROGRESS 或 DELETE_COMPLETE 以外，您可以為處於任何狀態的堆疊設定終止保護。

Note

在堆疊上啟用或停用終止保護的同時，也將對屬於該堆疊的任何巢狀堆疊套用相同選擇。您無法直接在巢狀堆疊上啟用或停用終止保護。您無法直接刪除屬於已啟用終止保護之堆疊的巢狀

堆疊。如果堆疊名稱旁顯示 NESTED (巢狀)，則該堆疊為巢狀堆疊。您只能在該巢狀堆疊所屬的根堆疊上啟用終止保護。

修補

若要在 CloudFormation 堆疊上啟用終止保護，請參閱AWS CloudFormation 《使用者指南》中的[保護 CloudFormation 堆疊不會被刪除](#)。

【CloudFormation.4】CloudFormation 堆疊應具有相關聯的服務角色

類別：偵測 > 安全存取管理

嚴重性：中

資源類型：AWS::CloudFormation::Stack

AWS Config 規則：[cloudformation-stack-service-role-check](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 AWS CloudFormation 堆疊是否具有與其相關聯的服務角色。如果沒有與 CloudFormation 堆疊相關聯的服務角色，則控制項會失敗。

服務受管 StackSets 透過 AWS Organizations 受信任的存取整合使用執行角色。控制項也會為服務受管 StackSets 建立的 AWS CloudFormation 堆疊產生 FAILED 調查結果，因為沒有與其相關聯的服務角色。由於服務受管 StackSets 驗證的方式，無法為這些堆疊填入 roleARN 欄位。

搭配 CloudFormation 堆疊使用服務角色有助於實作最低權限存取，方法是將建立/更新堆疊的使用者與 CloudFormation 建立/更新資源所需的許可分開。這可降低權限提升的風險，並有助於在不同操作角色之間維持安全界限。

Note

建立堆疊後，就無法移除連接至堆疊的服務角色。其他具有在此堆疊上執行這些操作之許可的使用者，都能夠使用此角色，不論這些使用者是否有 `iam:PassRole` 許可。如果該角色包含使用者不該有的許可，您可能在無意中提升使用者的許可。確定該角色授予最低權限。

修補

若要將服務角色與 CloudFormation 堆疊建立關聯，請參閱AWS CloudFormation 《使用者指南》中的[CloudFormation 服務角色](#)。

Amazon CloudFront 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon CloudFront 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【CloudFront.1】CloudFront 分佈應設定預設根物件

相關要求：NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、PCI DSS v4.0.1/2.2.6

類別：保護 > 安全存取管理 > 不可公開存取的資源

嚴重性：高

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-default-root-object-configured](#)

排程類型：已觸發變更

參數：無

此控制項會檢查具有 S3 原始伺服器的 Amazon CloudFront 分佈是否設定為傳回預設根物件的特定物件。如果 CloudFront 分佈使用 S3 原始伺服器且未設定預設根物件，則控制項會失敗。此控制項不適用於使用自訂原始伺服器的 CloudFront 分佈。

使用者有時可能會請求分佈的根 URL，而不是分佈中的物件。發生這種情況時，指定預設根物件可協助避免暴露 Web 分佈的內容。

修補

若要設定 CloudFront 分佈的預設根物件，請參閱《Amazon CloudFront 開發人員指南》中的[如何指定預設根物件](#)。

【CloudFront.3】CloudFront 分佈應要求傳輸中加密

相關要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-85、NIST.800-53.r5 SI-7

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-viewer-policy-https](#)

排程類型：已觸發變更

參數：無

此控制可檢查 Amazon CloudFront 分佈是否要求檢視者直接使用 HTTPS，或其是否使用重新導向。如果 ViewerProtocolPolicy 設為allow-all適用於 defaultCacheBehavior或適用於的，則控制項會失敗cacheBehaviors。

HTTPS (TLS) 可用來防止潛在攻擊者使用中間人攻擊或類似的攻擊手法來竊聽或操控網路流量。只能允許透過 HTTPS (TLS) 進行加密連線。加密傳輸中的資料可能會影響效能。您應該使用此功能測試應用程式，以了解效能描述檔和 TLS 的影響。

修補

若要加密傳輸中的 CloudFront 分佈，請參閱《Amazon CloudFront 開發人員指南》中的[檢視器與 CloudFront 之間的通訊需要 HTTPS](#)。Amazon CloudFront

【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉

相關需求：NIST.800-53.r5 CP-10、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：低

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-origin-failover-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon CloudFront 分佈是否設定為具有兩個或多個原始伺服器的原始伺服器群組。

CloudFront 原始伺服器容錯移轉可以提高可用性。如果主要原始伺服器無法使用或傳回特定 HTTP 回應狀態碼，原始伺服器容錯移轉會自動將流量重新導向至次要原始伺服器。

修補

若要設定 CloudFront 分佈的原始伺服器容錯移轉，請參閱《Amazon CloudFront 開發人員指南》中的[建立原始伺服器群組](#)。

【CloudFront.5】CloudFront 分佈應該已啟用記錄

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.4.2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-accesslogs-enabled](#)

排程類型：已觸發變更

參數：無

此控制可檢查是否已在 CloudFront 分佈上啟用伺服器存取日誌記錄。如果未針對分佈啟用存取日誌記錄，則此控制會失敗。此控制項只會評估分佈是否啟用標準記錄（舊版）。

CloudFront 存取日誌可提供 CloudFront 所收到的每個使用者請求的詳細資訊。每個日誌都包含收到請求的日期和時間、提出請求的檢視者 IP 地址、請求的來源，以及檢視者提出請求的連接埠號碼等資訊。這些日誌適用於安全與存取稽核及鑑識調查等應用程式。如需分析存取日誌的詳細資訊，請參閱[《Amazon Athena 使用者指南》中的查詢 Amazon CloudFront 日誌](#)。Amazon Athena

修補

若要設定 CloudFront 分佈的標準記錄（舊版），請參閱《Amazon CloudFront 開發人員指南》中的[設定標準記錄（舊版）](#)。

【CloudFront.6】CloudFront 分佈應該啟用 WAF

相關要求：NIST.800-53.r5 AC-4(21)、PCI DSS v4.0.1/6.4.2

類別：保護 > 保護服務

嚴重性：中

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-associated-with-waf](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 CloudFront 分佈是否與 AWS WAF Classic 或 AWS WAF Web ACLs 相關聯。如果分佈未與 Web ACL 相關聯，則控制項會失敗。

AWS WAF 是一種 Web 應用程式防火牆，可協助保護 Web 應用程式和 APIs 免受攻擊。其可讓您設定一組稱為 Web 存取控制清單 (Web ACL) 的規則，該組規則可根據您定義的可自訂 Web 安全規則與條件來允許、封鎖或計數 Web 請求。確保您的 CloudFront 分佈與 AWS WAF Web ACL 相關聯，以協助保護它免受惡意攻擊。

修補

若要將 AWS WAF Web ACL 與 CloudFront 分佈建立關聯，請參閱《Amazon CloudFront 開發人員指南》中的[使用 AWS WAF 控制對內容的存取](#)。

【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證

相關要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-855.r5 SC-8 SI-7 3.13.15

類別：保護 > 資料保護 > data-in-transit 加密

嚴重性：低

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-custom-ssl-certificate](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 CloudFront 分佈是否使用 CloudFront 提供的預設 SSL/TLS 憑證。如果 CloudFront 分佈使用自訂 SSL/TLS 憑證，則此控制項會通過。如果 CloudFront 分佈使用預設 SSL/TLS 憑證，則此控制項會失敗。

自訂 SSL/TLS 可讓您的使用者使用替代網域名稱存取內容。您可以將自訂憑證存放在 AWS Certificate Manager（建議）或 IAM 中。

修補

若要使用自訂 SSL/TLS 憑證為 CloudFront 分佈新增替代網域名稱，請參閱《Amazon CloudFront 開發人員指南》中的[新增替代網域名稱](#)。

【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

類別：保護 > 安全網路組態

嚴重性：低

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-sni-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon CloudFront 分佈是否使用自訂 SSL/TLS 憑證，並設定為使用 SNI 來提供 HTTPS 請求。如果自訂 SSL/TLS 憑證相關聯，但 SSL/TLS 支援方法是專用 IP 地址，則此控制會失敗。

伺服器名稱指示 (SNI) 是 TLS 通訊協定的延伸，2010 年之後推出的瀏覽器 and 用戶端支援此選項。如果設定 CloudFront 使用 SNI 來提供 HTTPS 請求，則 CloudFront 會將您的替代網域名稱，與每個節點中的 IP 位址建立關聯。當檢視器提交內容的 HTTPS 請求時，DNS 會將請求路由到正確節點的 IP 位址。您網域名稱的 IP 位址在 SSL/TLS 交握溝通期間決定；IP 位址並非專用於您的分佈。

修補

若要設定 CloudFront 分佈以使用 SNI 提供 HTTPS 請求，請參閱CloudFront 開發人員指南》中的[使用 SNI 提供 HTTPS 請求（適用於大多數用戶端）](#)。如需自訂 SSL 憑證的相關資訊，請參閱[搭配 CloudFront 使用 SSL/TLS 憑證的要求](#)。

【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器

相關需求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-855.r5 SI-7

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-traffic-to-origin-encrypted](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon CloudFront 分佈是否正在加密流向自訂原始伺服器的流量。此控制項對於原始伺服器通訊協定政策允許 'http-only' 的 CloudFront 分佈失敗。如果分佈的原始通訊協定政策為 'match-viewer'，而檢視器通訊協定政策為 'allow-all'，則此控制項也會失敗。

HTTPS (TLS) 可用來協助防止竊聽或操控網路流量。只能允許透過 HTTPS (TLS) 進行加密連線。

修補

若要更新原始伺服器通訊協定政策以要求 CloudFront 連線加密，請參閱《Amazon CloudFront 開發人員指南》中的[在 CloudFront 與自訂原始伺服器之間通訊需要 HTTPS](#)。

【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定

相關要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8SI-7(2)、NIST.50505.5 3.13.15

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-no-deprecated-ssl-protocols](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon CloudFront 分佈是否使用已棄用的 SSL 通訊協定，以便在 CloudFront 節點和自訂原始伺服器之間進行 HTTPS 通訊。如果 CloudFront 分佈的 `OriginSslProtocols` 包含 `CustomOriginConfig`，則此控制項會失敗 SSLv3。

在 2015 年，網際網路工程任務小組 (IETF) 正式宣布，由於通訊協定不夠安全，SSL 3.0 應予以棄用。建議您將 TLSv1.2 或更新版本用於與自訂原始伺服器的 HTTPS 通訊。

修補

若要更新 CloudFront 分佈的原始伺服器 SSL 通訊協定，請參閱《Amazon CloudFront 開發人員指南》中的[需要 HTTPS 才能在 CloudFront 與自訂原始伺服器之間進行通訊](#)。

【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器

相關要求：NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、PCI DSS v4.0.1/2.2.6

類別：識別 > 資源組態

嚴重性：高

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-s3-origin-non-existent-bucket](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon CloudFront 分佈是否指向不存在的 Amazon S3 原始伺服器。如果原始伺服器設定為指向不存在的儲存貯體，則 CloudFront 分佈的控制項會失敗。此控制僅適用於沒有靜態網站託管的 S3 儲存貯體是 S3 原始伺服器的 CloudFront 分發。

當您帳戶中的 CloudFront 分佈設定為指向不存在的儲存貯體時，惡意的第三方可以建立參考的儲存貯體，並透過您的分佈提供自己的內容。建議您檢查所有原始伺服器，無論路由行為為何，以確保您的分佈指向適當的原始伺服器。

修補

若要修改 CloudFront 分佈以指向新的原始伺服器，請參閱《Amazon CloudFront 開發人員指南》中的[更新分佈](#)。

【CloudFront.13】CloudFront 分佈應使用原始存取控制

類別：保護 > 安全存取管理 > 資源不可公開存取

嚴重性：中

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-s3-origin-access-control-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查具有 Amazon S3 原始伺服器的 Amazon CloudFront 分佈是否已設定原始存取控制 (OAC)。Amazon S3 如果 CloudFront 分佈未設定 OAC，則控制項會失敗。

使用 S3 儲存貯體做為 CloudFront 分佈的原始伺服器時，您可以啟用 OAC。這僅允許透過指定的 CloudFront 分佈存取儲存貯體中的內容，並禁止直接從儲存貯體或其他分佈存取。雖然 CloudFront 支援原始存取身分 (OAI)，但 OAC 提供額外的功能，而使用 OAI 的分佈可以遷移到 OAC。雖然 OAI 提供安全的方式來存取 S3 原始伺服器，但它有限制，例如缺少對精細政策組態的支援，以及對於在中使用 POST 方法 AWS 區域且需要 AWS 簽章版本 4 (SigV4) 的 HTTP/HTTPS 請求。OAI 也不支援使用加密 AWS Key Management Service。OAC 是以使用 IAM 服務主體向 S3 原始伺服器進行身分驗證的 AWS 最佳實務為基礎。

修補

若要為具有 S3 原始伺服器的 CloudFront 分佈設定 OAC，請參閱《[Amazon CloudFront 開發人員指南](#)》中的[限制對 Amazon S3 原始伺服器的存取](#)。Amazon CloudFront

【CloudFront.14】應標記 CloudFront 分佈

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::CloudFront::Distribution

AWS Config rule：tagged-cloudfront-distribution (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon CloudFront 分佈是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果分佈沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果分佈未標記任何索引鍵，則 會失敗。系統會忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 CloudFront 分佈，請參閱 [《Amazon CloudFront 開發人員指南》](#) 中的標記 [Amazon CloudFront 分佈](#)。Amazon CloudFront

【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策

類別：保護 > 資料保護 > data-in-transit

嚴重性：中

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-ssl-policy-check](#)

排程類型：已觸發變更

參數：securityPolicies：TLSv1.2_2021, TLSv1.2_2025, TLSv1.3_2025 (不可自訂)

此控制項會檢查 Amazon CloudFront 分佈是否設定為使用建議的 TLS 安全政策。如果 CloudFront 分佈未設定為使用建議的 TLS 安全政策，則控制項會失敗。

如果您將 Amazon CloudFront 分佈設定為要求檢視器使用 HTTPS 存取內容，則必須選擇安全政策並指定要使用的最低 SSL/TLS 通訊協定版本。這會決定 CloudFront 用來與瀏覽者通訊的通訊協定版本，以及 CloudFront 用來加密通訊的密碼。我們建議您使用 CloudFront 提供的最新安全政策。這可確保 CloudFront 使用最新的密碼套件來加密檢視器和 CloudFront 分佈之間的傳輸中資料。

Note

此控制項只會針對設定為使用自訂 SSL 憑證且未設定為支援舊版用戶端的 CloudFront 分佈產生調查結果。

修補

如需有關為 CloudFront 分佈設定安全政策的資訊，請參閱《Amazon CloudFront 開發人員指南》中的[更新分佈](#)。當您設定分佈的安全政策時，請選擇最新的安全政策。

【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制

類別：保護 > 安全存取控制 > 存取控制

嚴重性：中

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-origin-lambda-url-oac-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查以 AWS Lambda 函數 URL 做為原始伺服器的 Amazon CloudFront 分佈是否已啟用原始存取控制 (OAC)。如果 CloudFront 分佈具有 Lambda 函數 URL 作為原始伺服器且未啟用 OAC，則控制項會失敗。

AWS Lambda 函數 URL 是 Lambda 函數的專用 HTTPS 端點。如果 Lambda 函數 URL 是 CloudFront 分佈的原始伺服器，則函數 URL 必須可公開存取。因此，作為安全最佳實務，您應該建立 OAC，並將其新增至分佈中的 Lambda 函數 URL。OAC 使用 IAM 服務主體來驗證 CloudFront 與函數 URL 之間的請求。它還支援使用資源型政策，只有在請求代表政策中指定的 CloudFront 分佈時，才允許叫用函數。

修補

如需有關為使用 Lambda 函數 URL 做為原始伺服器的 Amazon CloudFront 分佈設定 OAC 的資訊，請參閱《Amazon CloudFront 開發人員指南》中的[限制對 AWS Lambda 函數 URL 原始伺服器的存取](#)。

【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組

類別：保護 > 安全存取控制 > 存取控制

嚴重性：中

資源類型：AWS::CloudFront::Distribution

AWS Config 規則：[cloudfront-distribution-key-group-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon CloudFront 分佈是否設定為使用信任的金鑰群組進行簽章的 URL 或簽章的 Cookie 驗證。如果 CloudFront 分佈使用信任簽署者，或分佈未設定身分驗證，則控制項會失敗。

若要使用已簽署 URL 或已簽署 Cookie，您需要簽署者。簽署者是您在 CloudFront 中建立的受信任金鑰群組，或是包含 CloudFront 金鑰對 AWS 的帳戶。我們建議您使用信任的金鑰群組，因為使用 CloudFront 金鑰群組時，您不需要使用 AWS 帳戶根使用者來管理 CloudFront 簽章 URLs 公有金鑰。

Note

此控制項不會評估多租戶 CloudFront 分佈 (connectionMode=tenant-only)。

修補

如需搭配簽章 URLs 和 Cookie 使用受信任金鑰群組的詳細資訊，請參閱《Amazon CloudFront 開發人員指南》中的[使用受信任金鑰群組](#)。

的 Security Hub CSPM 控制項 AWS CloudTrail

這些 AWS Security Hub CSPM 控制項會評估 AWS CloudTrail 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【CloudTrail.1】CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤

相關要求：CIS AWS Foundations Benchmark 5.0.0/3.1 版，CIS AWS Foundations Benchmark 1.2.0/2.1 版，CIS AWS Foundations Benchmark 1.4.0/3.1 版，CIS AWS Foundations Benchmark 3.0.0/3.1 版，NIST.800-53.r5 AC-2(4)，NIST.800-53.r5 AC-4(26)，NIST.800-53.r5 AC-6(9)，NIST.800-53.r5 AU-10，NIST.800-53.r5 AU-12，NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)，NIST.800-53.r5 AU-6(4)，NIST.800-53.r5 AU-14(1)，NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)，NIST.800-53.r5 SI-3(8)，NIST.800-53.r5 SI-4(20)，NIST.800-53.r5 SI-7(8)，NIST.800-53.r5 SA-8(22)

類別：識別 > 記錄日誌

嚴重性：高

資源類型：AWS::::Account

AWS Config 規則：[multi-region-cloudtrail-enabled](#)

排程類型：定期

參數：

- readWriteType : ALL (不可自訂)
- includeManagementEvents : true (不可自訂)

此控制項會檢查是否有至少一個擷取讀取和寫入管理事件的多區域 AWS CloudTrail 線索。如果 CloudTrail 已停用，或沒有至少一個 CloudTrail 追蹤可擷取讀取和寫入管理事件，則控制項會失敗。

AWS CloudTrail 會記錄您帳戶的 AWS API 呼叫，並將日誌檔案交付給您。記錄的資訊包括下列資訊：

- API 發起人的身分
- API 呼叫的時間
- API 發起人的來源 IP 地址
- 請求參數
- 傳回的回應元素 AWS 服務

CloudTrail 提供帳戶的 AWS API 呼叫歷史記錄，包括從 AWS 管理主控台、AWS SDKs、命令列工具發出的 API 呼叫。歷史記錄也包含來自更高層級的 API 呼叫，AWS 服務例如 AWS CloudFormation。

CloudTrail 產生的 AWS API 呼叫歷史記錄可啟用安全性分析、資源變更追蹤和合規稽核。多區域線索也提供了下列優勢。

- 多區域線索可協助偵測在未使用區域中發生的未預期活動。
- 多區域線索可確保根據預設，為線索啟用全域服務記錄日誌。全域服務事件記錄會記錄 AWS 全域服務所產生的事件。
- 對於多區域追蹤，所有讀取和寫入操作的管理事件可確保 CloudTrail 記錄中所有資源的管理操作 AWS 帳戶。

根據預設，使用建立的 CloudTrail 追蹤 AWS 管理主控台 是多區域追蹤。

修補

若要在 CloudTrail 中建立新的多區域追蹤，請參閱AWS CloudTrail 《使用者指南》中的[建立追蹤](#)。使用下列的值：

欄位	Value
其他設定、日誌檔案驗證	已啟用
選擇日誌事件、管理事件、API 活動	讀取和寫入。清除排除項目的核取方塊。

若要更新現有的線索，請參閱AWS CloudTrail 《使用者指南》中的[更新線索](#)。在管理事件中，針對API 活動，選擇讀取和寫入。

[CloudTrail.2] CloudTrail 應啟用靜態加密

相關要求：CIS AWS Foundations Benchmark v5.0.0/3.5、CIS AWS Foundations Benchmark v1.2.0/2.7、CIS AWS Foundations Benchmark v1.4.0/3.7、CIS AWS Foundations Benchmark v3.0.0/3.5、NIST.800-53.r5 AU-9、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28(1)SC-28、NIST.800-53.r5 SC-7 SI-710.3.2

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::CloudTrail::Trail

AWS Config 規則：[cloud-trail-encryption-enabled](#)

排程類型：定期

參數：無

此控制項會檢查 CloudTrail 是否設定為使用伺服器端加密 (SSE) AWS KMS key 加密。如果KmsKeyId未定義，則控制項會失敗。

為了為您的敏感 CloudTrail 日誌檔案增加一層安全性，您應該使用[伺服器端加密搭配 AWS KMS keys \(SSE-KMS\)](#) 用於 CloudTrail 日誌檔案，以進行靜態加密。請注意，CloudTrail 交付至您儲存貯體的日誌檔案預設為使用 [Amazon S3-managed加密金鑰 \(SSE-S3\)](#) 進行 Amazon 伺服器端加密。

修補

若要啟用 CloudTrail 日誌檔案的 SSE-KMS 加密，請參閱AWS CloudTrail 《使用者指南》中的[更新線索以使用 KMS 金鑰](#)。

【CloudTrail.3】至少應啟用一個 CloudTrail 追蹤

相關要求：NIST.800-171.r2 3.3.1、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7、PCI DSS v3.2.1/10.1、PCI DSS v3.2.1/10.2.1、PCI DSS v3.2.1/10.2.2、PCI DSS v3.2.1/10.2.3、PCI DSS v3.2.1/10.2.4、PCI DSS v3.2.1/10.2.510.2.6、PCI DSS v3.2.1/10.2.7、PCI v3.2.1/、PCI v310.3.1.2.1/10.3.2。10.3.310.3.410.3.510.3.610.2.1

類別：識別 > 記錄日誌

嚴重性：高

資源類型：AWS:::Account

AWS Config 規則：[cloudtrail-enabled](#)

排程類型：定期

參數：無

此控制項會檢查 中的 AWS CloudTrail 追蹤是否已啟用 AWS 帳戶。如果您的帳戶未啟用至少一個 CloudTrail 追蹤，則控制項會失敗。

不過，某些 AWS 服務不會啟用所有 APIs 和事件的記錄。您應該實作 CloudTrail 以外的任何其他稽核線索，並在 [CloudTrail 支援的服務和整合](#) 中檢閱每個服務的文件。

修補

若要開始使用 CloudTrail 並建立線索，請參閱AWS CloudTrail 《使用者指南》中的[入門 AWS CloudTrail 教學](#)課程。

【CloudTrail.4】應啟用 CloudTrail 日誌檔案驗證

相關要求：CIS AWS Foundations Benchmark v5.0.0/3.2、CIS AWS Foundations Benchmark v1.2.0/2.2、CIS AWS Foundations Benchmark v1.4.0/3.2、CIS AWS Foundations Benchmark v3.0.0/3.2、NIST.800-53.r5 AU-9、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-7(1)、NIST.800-53.r5 SI-7(3)、NIST.800-53.r5 SI-7(7)、NIST.800-171.r2 3.3.2 13.2 、PCI.10.5.210.5.510.3.22

類別：資料保護 > 資料完整性

嚴重性：低

資源類型：AWS::CloudTrail::Trail

AWS Config 規則：[cloud-trail-log-file-validation-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否在 CloudTrail 追蹤上啟用日誌檔案完整性驗證。

CloudTrail 日誌檔案驗證會建立數位簽章的摘要檔案，其中包含 CloudTrail 寫入 Amazon S3 的每個日誌的雜湊。您可以使用這些摘要檔案來判斷在 CloudTrail 交付日誌之後，日誌檔案是否已變更、刪除或保持不變。

Security Hub CSPM 建議您在所有線索上啟用檔案驗證。日誌檔案驗證提供額外的 CloudTrail 日誌完整性檢查。

修補

若要啟用 CloudTrail 日誌檔案驗證，請參閱AWS CloudTrail 《使用者指南》中的[啟用 CloudTrail 的日誌檔案完整性驗證](#)。

【CloudTrail.5】CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合

相關要求：CIS AWS Foundations Benchmark 5.0.0/3.4 版，PCI DSS 3.2.1/10.5.3 版，CIS AWS Foundations Benchmark 1.2.0/2.4 版，CIS AWS Foundations Benchmark 1.4.0/3.4 版，NIST.800-53.r5 AC-2(4)，NIST.800-53.r5 AC-4(26)，NIST.800-53.r5 AC-6(9)，NIST.800-53.r5 AU-10，NIST.800-53.r5 AU-12，NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(1)，NIST.800-53.r5 AU-6(3)，NIST.800-53.r5 AU-6(4)，NIST.800-53.r5 AU-6(5)，NIST.800-53.r5 AU-7(1)，NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)，NIST.800-53.r5 SI-20、NIST.800-53.r5 SI-3(8)，NIST.800-53.r5 SI-4(20)，NIST.800-53.r5 SI-4(5)，NIST.800-53.r5 SI-7(8)

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::CloudTrail::Trail

AWS Config 規則：[cloud-trail-cloud-watch-logs-enabled](#)

排程類型：定期

參數：無

此控制項會檢查 CloudTrail 追蹤是否設定為將日誌傳送至 CloudWatch Logs。如果線索的 CloudWatchLogsLogGroupArn 屬性為空，則控制項會失敗。

CloudTrail 會記錄在特定帳戶中進行的 AWS API 呼叫。記錄的資訊包括下列項目：

- API 呼叫者的身分
- API 呼叫的時間

- API 呼叫者的來源 IP 地址
- 請求參數
- 傳回的回應元素 AWS 服務

CloudTrail 使用 Amazon S3 進行日誌檔案儲存和交付。您可以在指定的 S3 儲存貯體中擷取 CloudTrail 日誌以進行長期分析。若要執行即時分析，您可以設定 CloudTrail 將日誌傳送至 CloudWatch Logs。

對於在帳戶的所有區域中啟用的線索，CloudTrail 會將所有這些區域的日誌檔案傳送至 CloudWatch Logs 日誌群組。

Security Hub CSPM 建議您將 CloudTrail 日誌傳送至 CloudWatch Logs。請注意，此建議旨在確保擷取、監控和適當警示帳戶活動。您可以使用 CloudWatch Logs 來設定您的 AWS 服務。此建議不會排除使用不同的解決方案。

將 CloudTrail 日誌傳送至 CloudWatch Logs 可促進根據使用者、API、資源和 IP 地址的即時和歷史活動記錄。您可以使用此方法來建立異常或敏感帳戶活動的警示和通知。

修補

若要將 CloudTrail 與 CloudWatch Logs 整合，請參閱 AWS CloudTrail 《使用者指南》中的[將事件傳送至 CloudWatch Logs](#)。

【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取

相關要求：CIS AWS Foundations Benchmark v1.2.0/2.3、CIS AWS Foundations Benchmark v1.4.0/3.3、PCI DSS v4.0.1/1.4.4

類別：識別 > 記錄日誌

嚴重性：嚴重

資源類型：AWS::S3::Bucket

AWS Config 規則：無（自訂 Security Hub CSPM 規則）

排程類型：定期觸發和變更

參數：無

CloudTrail 會記錄您帳戶中每次 API 呼叫的記錄。這些日誌檔案會存放在 S3 儲存貯體中。CIS 建議將 S3 儲存貯體政策或存取控制清單 (ACL) 套用至 CloudTrail 記錄的 S3 儲存貯體，以防止公開存取

CloudTrail 日誌。允許公開存取 CloudTrail 日誌內容可能有助於對手識別受影響帳戶的使用或組態中的弱點。

若要執行此檢查，Security Hub CSPM 會先使用自訂邏輯來尋找存放 CloudTrail 日誌的 S3 儲存貯體。然後，它會使用 AWS Config 受管規則來檢查儲存貯體是否可公開存取。

如果您將日誌彙總到單一集中式 S3 儲存貯體，則 Security Hub CSPM 只會針對集中式 S3 儲存貯體所在的帳戶和區域執行檢查。對於其他帳戶和區域，控制狀態為無資料。

如果儲存貯體可公開存取，則檢查會產生失敗的問題清單。

修補

若要封鎖對 CloudTrail S3 儲存貯體的公開存取，請參閱《Amazon Simple Storage Service 使用者指南》中的[設定 S3 儲存貯體的封鎖公開存取設定](#)。選取所有四個 Amazon S3 封鎖公開存取設定。

【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄

相關要求：CIS AWS Foundations Benchmark v1.2.0/2.6、CIS AWS Foundations Benchmark v1.4.0/3.6、CIS AWS Foundations Benchmark v3.0.0/3.4、PCI DSS v4.0.1/10.2.1

類別：識別 > 記錄日誌

嚴重性：低

資源類型：AWS::S3::Bucket

AWS Config rule：None（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

S3 儲存貯體存取記錄會產生日誌，其中包含對 S3 儲存貯體提出的每個請求的存取記錄。存取日誌記錄包含要求的詳細資訊，例如要求類型、要求工作負載中指定的資源，以及要求的處理時間與日期。

CIS 建議您在 CloudTrail S3 儲存貯體上啟用儲存貯體存取記錄。

透過在目標 S3 儲存貯體上啟用 S3 儲存貯體記錄，您可以擷取可能影響目標儲存貯體中物件的所有事件。設定日誌放在單獨的儲存貯體中，可存取日誌資訊，這對安全性和事件反應工作流程極有幫助。

若要執行此檢查，Security Hub CSPM 會先使用自訂邏輯來尋找存放 CloudTrail 日誌的儲存貯體，然後使用 AWS Config 受管規則來檢查記錄是否已啟用。

如果 CloudTrail 將多個的日誌檔案交付 AWS 帳戶至單一目的地 Amazon S3 儲存貯體，Security Hub CSPM 只會針對其所在區域中的目的地儲存貯體評估此控制項。這可簡化您的問題清單。不過，您應該在所有將日誌傳送到目的地儲存貯體的帳戶中開啟 CloudTrail。對於保留目的地儲存貯體的所有帳戶，控制狀態為無資料。

修補

若要啟用 CloudTrail S3 儲存貯體的伺服器存取記錄，請參閱 [《Amazon Simple Storage Service 使用者指南》](#) 中的 [啟用 Amazon S3 伺服器存取記錄](#)。

【CloudTrail.9】應標記 CloudTrail 追蹤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::CloudTrail::Trail

AWS Config rule：tagged-cloudtrail-trail (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS CloudTrail 追蹤是否具有具有參數中定義之特定索引鍵的標籤 requiredTagKeys。如果線索沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果追蹤未標記任何索引鍵，則失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義

許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 CloudTrail 追蹤，請參閱 AWS CloudTrail API 參考中的 [AddTags](#)。

【CloudTrail.10】CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys

相關要求：NIST.800-53.r5 AU-9、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::CloudTrail::EventDataStore

AWS Config 規則：[event-data-store-cmk-encryption-enabled](#)

排程類型：定期

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
kmsKeyArns	AWS KMS keys 要包含在評估中的 Amazon Resource Name	StringList (最多 3 個項目)	現有 KMS 金鑰的 1–3 ARNs。例如：arn:aws:k	無預設值

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
	(ARNs清單。如果事件資料存放區未在清單中使用 KMS 金鑰加密，則控制項會產生FAILED問題清單。		ms:us-west-2:11112223333:key/1234abcd-12ab-34cd-56ef-1234567890ab。	

此控制項會檢查 AWS CloudTrail Lake 事件資料存放區是否使用客戶受管的靜態加密 AWS KMS key。如果事件資料存放區未使用客戶受管 KMS 金鑰加密，則控制項會失敗。您可以選擇性地為控制項指定要包含在評估中的 KMS 金鑰清單。

根據預設，AWS CloudTrail Lake 會使用 AES-256 演算法，使用 Amazon S3 受管金鑰 (SSE-S3) 加密事件資料存放區。如需其他控制，您可以設定 CloudTrail Lake，改為使用客戶受管 AWS KMS key (SSE-KMS) 加密事件資料存放區。客戶受管 KMS 金鑰是 AWS KMS key 您在 中建立、擁有和管理的 AWS 帳戶。您可以完全控制此類型的 KMS 金鑰。這包括定義和維護金鑰政策、管理授予、輪換密碼編譯材料、指派標籤、建立別名，以及啟用和停用金鑰。您可以在 CloudTrail 資料的密碼編譯操作中使用客戶受管 KMS 金鑰，並使用 CloudTrail 日誌稽核使用情況。

修補

如需有關使用您指定的 加密 AWS CloudTrail Lake AWS KMS key 事件資料存放區的資訊，請參閱AWS CloudTrail 《使用者指南》中的[更新事件資料存放區](#)。將事件資料存放區與 KMS 金鑰建立關聯後，您便無法移除或變更 KMS 金鑰。

Amazon CloudWatch 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon CloudWatch 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【CloudWatch.1】應該存在日誌指標篩選條件和警示以使用「根」使用者

相關要求：CIS AWS Foundations Benchmark v1.2.0/1.1、CIS AWS Foundations Benchmark v1.2.0/3.3、CIS AWS Foundations Benchmark v1.4.0/1.7、CIS AWS Foundations Benchmark v1.4.0/4.3、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7、PCI DSS v3.2.1/7.2.1

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config 規則：無（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

根使用者可以不受限制地存取中的所有服務和資源 AWS 帳戶。強烈建議您避免將根使用者用於日常任務。將根使用者的使用量降至最低，並採用最低權限原則進行存取管理，可降低意外變更和意外公開高權限憑證的風險。

最佳實務是，只有在需要[執行帳戶和服務管理任務](#)時，才使用您的根使用者憑證。Apply AWS Identity and Access Management (IAM) 政策直接套用至群組和角色，但不適用於使用者。如需如何設定管理員以供日常使用的教學課程，請參閱《[IAM 使用者指南](#)》中的[建立您的第一個 IAM 管理員使用者和群組](#)

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.4.0](#) 版中針對控制項 1.7 指定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在 NO_DATA 下列情況下，檢查會導致 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。

- 多區域追蹤屬於不同的帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生調查結果。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估NO_DATA的控制項，使用組織追蹤會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題ListSubscriptionsByTopic。否則 Security Hub CSPM 會產生控制項的問題WARNING清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。
2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱AWS CloudTrail 《使用者指南》中的[建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《Amazon CloudWatch 使用者指南》中的[為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<code>{\$.userIdentity.type="Root" && \$.userIdentity.invokedBy NOT EXISTS && \$.eventType != "AwsServiceEvent"}</code>
指標命名空間	<code>LogMetrics</code>

欄位	Value
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.2】確保未經授權的 API 呼叫存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.1、NIST.800-171.r2 3.13.1、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config rule：None（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

您可以將 CloudTrail 日誌導向 CloudWatch Logs 並建立對應的指標篩選條件和警示，以即時監控 API 呼叫。

CIS 建議您為未經授權的 API 呼叫建立指標篩選條件和警示。監控未經授權的 API 呼叫有助於揭露應用程式錯誤，可能會降低偵測惡意活動的時間。

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.2 版中針對控制項 3.1](#) 指定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在 NO_DATA 下列情況下，檢查會導致 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的 帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生調查結果。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估 NO_DATA 的控制項，使用組織追蹤會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題 `ListSubscriptionsByTopic`。否則 Security Hub CSPM 會產生控制項的問題 WARNING 清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。

2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱AWS CloudTrail 《使用者指南》中的[建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《Amazon CloudWatch 使用者指南》中的[為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<code>{{\$.errorCode="*UnauthorizedOperation"}} {{\$.errorCode="AccessDenied*"}}}</code>
指標命名空間	LogMetrics
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.3】確保沒有 MFA 的管理主控台登入存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.2

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config rule：None（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

您可以將 CloudTrail 日誌導向 CloudWatch Logs 並建立對應的指標篩選條件和警示，以即時監控 API 呼叫。

CIS 建議您建立不受 MFA 保護的指標篩選條件和警示主控台登入。監控單一因素主控台登入會增加不受 MFA 保護的帳戶可見性。

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.2 版中針對控制項 3.2 指定的確切稽核步驟](#)。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在下列情況下，檢查會導致 NO_DATA 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生調查結果。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估 NO_DATA 的控制項，使用組織線索會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的

帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題 `ListSubscriptionsByTopic`。否則 Security Hub CSPM 會產生控制項的問題 `WARNING` 清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。
2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱 AWS CloudTrail 《使用者指南》中的 [建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《Amazon CloudWatch 使用者指南》中的 [為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<pre>{ (\$.eventName = "ConsoleLogin") && (\$.additionalEventData.MFAUsed != "Yes") && (\$.userIdentity.type = "IAMUser") && (\$.responseElements.ConsoleLogin = "Success") }</pre>
指標命名空間	LogMetrics
指標值	1

欄位	Value
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.4】確保 IAM 政策變更存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.4、CIS AWS Foundations Benchmark v1.4.0/4.4、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config rule：None（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

此控制項會檢查您是否即時監控 API 呼叫，方法是將 CloudTrail 日誌導向 CloudWatch Logs，並建立對應的指標篩選條件和警示。

CIS 建議您為 IAM 政策所做的變更建立指標篩選條件和警示。監控這些變更有助於確保身分驗證和授權控制保持不變。

 Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在下列情況下，檢查會導致 NO_DATA 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生調查結果。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估 NO_DATA 的控制項，使用組織線索會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題 ListSubscriptionsByTopic。否則 Security Hub CSPM 會產生控制項的問題 WARNING 清單。

修補

 Note

我們在這些修復步驟中建議的篩選條件模式與 CIS 指引中的篩選條件模式不同。我們建議的篩選條件僅針對來自 IAM API 呼叫的事件。

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱 [《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。
2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱 AWS CloudTrail [《使用者指南》中的 建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱 [《Amazon CloudWatch 使用者指南》中的 為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<pre>{(\$.eventSource=iam.amazons.com) && ((\$.eventName=DeleteGroupPolicy) (\$.eventName=DeleteRolePolicy) (\$.eventName=DeleteUserPolicy) (\$.eventName=PutGroupPolicy) (\$.eventName=PutRolePolicy) (\$.eventName=PutUserPolicy) (\$.eventName=CreatePolicy) (\$.eventName=DeletePolicy) (\$.eventName=CreatePolicyVersion) (\$.eventName=DeletePolicyVersion) (\$.eventName=AttachRolePolicy) (\$.eventName=DetachRolePolicy) (\$.eventName=AttachUserPolicy) (\$.eventName=DetachUserPolicy) (\$.eventName=AttachGroupPolicy) (\$.eventName=DetachGroupPolicy))}</pre>
指標命名空間	LogMetrics

欄位	Value
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.5】確保 CloudTrail 組態變更存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.5、CIS AWS Foundations Benchmark v1.4.0/4.5、NIST.800-171.r2 3.3.8、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config rule：None（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

您可以將 CloudTrail 日誌導向 CloudWatch Logs 並建立對應的指標篩選條件和警示，以即時監控 API 呼叫。

CIS 建議您為 CloudTrail 組態設定的變更建立指標篩選條件和警示。監控這些變更有助於確保帳戶活動的持續可見性。

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.4.0](#) 版中針對控制項 4.5 指定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制項會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在下列情況下，檢查會導致 NO_DATA 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生問題清單。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估 NO_DATA 的控制項，使用組織追蹤會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題 `ListSubscriptionsByTopic`。否則 Security Hub CSPM 會產生控制項的問題 WARNING 清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。

2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱AWS CloudTrail 《使用者指南》中的[建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《Amazon CloudWatch 使用者指南》中的[為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	{ (\$.eventName=CreateTrail) (\$.eventName=UpdateTrail) (\$.eventName>DeleteTrail) (\$.eventName=StartLogging) (\$.eventName=StopLogging)}
指標命名空間	LogMetrics
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.6】確保 AWS 管理主控台 驗證失敗時存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.6、CIS AWS Foundations Benchmark v1.4.0/4.6、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config 規則：無（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

您可以將 CloudTrail 日誌導向 CloudWatch Logs 並建立對應的指標篩選條件和警示，以即時監控 API 呼叫。

CIS 建議您為失敗的主控台身分驗證嘗試建立指標篩選條件和警示。監控失敗的主控台登入可能會降低偵測嘗試暴力破解登入資料的前置時間，這可能會提供可用於其他事件相互關聯的指標，例如來源 IP。

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.4.0](#) 版中針對控制項 4.6 指定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在 NO_DATA 下列情況下，檢查會導致 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的 帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生問題清單。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中

評估NO_DATA的控制項，使用組織追蹤會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題ListSubscriptionsByTopic。否則 Security Hub CSPM 會產生控制項的問題WARNING清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。
2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱AWS CloudTrail 《使用者指南》中的[建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《Amazon CloudWatch 使用者指南》中的[為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<code>{{\$.eventName=ConsoleLogin}&& (\$.errorMessage="Failed authentication")}}</code>
指標命名空間	LogMetrics
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.7】確保日誌指標篩選條件和警示存在，以停用或排程刪除客戶受管金鑰

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.7、CIS AWS Foundations Benchmark v1.4.0/4.7、NIST.800-171.r2 3.13.10、NIST.800-171.r2 3.13.16、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config rule：None（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

您可以將 CloudTrail 日誌導向 CloudWatch Logs 並建立對應的指標篩選條件和警示，以即時監控 API 呼叫。

CIS 建議您為狀態已變更為已停用或排程刪除的客戶受管金鑰建立指標篩選條件和警示。無法繼續存取使用已停用或已刪除金鑰加密的資料。

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.4.0](#) 版中針對控制項 4.7 指定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制

會失敗。無法將其他欄位或術語新增至指標篩選條件。如果 `ExcludeManagementEventSources` 包含 `kms.amazonaws.com`，則控制項也會失敗。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在 NO_DATA 下列情況下，檢查會導致 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的 帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生問題清單。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估 NO_DATA 的控制項，使用組織追蹤會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題 `ListSubscriptionsByTopic`。否則 Security Hub CSPM 會產生控制項的問題 WARNING 清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱 [《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。

2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱AWS CloudTrail 《使用者指南》中的[建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《Amazon CloudWatch 使用者指南》中的[為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<code>{{\$.eventSource=kms.amazonaws.com) && ((\$.eventName=DisableKey) (\$.eventName=ScheduleKeyDeletion))}}</code>
指標命名空間	LogMetrics
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.8】確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.8、CIS AWS Foundations Benchmark v1.4.0/4.8、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config rule：None（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

您可以將 CloudTrail 日誌導向 CloudWatch Logs 並建立對應的指標篩選條件和警示，以即時監控 API 呼叫。

CIS 建議您為 S3 儲存貯體政策的變更建立指標篩選條件和警示。監控這些變更可能會降低偵測和更正敏感 S3 儲存貯體寬鬆政策的時間。

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.4.0](#) 版中針對控制項 4.8 指定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在 NO_DATA 下列情況下，檢查會導致 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的 帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生問題清單。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估 NO_DATA 的控制項，使用組織追蹤會導致 的控制狀態。在成員帳戶中，Security Hub

CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫來存取 Amazon SNS 主題 `ListSubscriptionsByTopic`。否則 Security Hub CSPM 會產生控制項的問題 WARNING 清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。
2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱 AWS CloudTrail 《使用者指南》中的 [建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《Amazon CloudWatch 使用者指南》中的 [為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<pre>{(\$.eventSource=s3.amazonaws.com) && ((\$.eventName=PutBucketAcl) (\$.eventName=PutBucketPolicy) (\$.eventName=PutBucketCors) (\$.eventName=PutBucketLifecycle) (\$.eventName=PutBucketReplication) (\$.eventName=DeleteBucketPolicy) (\$.eventName=DeleteBucketCors) (\$.eventName=DeleteBucketLi</pre>

欄位	Value
	<code>fecycle) (\$.eventName=DeleteBucketReplication))}</code>
指標命名空間	LogMetrics
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.9】確保 AWS Config 組態變更存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.9、CIS AWS Foundations Benchmark v1.4.0/4.9、NIST.800-171.r2 3.3.8、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config rule：None（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

您可以將 CloudTrail 日誌導向 CloudWatch Logs 並建立對應的指標篩選條件和警示，以即時監控 API 呼叫。

CIS 建議您為組態設定的變更 AWS Config 建立指標篩選條件和警示。監控這些變更有助於確保帳戶組態項目的持續可見性。

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.4.0](#) 版中針對控制項 4.9 指定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在 NO_DATA 下列情況下，檢查會導致 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的 帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生問題清單。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估 NO_DATA 的控制項，使用組織追蹤會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題 `ListSubscriptionsByTopic`。否則 Security Hub CSPM 會產生控制項的問題 WARNING 清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。
2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱AWS CloudTrail 《使用者指南》中的[建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《Amazon CloudWatch 使用者指南》中的[為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<code>{ (\$.eventSource=config.amazonaws.com) && ((\$.eventName=StopConfigurationRecorder) (\$.eventName=DeleteDeliveryChannel) (\$.eventName=PutDeliveryChannel) (\$.eventName=PutConfigurationRecorder)) }</code>
指標命名空間	LogMetrics
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態

欄位	Value
每當您 <i>your-metric-name</i> 為...	大於/等於
大於...	1

【CloudWatch.10】確保安全群組變更存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.10、CIS AWS Foundations Benchmark v1.4.0/4.10、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config rule：None（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

您可以將 CloudTrail 日誌導向 CloudWatch Logs 並建立對應的指標篩選條件和警示，以即時監控 API 呼叫。安全群組是控制 VPC 中輸入和輸出流量的狀態封包篩選條件。

CIS 建議您為安全群組的變更建立指標篩選條件和警示。監控這些變更有助於確保不會意外公開資源和服務。

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.4.0 版中針對控制項 4.10](#) 指定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。

檢查會在下列情況下產生FAILED問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在NO_DATA下列情況下，檢查會導致 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的 帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生調查結果。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估NO_DATA的控制項，使用組織追蹤會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題ListSubscriptionsByTopic。否則 Security Hub CSPM 會產生控制項的問題WARNING清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。
2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱AWS CloudTrail 《使用者指南》中的[建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《Amazon CloudWatch 使用者指南》中的[為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<code>{{(\$.eventName=AuthorizeSecurityGroupIngress) (\$.eventName=AuthorizeSecurityGroupEgress) (\$.eventName=RevokeSecurityGroupIngress) (\$.eventName=RevokeSecurityGroupEgress) (\$.eventName=CreateSecurityGroup) (\$.eventName>DeleteSecurityGroup)}}</code>
指標命名空間	LogMetrics
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.11】確定網路存取控制清單 (NACL) 的變更存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.11、CIS AWS Foundations Benchmark v1.4.0/4.11、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config 規則：無（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

您可以將 CloudTrail 日誌導向 CloudWatch Logs 並建立對應的指標篩選條件和警示，以即時監控 API 呼叫。NACL 做為無狀態封包篩選條件使用，可控制 VPC 中子網路的輸入和輸出流量。

CIS 建議您為 NACLs 的變更建立指標篩選條件和警示。監控這些變更有助於確保 AWS 資源和服務不會意外公開。

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.4.0 版中針對控制項 4.11](#) 指定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在 NO_DATA 下列情況下，檢查會導致 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的 帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生調查結果。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估 NO_DATA 的控制項，使用組織追蹤會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的

帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題 `ListSubscriptionsByTopic`。否則 Security Hub CSPM 會產生控制項的問題 `WARNING` 清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。
2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱 AWS CloudTrail 《使用者指南》中的 [建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《Amazon CloudWatch 使用者指南》中的 [為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<code>{{(\$.eventName>CreateNetworkAcl) (\$.eventName>CreateNetworkAclEntry) (\$.eventName>DeleteNetworkAcl) (\$.eventName>DeleteNetworkAclEntry) (\$.eventName=ReplaceNetworkAclEntry) (\$.eventName=ReplaceNetworkAclAssociation)}}</code>
指標命名空間	<code>LogMetrics</code>

欄位	Value
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.12】確保網路閘道變更存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.12、CIS AWS Foundations Benchmark v1.4.0/4.12、NIST.800-171.r2 3.3.1、NIST.800-171.r2 3.13.1

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config rule：None（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

您可以將 CloudTrail 日誌導向 CloudWatch Logs 並建立對應的指標篩選條件和警示，以即時監控 API 呼叫。需要有網路閘道才能在 VPC 外部的目標傳送和接收流量。

CIS 建議您為網路閘道的變更建立指標篩選條件和警示。監控這些變更有助於確保所有輸入和輸出流量透過控制路徑周遊 VPC 邊界。

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.2 版中針對控制項 4.12](#) 指定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在 NO_DATA 下列情況下，檢查會導致 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的 帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生調查結果。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估 NO_DATA 的控制項，使用組織追蹤會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題 ListSubscriptionsByTopic。否則 Security Hub CSPM 會產生控制項的問題 WARNING 清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。

2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱AWS CloudTrail 《使用者指南》中的[建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《Amazon CloudWatch 使用者指南》中的[為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<code>{ (\$.eventName=CreateCustomerGateway) (\$.eventName>DeleteCustomerGateway) (\$.eventName=AttachInternetGateway) (\$.eventName=CreateInternetGateway) (\$.eventName>DeleteInternetGateway) (\$.eventName=DetachInternetGateway)}</code>
指標命名空間	LogMetrics
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.13】確保路由表變更存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.13、CIS AWS Foundations Benchmark v1.4.0/4.13、NIST.800-171.r2 3.3.1、NIST.800-171.r2 3.13.1、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config 規則：無（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

此控制項會檢查您是否即時監控 API 呼叫，方法是將 CloudTrail 日誌導向 CloudWatch Logs，並建立對應的指標篩選條件和警示。路由表會在子網路間路由網路流量，並路由到網路閘道。

CIS 建議您為路由表的變更建立指標篩選條件和警示。監控這些變更有助於確保所有 VPC 流量流經預期的路徑。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。

檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在下列情況下，檢查會導致 NO_DATA 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生調查結果。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估 NO_DATA 的控制項，使用組織線索會導致 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題 ListSubscriptionsByTopic。否則 Security Hub CSPM 會產生控制項的問題 WARNING 清單。

修補

Note

我們在這些修復步驟中建議的篩選條件模式與 CIS 指引中的篩選條件模式不同。我們建議的篩選條件僅針對來自 Amazon Elastic Compute Cloud (EC2) API 呼叫的事件。

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。
2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱 AWS CloudTrail 《[使用者指南](#)》中的 [建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱《[Amazon CloudWatch 使用者指南](#)》中的 [為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<code>{ (\$.eventSource=ec2.amazonaws.com) && ((\$.eventName=CreateRoute) (\$.eventName=CreateRouteTable) (\$.eventName=ReplaceRoute) (\$.eventName=ReplaceRouteTableAssociation) (\$.eventName>DeleteRouteTable) (\$.eventName>DeleteRoute) (\$.eventName=DisassociateRouteTable)) }</code>
指標命名空間	LogMetrics
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.14】確保 VPC 變更存在日誌指標篩選條件和警示

相關要求：CIS AWS Foundations Benchmark v1.2.0/3.14、CIS AWS Foundations Benchmark v1.4.0/4.14、NIST.800-171.r2 3.3.1、NIST.800-171.r2 3.13.1、NIST.800-171.r2 3.14.6、NIST.800-171.r2 3.14.7

類別：偵測 > 偵測服務

嚴重性：低

資源類

型：AWS::Logs::MetricFilter、AWS::CloudWatch::Alarm、AWS::CloudTrail::Trail、AWS::SNS::Topic

AWS Config rule：None（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：無

您可以將 CloudTrail 日誌導向 CloudWatch Logs 並建立對應的指標篩選條件和警示，以即時監控 API 呼叫。一個帳戶可有多個 VPC，而您可在兩個 VPC 之間建立對等連線，在 VPC 之間路由網路流量。

CIS 建議您為 VPCs 的變更建立指標篩選條件和警示。監控這些變更有助於確保身分驗證和授權控制保持不變。

若要執行此檢查，Security Hub CSPM 會使用自訂邏輯來執行 [CIS AWS Foundations Benchmark 1.4.0 版中針對控制項 4.14](#) 指定的確切稽核步驟。如果未使用 CIS 所規定的確切指標篩選條件，此控制會失敗。無法將其他欄位或術語新增至指標篩選條件。

Note

當 Security Hub CSPM 執行此控制項的檢查時，它會尋找目前帳戶使用的 CloudTrail 追蹤。這些線索可能是屬於另一個帳戶的組織線索。多區域線索也可能位於不同的區域。檢查會在下列情況下產生 FAILED 問題清單：

- 未設定線索。
- 目前區域和目前帳戶擁有的可用線索不符合控制要求。

在下列情況下，檢查會導致 NO_DATA 的控制狀態：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生調查結果。

我們建議組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估 NO_DATA 的控制項，使用組織線索會導致 的控制狀態。在成員帳戶中，Security Hub

CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

對於警示，目前帳戶必須擁有參考的 Amazon SNS 主題，或必須呼叫 來存取 Amazon SNS 主題 `ListSubscriptionsByTopic`。否則 Security Hub CSPM 會產生控制項的問題 WARNING 清單。

修補

若要傳遞此控制項，請依照下列步驟建立 Amazon SNS 主題、AWS CloudTrail 線索、指標篩選條件，以及指標篩選條件的警示。

1. 建立 Amazon SNS 主題。如需說明，請參閱 [《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 入門](#)。建立接收所有 CIS 警示的主題，並建立至少一個主題訂閱。
2. 建立適用於所有的 CloudTrail 追蹤 AWS 區域。如需說明，請參閱 AWS CloudTrail [《使用者指南》中的 建立線索](#)。

請記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以在下一個步驟中為該日誌群組建立指標篩選條件。

3. 建立指標篩選條件。如需說明，請參閱 [《Amazon CloudWatch 使用者指南》中的 為日誌群組建立指標篩選條件](#)。使用下列的值：

欄位	Value
定義模式、篩選條件模式	<pre>{ (\$.eventName=CreateVpc) (\$.eventName>DeleteVpc) (\$.eventName=ModifyVpcAttribute) (\$.eventName=AcceptVpcPeeringConnection) (\$.eventName=CreateVpcPeeringConnection) (\$.eventName>DeleteVpcPeeringConnection) (\$.eventName=RejectVpcPeeringConnection) (\$.eventName=AttachClassicL</pre>

欄位	Value
	inkVpc) (\$.eventName=DetachClassicLinkVpc) (\$.eventName=DisableVpcClassicLink) (\$.eventName=EnableVpcClassicLink)}
指標命名空間	LogMetrics
指標值	1
預設值	0

4. 根據篩選條件建立警示。如需說明，請參閱《Amazon [CloudWatch 使用者指南](#)》中的[根據日誌群組指標篩選條件建立 CloudWatch 警示](#)。Amazon CloudWatch 使用下列的值：

欄位	Value
條件、閾值類型	靜態
每當您 <code>your-metric-name</code> 為...	大於/等於
大於...	1

【CloudWatch.15】CloudWatch 警示應已設定指定的動作

相關要求：NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 CA-7、NIST.800-53.r5 IR-4(1)、NIST.800-53.r5 IR-4(5)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-20、NIST.800-53.r5 SI-4(12)、NIST.800-53.r5 SI-4(5)、NIST.800-171.r2、NIST.40

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::CloudWatch::Alarm

AWS Config 規則：[cloudwatch-alarm-action-check](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
alarmActionRequired	如果 參數設定為 <code>true</code> 且警示狀態變更為 時有動作，則控制項會產生 PASSED 調查結果 ALARM。	Boolean	無法自訂	true
insufficientDataActionRequired	如果 參數設定為 <code>true</code> 且警示狀態變更為 時有動作，則控制項會產生 PASSED 問題清單 INSUFFICIENT_DATA。	Boolean	true 或 false *	false
okActionRequired	如果 參數設定為 <code>true</code> 且警示狀態變更為 時有動作，則控制項會產生 PASSED 問題清單 OK。	Boolean	true 或 false *	false

此控制項會檢查 Amazon CloudWatch 警示是否已針對 ALARM 狀態設定至少一個動作。如果警示未針對 ALARM 狀態設定動作，則控制項會失敗。或者，您可以包含自訂參數值，以同時需要 INSUFFICIENT_DATA 或 OK 狀態的警示動作。

Note

Security Hub CSPM 會根據 CloudWatch 指標警示評估此控制項。指標警示可能是已設定指定動作的複合警示的一部分。控制項會在下列情況下產生 FAILED 問題清單：

- 未針對指標警示設定指定的動作。
- 指標警示是已設定指定動作的複合警示的一部分。

此控制項著重於 CloudWatch 警示是否已設定警示動作，而 [CloudWatch.17](#) 則著重於 CloudWatch 警示動作的啟用狀態。

我們建議 CloudWatch 警示動作，以便在監控的指標超出定義的閾值時自動提醒您。監控警示可協助您識別異常活動，並在警示進入特定狀態時快速回應安全性和操作問題。最常見的警示動作類型是透過傳送訊息至 Amazon Simple Notification Service (Amazon SNS) 主題來通知一或多個使用者。

修補

如需有關 CloudWatch 警示支援之動作的資訊，請參閱《Amazon CloudWatch 使用者指南》中的[警示動作](#)。

【CloudWatch.16】CloudWatch 日誌群組應保留一段指定的時間

類別：識別 > 記錄日誌

相關要求：NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-11、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-12

嚴重性：中

資源類型：AWS::Logs::LogGroup

AWS Config 規則：[cw-loggroup-retention-period-check](#)

排程類型：定期

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
minRetentionTime	CloudWatch 日誌群組的最短保留期間，以天為單位	列舉	365, 400, 545, 731, 1827, 3653	365

此控制項會檢查 Amazon CloudWatch 日誌群組是否具有至少指定天數的保留期間。如果保留期間小於指定的數字，則控制項會失敗。除非您提供保留期間的自訂參數值，否則 Security Hub CSPM 會使用預設值 365 天。

CloudWatch Logs 會將所有系統、應用程式和 的日誌集中在單一、高度可擴展的服務 AWS 服務 中。您可以使用 CloudWatch Logs 從 Amazon Elastic Compute Cloud (EC2) 執行個體、Amazon Route 53 和其他來源監控 AWS CloudTrail、存放和存取您的日誌檔案。保留日誌至少 1 年可協助您符合日誌保留標準。

修補

若要設定日誌保留設定，請參閱《Amazon [CloudWatch 使用者指南](#)》中的在 [CloudWatch Logs 中變更日誌資料保留](#)。Amazon CloudWatch

【CloudWatch.17】應啟用 CloudWatch 警示動作

類別：偵測 > 偵測服務

相關需求：NIST.800-53.r5 AU-6(1)、NIST.800-53.r5 AU-6(5)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-4(12)

嚴重性：高

資源類型：AWS::CloudWatch::Alarm

AWS Config 規則：[cloudwatch-alarm-action-enabled-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 CloudWatch 警示動作是否已啟用 (ActionEnabled 應設為 true)。如果 CloudWatch 警示的警示動作已停用，則控制項會失敗。

Note

Security Hub CSPM 會根據 CloudWatch 指標警示評估此控制項。指標警示可能是啟用警示動作的複合警示的一部分。控制項會在下列情況下產生 FAILED 問題清單：

- 未針對指標警示設定指定的動作。
- 指標警示是已啟用警示動作的複合警示的一部分。

此控制項著重於 CloudWatch 警示動作的啟用狀態，而 [CloudWatch.15](#) 則著重於 CloudWatch 警示中是否設定任何 ALARM 動作。

當受監控的指標超出定義的閾值時，警示動作會自動提醒您。如果警示動作已停用，則警示變更狀態時不會執行任何動作，而且您不會收到監控指標變更的提醒。我們建議您啟用 CloudWatch 警示動作，以協助您快速回應安全性和操作問題。

修補

啟用 CloudWatch 警示動作（主控台）

1. 透過 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 在導覽窗格中的警示下，選擇所有警示。
3. 選取您要為其啟用動作的警示。
4. 針對動作，選擇警示動作-新，然後選擇啟用。

如需啟用 CloudWatch 警示動作的詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的[警示動作](#)。

CodeArtifact 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 AWS CodeArtifact 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::CodeArtifact::Repository

AWS Config rule：tagged-codeartifact-repository（自訂 Security Hub CSPM 規則）

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS CodeArtifact 儲存庫是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果儲存庫沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果儲存庫未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《[標記您的 AWS 資源](#)》中的 [標記您的 AWS 資源](#) 一般參考。

修補

若要將標籤新增至 CodeArtifact 儲存庫，請參閱 AWS CodeArtifact 《[使用者指南](#)》中的 [在 CodeArtifact 中標記儲存庫](#)。

CodeBuild 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 AWS CodeBuild 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料

相關要求：NIST.800-53.r5 SA-3、PCI DSS v3.2.1/8.2.1、PCI DSS v4.0.1/8.3.2

類別：保護 > 安全開發

嚴重性：嚴重

資源類型：AWS::CodeBuild::Project

AWS Config 規則：[codebuild-project-source-repo-url-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS CodeBuild 專案 Bitbucket 來源儲存庫 URL 是否包含個人存取字符或使用者名稱和密碼。如果 Bitbucket 來源儲存庫 URL 包含個人存取字符或使用者名稱和密碼，則控制項會失敗。

Note

此控制項會評估 CodeBuild 組建專案的主要來源和次要來源。如需專案來源的詳細資訊，請參閱AWS CodeBuild 《使用者指南》中的[多個輸入來源和輸出成品範例](#)。

登入憑證不應以純文字形式儲存或傳輸，也不應出現在來源儲存庫 URL 中。您應該在 CodeBuild 中存取來源提供者，並將來源儲存庫 URL 變更為僅包含 Bitbucket 儲存庫位置的路徑，而不是個人存取字符或登入憑證。使用個人存取字符或登入憑證可能會導致意外的資料暴露或未經授權的存取。

修補

您可以更新您的 CodeBuild 專案以使用 OAuth。

從 CodeBuild 專案來源移除基本身分驗證/(GitHub) 個人存取字符

1. 前往 <https://console.aws.amazon.com/codebuild/> 開啟 CodeBuild 主控台。
2. 選擇包含個人存取字符或使用者名稱及密碼的建置專案。
3. 從 Edit (編輯) 中，選擇 Source (來源)。
4. 選擇 Disconnect from GitHub / Bitbucket (從 GitHub / Bitbucket 中斷連線)。
5. 選擇 Connect using OAuth (使用 OAuth 連線)，然後選擇 Connect to GitHub / Bitbucket (連線至 GitHub / Bitbucket)。

6. 出現提示時，選擇 `authorize as appropriate` (適當授權)。
7. 視需要重新設定您的儲存庫 URL 和其他組態設定。
8. 選擇 `Update source` (更新來源)。

如需詳細資訊，請參閱AWS CodeBuild 《使用者指南》中的 [CodeBuild 使用案例型範例](#)。

【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料

相關要求：NIST.800-53.r5 IA-5(7)、NIST.800-53.r5 SA-3、PCI DSS v3.2.1/8.2.1、PCI DSS v4.0.1/8.3.2

類別：保護 > 安全開發

嚴重性：嚴重

資源類型：AWS::CodeBuild::Project

AWS Config 規則：[codebuild-project-envvar-awscred-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查專案是否包含環境變數 `AWS_ACCESS_KEY_ID` 和 `AWS_SECRET_ACCESS_KEY`。

身分驗證登入資料 `AWS_ACCESS_KEY_ID` 和 `AWS_SECRET_ACCESS_KEY` 永遠不應以純文字形式存放，應該這可能會意外公開資料或使其受到未經授權的存取。

修補

若要從 CodeBuild 專案中移除環境變數，請參閱AWS CodeBuild 《使用者指南》中的在 [中變更建置專案的設定 AWS CodeBuild](#)。確保未為環境變數選取任何項目。

您可以將具有敏感值的環境變數存放在 AWS Systems Manager 參數存放區或中，AWS Secrets Manager 然後從建置規格中擷取它們。如需說明，請參閱AWS CodeBuild 《使用者指南》中[環境區段](#)中標記為重要 的方塊。

【CodeBuild.3】CodeBuild S3 日誌應加密

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)、PCI DSS v4.0.1/10.3.2

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：低

資源類型：AWS::CodeBuild::Project

AWS Config 規則：[codebuild-project-s3-logs-encrypted](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS CodeBuild 專案的 Amazon S3 日誌是否已加密。如果 CodeBuild 專案的 S3 日誌停用加密，則控制項會失敗。

加密靜態資料是為資料新增一層存取管理的建議最佳實務。加密靜態日誌可降低使用者未經驗證 AWS 將存取磁碟上存放之資料的風險。它新增了另一組存取控制，以限制未經授權的使用者存取資料的能力。

修補

若要變更 CodeBuild 專案 S3 日誌的加密設定，請參閱AWS CodeBuild 《使用者指南》中的在 [中變更建置專案的設定 AWS CodeBuild](#)。

【CodeBuild.4】CodeBuild AWS Config專案環境應具有記錄 URL

相關需求：NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.8000-5.r5)、AU-6NIST.5 AU-9 CA-7 NIST.800-53.r5 SC-7 SI-3 SI-4 SI-7

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::CodeBuild::Project

AWS Config 規則：[codebuild-project-logging-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 CodeBuild 專案環境是否已啟用至少一個日誌選項，包括 S3 或 CloudWatch 日誌。如果 CodeBuild 專案環境未啟用至少一個日誌選項，則此控制項會失敗。

從安全角度來看，記錄是一項重要功能，可在發生任何安全事件時，為未來的鑑識工作提供支援。將 CodeBuild 專案中的異常與威脅偵測相關聯，可以提高對這些威脅偵測準確性的信心。

修補

如需如何設定 CodeBuild 專案日誌設定的詳細資訊，請參閱 CodeBuild 使用者指南中的[建立建置專案 \(主控台\)](#)。

【CodeBuild.5】CodeBuild 專案環境不應啟用特權模式

Important

Security Hub CSPM 已於 2024 年 4 月淘汰此控制項。如需詳細資訊，請參閱[Security Hub CSPM 控制項的變更日誌](#)。

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2)

類別：保護 > 安全存取管理

嚴重性：高

資源類型：AWS::CodeBuild::Project

AWS Config 規則：[codebuild-project-environment-privileged-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS CodeBuild 專案環境是否已啟用或停用特權模式。如果 CodeBuild 專案環境已啟用特殊權限模式，則控制項會失敗。

根據預設，Docker 容器不允許存取任何裝置。「Privileged」(特殊權限) 模式會授予建置專案之 Docker 容器對所有裝置的存取權。privilegedMode 使用值設定 true 可讓 Docker 協助程式在 Docker 容器內執行。Docker 協助程式會監聽 Docker API 請求，並管理 Docker 物件，例如映像、容器、網路和磁碟區。只有在建置專案用於建置 Docker 映像時，此參數才應該設定為 true。否則，應停用此設定，以防止意外存取 Docker APIs 和容器的基礎硬體。privilegedMode 將設定為 false 有助於保護關鍵資源免於遭到竄改和刪除。

修補

若要設定 CodeBuild 專案環境設定，請參閱 CodeBuild 使用者指南中的[建立建置專案（主控台）](#)。在環境區段中，不要選取特殊權限設定。

【CodeBuild.7】CodeBuild 報告群組匯出應靜態加密

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::CodeBuild::ReportGroup

AWS Config 規則：[codebuild-report-group-encrypted-at-rest](#)

排程類型：已觸發變更

參數：無

此控制項會檢查匯出至 Amazon Simple Storage Service (Amazon S3) 儲存貯體的報告 AWS CodeBuild 群組測試結果是否靜態加密。如果報告群組匯出未靜態加密，則控制項會失敗。

靜態資料是指存放在持久性、非揮發性儲存體中任何持續時間的資料。加密靜態資料可協助您保護其機密性，進而降低未經授權的使用者可存取資料的風險。

修補

若要加密匯出至 S3 的報告群組，請參閱AWS CodeBuild 《使用者指南》中的[更新報告群組](#)。

Amazon CodeGuru Profiler 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 Amazon CodeGuru Profiler 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::CodeGuruProfiler::ProfilingGroup

AWS Config 規則：codeguruprofiler-profiling-group-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon CodeGuru Profiler 分析群組是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果分析群組沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果分析群組未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 CodeGuru Profiler 分析群組，請參閱《Amazon CodeGuru Profiler 使用者指南》中的 [標記分析群組](#)。

Amazon CodeGuru Reviewer 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 Amazon CodeGuru Reviewer 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::CodeGuruReviewer::RepositoryAssociation

AWS Config 規則：codegurureviewer-repository-association-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon CodeGuru Reviewer 儲存庫關聯是否具有與參數中定義之特定金鑰的標籤 requiredKeyTags。如果儲存庫關聯沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果儲存庫關聯未標記任何索引鍵，則會失敗。系統會 aws: 忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 CodeGuru Reviewer 儲存庫關聯，請參閱《Amazon CodeGuru Reviewer 使用者指南》中的[標記儲存庫關聯](#)。

Amazon Cognito 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Cognito 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Cognito.1】 Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::Cognito::UserPool

AWS Config 規則：[cognito-user-pool-advanced-security-enabled](#)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
SecurityMode	控制項檢查的威脅防護強制執行模式。	String	AUDIT, ENFORCED	ENFORCED

此控制項會檢查 Amazon Cognito 使用者集區是否已啟用威脅防護，並將強制執行模式設定為標準身分驗證的完整函數。如果使用者集區已停用威脅防護，或強制執行模式未設定為標準身分驗證的完整函數，則控制項會失敗。除非您提供自訂參數值，否則 Security Hub CSPM 會將強制執行模式的預設值 ENFORCED 設為標準身分驗證的完整函數。

建立 Amazon Cognito 使用者集區後，您可以啟用威脅防護，並自訂為了回應不同風險而採取的動作。或者，您可以使用稽核模式來收集偵測到風險的指標，而無需套用任何安全性緩解措施。在稽核模式中，威脅防護會將指標發佈至 Amazon CloudWatch。您可以在 Amazon Cognito 產生第一個事件後看到指標。

修補

如需有關啟用 Amazon Cognito 使用者集區威脅防護的資訊，請參閱《Amazon Cognito 開發人員指南》中的進階[安全性與威脅防護](#)。

【Cognito.2】 Cognito 身分集區不應允許未驗證的身分

類別：保護 > 安全存取管理 > 無密碼身分驗證

嚴重性：中

資源類型：AWS::Cognito::IdentityPool

AWS Config 規則：[cognito-identity-pool-unauth-access-check](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon Cognito 身分集區是否設定為允許未驗證的身分。如果身分集區的訪客存取已啟用 (AllowUnauthenticatedIdentities 參數設定為 true)，則控制項會失敗。

如果 Amazon Cognito 身分集區允許未驗證的身分，則身分集區會提供臨時 AWS 憑證給未透過身分提供者（訪客）驗證的使用者。這會產生安全風險，因為它允許匿名存取 AWS 資源。如果您停用訪客存取，您可以協助確保只有經過適當驗證的使用者才能存取您的 AWS 資源，進而降低未經授權的存取和潛在安全漏洞的風險。最佳實務是，身分集區應要求透過支援的身分提供者進行身分驗證。如果需要未經驗證的存取，請務必謹慎限制未經驗證身分的許可，並定期檢閱和監控其使用情況。

修補

如需有關停用 Amazon Cognito 身分集區訪客存取權的資訊，請參閱《Amazon Cognito 開發人員指南》中的[啟用或停用訪客存取權](#)。

【Cognito.3】 Cognito 使用者集區的密碼政策應具有強大的組態

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::Cognito::UserPool

AWS Config 規則：[cognito-user-pool-password-policy-check](#)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
minLength	密碼必須包含的字元數下限。	Integer	8 至 128	8
requireLowercase	密碼中至少需要一個小寫字元。	Boolean	True, False	True
requireUppercase	密碼中至少需要一個大寫字元。	Boolean	True, False	True
requireNumbers	密碼中至少需要一個數字。	Boolean	True, False	True
requireSymbols	密碼中至少需要一個符號。	Boolean	True, False	True
temporaryPasswordValidity	密碼過期前可存在的天數上限。	Integer	1 至 365	7

此控制項會根據建議的密碼政策設定，檢查 Amazon Cognito 使用者集區的密碼政策是否需要使用強式密碼。如果使用者集區的密碼政策不需要強式密碼，則控制項會失敗。您可以選擇性地為控制項檢查的政策設定指定自訂值。

強式密碼是 Amazon Cognito 使用者集區的安全最佳實務。較弱的密碼可能會將使用者的登入資料公開給猜測密碼並嘗試存取資料的系統。對於開放給網際網路的應用程式來說尤其如此。密碼政策是使用者目錄安全性的中心元素。透過使用密碼政策，您可以設定使用者集區來要求密碼複雜性和其他符合您安全標準和需求的設定。

修補

如需有關建立或更新 Amazon Cognito 使用者集區密碼政策的資訊，請參閱《Amazon Cognito 開發人員指南》中的[新增使用者集區密碼需求](#)。

【Cognito.4】 Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::Cognito::UserPool

AWS Config 規則：[cognito-userpool-cust-auth-threat-full-check](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon Cognito 使用者集區是否已啟用威脅防護，並將強制執行模式設定為自訂身分驗證的完整函數。如果使用者集區已停用威脅防護，或者如果強制執行模式未設定為自訂身分驗證的完整函數，則控制項會失敗。

威脅防護先前稱為進階安全功能，是一組用於使用者集區中不需要活動的監控工具，以及用於自動關閉潛在惡意活動的組態工具。建立 Amazon Cognito 使用者集區後，您可以使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證，並自訂為了因應不同風險而採取的動作。全功能模式包含一組自動反應，用於偵測不需要的活動和洩露的密碼。

修補

如需有關啟用 Amazon Cognito 使用者集區威脅防護的資訊，請參閱《Amazon Cognito 開發人員指南》中的進階[安全性與威脅防護](#)。

【Cognito.5】 應為 Cognito 使用者集區啟用 MFA

類別：保護 > 安全存取管理 > 多重要素驗證

嚴重性：中

資源類型：AWS::Cognito::UserPool

AWS Config 規則：[cognito-user-pool-mfa-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查以僅限密碼登入政策設定的 Amazon Cognito 使用者集區是否已啟用多重要素驗證 (MFA)。如果設定僅密碼登入政策的使用者集區未啟用 MFA，則控制項會失敗。

多重要素驗證 (MFA) 會將您擁有的身分驗證要素新增至您知道的要素（通常是使用者名稱和密碼）。對於聯合身分使用者，Amazon Cognito 會將身分驗證委派給身分提供者 (IdP)，且不提供額外的身分

驗證因素。不過，如果您有具有密碼身分驗證的本機使用者，則設定使用者集區的 MFA 會增加其安全性。

 Note

此控制項不適用於聯合身分使用者和使用無密碼因素登入的使用者。

修補

如需有關如何為 Amazon Cognito 使用者集區設定 MFA 的資訊，請參閱《Amazon Cognito 開發人員指南》中的[將 MFA 新增至使用者集區](#)。

【Cognito.6】 Cognito 使用者集區應啟用刪除保護

類別：保護 > 資料保護 > 資料刪除保護

嚴重性：中

資源類型：AWS::Cognito::UserPool

AWS Config 規則：[cognito-user-pool-deletion-protection-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon Cognito 使用者集區是否已啟用刪除保護。如果使用者集區的刪除保護已停用，則控制項會失敗。

刪除保護有助於確保您的使用者集區不會意外刪除。當您設定具有刪除保護的使用者集區時，任何使用者都無法刪除集區。刪除保護可防止您請求刪除使用者集區，除非您先修改集區並停用刪除保護。

修補

若要設定 Amazon Cognito 使用者集區的刪除保護，請參閱《Amazon Cognito 開發人員指南》中的[使用者集區刪除保護](#)。

的 Security Hub CSPM 控制項 AWS Config

這些 Security Hub CSPM 控制項會評估 AWS Config 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Config.1】 AWS Config 應啟用並使用服務連結角色進行資源記錄

相關要求：CIS AWS Foundations Benchmark v5.0.0/3.3、CIS AWS Foundations Benchmark v1.2.0/2.5、CIS AWS Foundations Benchmark v1.4.0/3.5、CIS AWS Foundations Benchmark v3.0.0/3.3、NIST.800-53.r5 CM-3、NIST.800-53.r5 CM-6(1)、NIST.800-53.r5 CM-8、NIST.800-53.r5 CM-8(2)、PCI v3.2.1/10.5.2、PCI v3.2.1/1.5.5

類別：識別 > 清查

嚴重性：嚴重

資源類型：AWS::::Account

AWS Config 規則：無（自訂 Security Hub CSPM 規則）

排程類型：定期

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
includeConfigServiceLinkedRoleCheck	如果參數設定為 <code>true</code> ，則控制項不會評估是否 AWS Config 使用服務連結角色 <code>false</code> 。	Boolean	true 或 false *	true

此控制項 AWS Config 會檢查您的帳戶是否在目前中啟用 AWS 區域、記錄與目前區域中啟用的控制項對應的所有資源，並使用 [服務連結 AWS Config 角色](#)。服務連結角色的名稱為 `AWSServiceRoleForConfig`。如果您不使用服務連結角色，且未將 `includeConfigServiceLinkedRoleCheck` 參數設定為 `false`，則控制項會失敗，因為其他角色可能沒有必要許可 AWS Config 讓準確記錄您的資源。

AWS Config 服務會對您帳戶中支援 AWS 的資源執行組態管理，並交付日誌檔案給您。記錄的資訊包括組態項目 (AWS 資源)、組態項目之間的關係，以及資源內的任何組態變更。全域資源是可在任何區域中使用的資源。

控制項的評估方式如下：

- 如果目前區域設定為[彙總區域](#)，則控制項只會在記錄 AWS Identity and Access Management (IAM) 全域資源時產生PASSED調查結果（如果您已啟用需要它們的控制項）。
- 如果目前區域設定為連結的區域，則控制項不會評估是否記錄 IAM 全域資源。
- 如果目前區域不在彙總工具中，或者您的帳戶中未設定跨區域彙總，則只有在記錄 IAM 全域資源時（如果您已啟用需要它們的控制項），控制項才會產生PASSED調查結果。

無論您選擇每日還是持續記錄資源狀態的變更，控制結果都不會受到影響 AWS Config。不過，如果您已設定自動啟用新控制項，或具有自動啟用新控制項的中央組態政策，則發佈新控制項時，此控制項的結果可能會變更。在這些情況下，如果您未記錄所有資源，您必須為與新控制項相關聯的資源設定記錄，才能接收PASSED問題清單。

Security Hub CSPM 安全檢查只有在您在 AWS Config 所有區域中啟用 並為需要它的控制項設定資源記錄時，才能如預期運作。

Note

Config.1 AWS Config 要求在您使用 Security Hub CSPM 的所有區域中啟用。

由於 Security Hub CSPM 是區域服務，因此針對此控制項執行的檢查只會評估帳戶的目前區域。

若要允許對區域中的 IAM 全域資源進行安全檢查，您必須在該區域中記錄 IAM 全域資源。未記錄 IAM 全域資源的區域會收到檢查 IAM 全域資源之控制項的預設PASSED調查結果。由於 IAM 全域資源在各個區域之間都相同 AWS 區域，因此建議您僅在主要區域記錄 IAM 全域資源（如果您的帳戶已啟用跨區域彙總）。IAM 資源只會記錄在開啟全域資源記錄的區域中。

AWS Config 支援的 IAM 全域記錄資源類型是 IAM 使用者、群組、角色和客戶受管政策。您可以考慮停用 Security Hub CSPM 控制項，在關閉全域資源記錄的區域中檢查這些資源類型。如需詳細資訊，請參閱[在 Security Hub CSPM 中停用的建議控制項](#)。

修補

在不屬於彙總工具的主區域和區域中，記錄目前區域中啟用之控制項所需的所有資源，如果您已啟用需要 IAM 全域資源的控制項，則包括 IAM 全域資源。

在連結的區域中，只要您要記錄與目前區域中啟用的控制項對應的所有資源，就可以使用任何 AWS Config 錄製模式。在連結區域中，如果您已啟用需要記錄 IAM 全域資源的控制項，則不會收到FAILED調查結果（其他資源的記錄就足夠）。

問題清單Compliance物件中的 StatusReasons 欄位可協助您判斷為什麼此控制項的問題清單失敗。如需詳細資訊，請參閱[控制問題清單的合規詳細資訊](#)。

如需每個控制項必須記錄哪些資源的清單，請參閱 [控制問題清單所需的 AWS Config 資源](#)。如需啟用 AWS Config 和設定資源錄製的一般資訊，請參閱 [啟用和設定 AWS Config Security Hub CSPM](#)。

Amazon Connect 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 Amazon Connect 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::CustomerProfiles::ObjectType

AWS Config 規則：customerprofiles-object-type-tagged

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon Connect Customer Profiles 物件類型是否具有具有參數中定義之特定金鑰的標籤requiredKeyTags。如果物件類型沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗requiredKeyTags。如果requiredKeyTags未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果物件類型未標記任何索引鍵，則會失敗。系統會aws:忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知

的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至客戶設定檔物件類型，請參閱 Connect Customer 管理員指南中的[將標籤新增至 Amazon Connect Customer 中的資源](#)。

【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::Connect::Instance

AWS Config 規則：[connect-instance-logging-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Connect Customer 執行個體是否已設定為在 Amazon CloudWatch 日誌群組中產生和存放流程日誌。如果 Connect Customer 執行個體未設定為在 CloudWatch 日誌群組中產生和存放流程日誌，則控制項會失敗。

Amazon Connect Customer 流程日誌提供 Amazon Connect Customer 流程中事件的即時詳細資訊。流程定義了 Amazon Connect Customer 聯絡中心從頭到尾的客戶體驗。根據預設，當您建立新的 Amazon Connect Customer 執行個體時，會自動建立 Amazon CloudWatch 日誌群組，以存放執行個體的流程日誌。流程日誌可協助您分析流程、尋找錯誤，以及監控操作指標。您也可以為流程中可能發生的特定事件設定提醒。

修補

如需有關為 Amazon Connect Customer 執行個體啟用流程日誌的資訊，請參閱 [Amazon Connect Customer 管理員指南中的在 Amazon CloudWatch 日誌群組中啟用 Amazon Connect Customer 流程日誌](#)。

Amazon Data Firehose 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 Amazon Data Firehose 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【DataFirehose.1】Firehose 交付串流應靜態加密

相關需求：NIST.800-53.r5 AC-3、NIST.800-53.r5 AU-3、NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::KinesisFirehose::DeliveryStream

AWS Config 規則：[kinesis-firehose-delivery-stream-encrypted](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon Data Firehose 交付串流是否使用伺服器端加密進行靜態加密。如果 Firehose 交付串流未使用伺服器端加密進行靜態加密，則此控制會失敗。

伺服器端加密是 Amazon Data Firehose 交付串流的一項功能，使用在 AWS Key Management Service () 中建立的金鑰，在資料處於靜態狀態之前自動加密資料AWS KMS。資料會在寫入 Data Firehose 串流儲存層之前加密，並在從儲存體擷取後解密。這可讓您遵守法規要求，並增強資料的安全性。

修補

若要在 Firehose 交付串流上啟用伺服器端加密，請參閱 [《Amazon Data Firehose 開發人員指南》中的 Amazon Data Firehose](#) 中的資料保護。

的 Security Hub CSPM 控制項 AWS Database Migration Service

這些 AWS Security Hub CSPM 控制項會評估 AWS Database Migration Service (AWS DMS) AWS DMS 和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【DMS.1】 Database Migration Service 複寫執行個體不應為公有

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：AWS::DMS::ReplicationInstance

AWS Config 規則：[dms-replication-not-public](#)

排程類型：定期

參數：無

此控制項會檢查 AWS DMS 複寫執行個體是否為公有。若要這樣做，它會檢查 PubliclyAccessible 欄位的值。

私有複寫執行個體具有您無法在複寫網路外部存取的私有 IP 地址。當來源和目標資料庫位於相同網路時，複寫執行個體應具有私有 IP 地址。網路也必須使用 VPN Direct Connect 或 VPC 對等互連連線至複寫執行個體的 VPC。若要進一步了解公有和私有複寫執行個體，請參閱 AWS Database Migration Service 《使用者指南》中的[公有和私有複寫執行個體](#)。

您也應該確保僅授權使用者才能存取 AWS DMS 執行個體組態。若要這樣做，請限制使用者的 IAM 許可來修改 AWS DMS 設定和資源。

修補

您無法在建立 DMS 複寫執行個體之後變更其公有存取設定。若要變更公有存取設定，請[刪除您目前的執行個體](#)，然後[重新建立它](#)。請勿選取可公開存取選項。

【DMS.2】 DMS 憑證應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::DMS::Certificate

AWS Config rule：tagged-dms-certificate (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	No default value

此控制項會檢查 AWS DMS 憑證是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果憑證沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤金鑰是否存在，如果憑證未標記任何金鑰，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#)AWS 一般參考。

修補

若要將標籤新增至 DMS 憑證，請參閱AWS Database Migration Service 《使用者指南》中的在 [中標記資源 AWS Database Migration Service](#)。

【DMS.3】 DMS 事件訂閱應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::DMS::EventSubscription

AWS Config rule：tagged-dms-eventsubscription (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS DMS 事件訂閱是否具有具有參數 中定義之特定金鑰的標籤

requiredTagKeys。如果事件訂閱沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果事件訂閱未加上任何索引鍵的標籤，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 DMS 事件訂閱，請參閱AWS Database Migration Service 《使用者指南》中的在[中標記資源 AWS Database Migration Service](#)。

【DMS.4】 DMS 複寫執行個體應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::DMS::ReplicationInstance

AWS Config rule：tagged-dms-replicationinstance (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS DMS 複寫執行個體是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果複寫執行個體沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果複寫執行個體未標記任何索引鍵，則 控制會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 DMS 複寫執行個體，請參閱AWS Database Migration Service 《使用者指南》中的在 [中標記資源 AWS Database Migration Service](#)。

【DMS.5】 DMS 複寫子網路群組應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::DMS::ReplicationSubnetGroup

AWS Config rule：tagged-dms-replicationsubnetgroup (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS DMS 複寫子網路群組是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果複寫子網路群組沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果複寫子網路群組未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#)一般參考。

修補

若要將標籤新增至 DMS 複寫子網路群組，請參閱 AWS Database Migration Service 《使用者指南》中的在 [中標記資源 AWS Database Migration Service](#)。

【DMS.6】DMS 複寫執行個體應啟用自動次要版本升級

相關要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：AWS::DMS::ReplicationInstance

AWS Config 規則：[dms-auto-minor-version-upgrade-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查複 AWS DMS 寫執行個體是否已啟用自動次要版本升級。如果未針對 DMS 複寫執行個體啟用自動次要版本升級，則控制項會失敗。

DMS 提供每個支援的複寫引擎的自動次要版本升級，讓您可以將複寫執行個體保持在 up-to-date。次要版本可以引進新的軟體功能、錯誤修正、安全性修補程式和效能改善。透過在 DMS 複寫執行個體上

啟用自動次要版本升級，次要升級會在維護時段期間自動套用，或在選擇立即套用變更選項時立即套用。

修補

若要在 DMS 複寫執行個體上啟用自動次要版本升級，請參閱AWS Database Migration Service 《使用者指南》中的[修改複寫執行個體](#)。

【DMS.7】目標資料庫的 DMS 複寫任務應該已啟用記錄

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.4.2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::DMS::ReplicationTask

AWS Config 規則：[dms-replication-task-targetdb-logging](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否以 DMS LOGGER_SEVERITY_DEFAULT 複寫任務和 的最低嚴重性層級啟用記錄TARGET_APPLYTARGET_LOAD。如果未針對這些任務啟用記錄，或如果最低嚴重性等級小於，則控制項會失敗LOGGER_SEVERITY_DEFAULT。

DMS 使用 Amazon CloudWatch 在遷移程序期間記錄資訊。使用記錄任務設定，您可以指定記錄哪些元件活動，以及記錄多少資訊。您應該為下列任務指定記錄：

- TARGET_APPLY – 將資料和資料定義語言 (DDL) 陳述式套用到目標資料庫。
- TARGET_LOAD – 將資料載入目標資料庫。

記錄透過啟用監控、疑難排解、稽核、效能分析、錯誤偵測和復原，以及歷史分析和報告，在 DMS 複寫任務中扮演重要角色。它有助於確保資料庫之間的資料成功複寫，同時保持資料完整性並符合法規要求。在疑難排解期間，這些元件很少需要 DEFAULT 以外的日誌記錄層級。我們建議將這些元件的記錄層級維持為 DEFAULT，除非特別要求變更支援。最低的記錄層級DEFAULT可確保資訊性訊息、警告和錯誤訊息寫入日誌。此控制項會檢查上述複寫任務的記錄

層級是否至少為下列其中一項：LOGGER_SEVERITY_DEFAULT、LOGGER_SEVERITY_DEBUG或LOGGER_SEVERITY_DETAILED_DEBUG。

修補

若要啟用目標資料庫 DMS 複寫任務的記錄，請參閱AWS Database Migration Service 《使用者指南》中的[檢視和管理 AWS DMS 任務日誌](#)。

【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.4.2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::DMS::ReplicationTask

AWS Config 規則：[dms-replication-task-sourcedb-logging](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否以 DMS LOGGER_SEVERITY_DEFAULT 複寫任務和 的最低嚴重性層級啟用記錄SOURCE_CAPTURESOURCE_UNLOAD。如果未針對這些任務啟用記錄，或如果最低嚴重性等級小於，則控制項會失敗LOGGER_SEVERITY_DEFAULT。

DMS 使用 Amazon CloudWatch 在遷移程序期間記錄資訊。使用記錄任務設定，您可以指定記錄哪些元件活動，以及記錄多少資訊。您應該為下列任務指定記錄：

- SOURCE_CAPTURE – 持續複寫或變更資料擷取 (CDC) 資料會從來源資料庫或服務擷取，並傳遞至SORTER服務元件。
- SOURCE_UNLOAD – 資料會在完全載入期間從來源資料庫或服務卸載。

記錄透過啟用監控、疑難排解、稽核、效能分析、錯誤偵測和復原，以及歷史分析和報告，在 DMS 複寫任務中扮演重要角色。它有助於確保資料庫之間的資料成功複寫，同時保持資料完整性並符合法規要求。在疑難排解期間，這些元件很少需要 DEFAULT 以外的日誌記錄層級。

我們建議將這些元件的記錄層級維持為 DEFAULT，除非 特別要求變更 支援。最低的記錄層級 DEFAULT 可確保資訊性訊息、警告和錯誤訊息寫入日誌。此控制項會檢查上述複寫任務的記錄層級是否至少為下列其中一項：LOGGER_SEVERITY_DEFAULT、LOGGER_SEVERITY_DEBUG 或 LOGGER_SEVERITY_DETAILED_DEBUG。

修補

若要啟用來源資料庫 DMS 複寫任務的記錄，請參閱 AWS Database Migration Service 《使用者指南》中的 [檢視和管理 AWS DMS 任務日誌](#)。

【DMS.9】 DMS 端點應使用 SSL

相關要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、PCI DSS v4.0.1/4.2.1

類別：保護 > 資料保護 > data-in-transit

嚴重性：中

資源類型：AWS::DMS::Endpoint

AWS Config 規則：[dms-endpoint-ssl-configured](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS DMS 端點是否使用 SSL 連線。如果端點不使用 SSL，則控制項會失敗。

SSL/TLS 連線透過加密 DMS 複寫執行個體和資料庫之間的連線，提供一層安全性。使用憑證可驗證是否與預期的資料庫建立連線，藉此提供額外的安全層。它透過檢查自動安裝在您佈建的所有資料庫執行個體上的伺服器憑證來執行此操作。透過在 DMS 端點上啟用 SSL 連線，您可以在遷移期間保護資料的機密性。

修補

若要將 SSL 連線新增至新的或現有的 DMS 端點，請參閱 AWS Database Migration Service 《使用者指南》中的 [搭配使用 SSL AWS Database Migration Service](#)。

【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權

相關要求：NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-17、NIST.800-53.r5 IA-2、NIST.800-53.r5 IA-5、PCI DSS v4.0.1/7.3.1

類別：保護 > 安全存取管理 > 無密碼身分驗證

嚴重性：中

資源類型：AWS::DMS::Endpoint

AWS Config 規則：[dms-neptune-iam-authorization-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Neptune 資料庫的 AWS DMS 端點是否已設定 IAM 授權。如果 DMS 端點未啟用 IAM 授權，則控制項會失敗。

AWS Identity and Access Management (IAM) 提供跨 的精細存取控制 AWS。透過 IAM，您可以指定誰可以存取哪些 服務和資源，以及在哪些條件下。使用 IAM 政策，您可以管理人力資源和系統的許可，以確保最低權限許可。透過在 Neptune 資料庫的 AWS DMS 端點上啟用 IAM 授權，您可以使用 ServiceAccessRoleARN 參數指定的服務角色，將授權權限授予 IAM 使用者。

修補

若要在 Neptune 資料庫的 DMS 端點上啟用 IAM 授權，請參閱AWS Database Migration Service 《使用者指南》中的[使用 Amazon Neptune 作為的目標 AWS Database Migration Service](#)。

【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制

相關要求：NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-6、NIST.800-53.r5 IA-2、NIST.800-53.r5 IA-5、PCI DSS v4.0.1/7.3.1

類別：保護 > 安全存取管理 > 無密碼身分驗證

嚴重性：中

資源類型：AWS::DMS::Endpoint

AWS Config 規則：[dms-mongo-db-authentication-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 MongoDB 的 AWS DMS 端點是否已設定身分驗證機制。如果未為端點設定身分驗證類型，則控制項會失敗。

AWS Database Migration Service 支援適用於 MongoDB 2.x 版的 MongoDB—MONGODB-CR 的兩種身分驗證方法，以及適用於 MongoDB 3.x 版或更新版本的 SCRAM-SHA-1。如果使用者想要使用密碼來存取資料庫，這些身分驗證方法會用來驗證和加密 MongoDB 密碼。AWS DMS 端點上的身分驗證可確保只有授權使用者才能存取和修改在資料庫之間遷移的資料。如果沒有適當的身分驗證，未經授權的使用者可能可以在遷移過程中存取敏感資料。這可能會導致資料外洩、資料遺失或其他安全事件。

修補

若要在 MongoDB 的 DMS 端點上啟用身分驗證機制，請參閱AWS Database Migration Service 《使用者指南》中的[使用 MongoDB 作為的來源 AWS DMS](#)。

【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS

相關要求：NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-13、PCI DSS v4.0.1/4.2.1

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::DMS::Endpoint

AWS Config 規則：[dms-redis-tls-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Redis OSS 的 AWS DMS 端點是否已設定 TLS 連線。如果端點未啟用 TLS，則控制項會失敗。

當透過網際網路在應用程式或資料庫之間傳送資料時，TLS 會提供end-to-end安全性。當您為 DMS 端點設定 SSL 加密時，它會在遷移程序期間啟用來源和目標資料庫之間的加密通訊。這有助於防止惡意人士竊聽和攔截敏感資料。如果沒有 SSL 加密，可能會存取敏感資料，導致資料外洩、資料遺失或其他安全事件。

修補

若要在 Redis 的 DMS 端點上啟用 TLS 連線，請參閱AWS Database Migration Service 《使用者指南》中的[使用 Redis 作為的目標 AWS Database Migration Service](#)。

【DMS.13】 DMS 複寫執行個體應設定為使用多個可用區域

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::DMS::ReplicationInstance

AWS Config 規則：[dms-replication-instance-multi-az-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS Database Migration Service (AWS DMS) 複寫執行個體是否設定為使用多個可用區域（異地同步備份部署）。如果 AWS DMS 複寫執行個體未設定為使用異地同步備份部署，則控制項會失敗。

在異地同步備份部署中，AWS DMS 會自動佈建和維護不同可用區域 (AZ) 中複寫執行個體的待命複本。然後，主要複寫執行個體會同步複寫到待命複本。若主要複寫執行個體失敗或沒有回應，待命會繼續任何執行中的任務，將插斷降至最低。如需詳細資訊，請參閱AWS Database Migration Service 《使用者指南》中的[使用複寫執行個體](#)。

修補

建立 AWS DMS 複寫執行個體之後，您可以變更其多可用區域部署設定。如需有關為現有複寫執行個體變更此設定和其他設定的資訊，請參閱AWS Database Migration Service 《使用者指南》中的[修改複寫執行個體](#)。

的 Security Hub CSPM 控制項 AWS DataSync

這些 Security Hub CSPM 控制項會評估 AWS DataSync 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【DataSync.1】DataSync 任務應該已啟用記錄

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::DataSync::Task

AWS Config 規則：[datasync-task-logging-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 AWS DataSync 任務是否已啟用記錄。如果任務未啟用記錄，則控制項會失敗。

稽核日誌會追蹤和監控系統活動。它們提供事件的記錄，可協助您偵測安全漏洞、調查事件並遵守法規。稽核日誌也會增強組織的整體責任和透明度。

修補

如需有關設定 AWS DataSync 任務記錄的資訊，請參閱AWS DataSync 《使用者指南》中的[使用 Amazon CloudWatch Logs 監控資料傳輸](#)。

【DataSync.2】應標記 DataSync 任務

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::DataSync::Task

AWS Config 規則：[datasync-task-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS DataSync 任務是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果任務沒有任何標籤索引鍵，或沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果任務沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws: 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多 存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需有關將標籤新增至 AWS DataSync 任務的資訊，請參閱AWS DataSync 《使用者指南》中的[標記您的 AWS DataSync 任務](#)。

Amazon Detective 的 Security Hub CSPM 控制項

此 AWS Security Hub CSPM 控制項會評估 Amazon Detective 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Detective.1】應標記 Detective 行為圖表

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Detective::Graph

AWS Config rule：tagged-detective-graph (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon Detective 行為圖表是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果行為圖表沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控

制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果行為圖表未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Detective 行為圖表，請參閱《Amazon Detective 管理指南》中的[將標籤新增至行為圖表](#)。

Amazon DocumentDB 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon DocumentDB（與 MongoDB 相容）服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【DocumentDB.1】Amazon DocumentDB 叢集應靜態加密

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[docdb-cluster-encrypted](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon DocumentDB 叢集是否靜態加密。如果 Amazon DocumentDB 叢集未靜態加密，則控制項會失敗。

靜態資料是指在任何期間內存放在持久性、非揮發性儲存體中的任何資料。加密可協助您保護此類資料的機密性，降低未經授權的使用者存取資料的風險。Amazon DocumentDB 叢集中的資料應靜態加密，以增加一層安全性。Amazon DocumentDB 使用 256 位元進階加密標準 (AES-256)，使用存放在 AWS Key Management Service () 中的加密金鑰來加密您的資料AWS KMS。

修補

您可以在建立 Amazon DocumentDB 叢集時啟用靜態加密。您無法在建立叢集後變更加密設定。如需詳細資訊，請參閱《[Amazon DocumentDB 開發人員指南](#)》中的為 [Amazon DocumentDB 叢集啟用靜態加密](#)。Amazon DocumentDB

【DocumentDB.2】Amazon DocumentDB 叢集應具有足夠的備份保留期

相關要求：NIST.800-53.r5 SI-12、PCI DSS v4.0.1/3.2.1

類別：復原 > 恢復 > 備份已啟用

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[docdb-cluster-backup-retention-check](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值	
minimumBackupRetentionPeriod	最短備份保留期間，以天為單位	Integer	7 至 35	7	

此控制項會檢查 Amazon DocumentDB 叢集的備份保留期間是否大於或等於指定的時間範圍。如果備份保留期小於指定的時間範圍，則控制項會失敗。除非您提供備份保留期間的自訂參數值，否則 Security Hub CSPM 會使用預設值 7 天。

備份可協助您更快地從安全事件中復原，並強化系統的彈性。透過自動化 Amazon DocumentDB 叢集的備份，您將能夠將系統還原到某個時間點，並將停機時間和資料遺失降至最低。在 Amazon DocumentDB 中，叢集的預設備份保留期間為 1 天。這必須增加到 7 到 35 天之間的值，才能通過此控制。

修補

若要變更 Amazon DocumentDB 叢集的備份保留期，請參閱 [《Amazon DocumentDB 開發人員指南》中的修改 Amazon DocumentDB 叢集](#)。Amazon DocumentDB 針對備份，選擇備份保留期。

【DocumentDB.3】Amazon DocumentDB 手動叢集快照不應公開

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7 5

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：AWS::RDS::DBClusterSnapshot

AWS Config 規則：[docdb-cluster-snapshot-public-prohibited](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon DocumentDB 手動叢集快照是否為公有。如果手動叢集快照為公有，則控制項會失敗。

除非預期，否則 Amazon DocumentDB 手動叢集快照不應公開。如果您將未加密的手動快照共用為公有，則該快照可供所有使用 AWS 帳戶。公有快照可能會導致意外的資料暴露。

Note

此控制項會評估手動叢集快照。您無法共用 Amazon DocumentDB 自動化叢集快照。不過，您可以透過複製自動化快照來建立手動快照，然後共用複本。

修補

若要移除 Amazon DocumentDB 手動叢集快照的公有存取權，請參閱《Amazon DocumentDB 開發人員指南》中的[共用快照](#)。您可以透過程式設計方式使用 Amazon DocumentDB 操作 `modify-db-snapshot-attribute`。將 `attribute-name` 設定為 `restore`，將 `values-to-remove` 設定為 `all`。

【DocumentDB.4】Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.3.3

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[docdb-cluster-audit-logging-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon DocumentDB 叢集是否將稽核日誌發佈至 Amazon CloudWatch Logs。如果叢集未將稽核日誌發佈至 CloudWatch Logs，則控制項會失敗。

Amazon DocumentDB（與 MongoDB 相容）可讓您稽核在叢集中執行的事件。已記錄事件的範例包括成功和失敗的身分驗證嘗試、在資料庫中放入集合，或建立索引。在預設情況下，稽核會在 Amazon DocumentDB 中停用，並要求您採取動作來啟用它。

修補

若要將 Amazon DocumentDB 稽核日誌發佈至 CloudWatch Logs，請參閱《Amazon DocumentDB 開發人員指南》中的[啟用稽核](#)。

【DocumentDB.5】Amazon DocumentDB 叢集應該啟用刪除保護

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

類別：保護 > 資料保護 > 資料刪除保護

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[docdb-cluster-deletion-protection-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon DocumentDB 叢集是否已啟用刪除保護。如果叢集未啟用刪除保護，則控制項會失敗。

啟用叢集刪除保護可提供額外的保護層，防止未經授權的使用者意外刪除或刪除資料庫。啟用刪除保護時，無法刪除 Amazon DocumentDB 叢集。您必須先停用刪除保護，刪除請求才能成功。當您在 Amazon DocumentDB 主控台中建立叢集時，預設會啟用刪除保護。

修補

若要啟用現有 Amazon DocumentDB 叢集的刪除保護，請參閱《[Amazon DocumentDB 開發人員指南](#)》中的[修改 Amazon DocumentDB 叢集](#)。Amazon DocumentDB 在修改叢集區段中，選擇啟用刪除保護。

【DocumentDB.6】Amazon DocumentDB 叢集應在傳輸中加密

類別：保護 > 資料保護 > data-in-transit

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[docdb-cluster-encrypted-in-transit](#)

排程類型：定期

參數：excludeTlsParameters：disabled、enabled (不可自訂)

此控制項會檢查 Amazon DocumentDB 叢集是否需要 TLS 才能連線至叢集。如果與叢集相關聯的叢集參數群組未同步，或 TLS 叢集參數設定為 disabled 或 enabled，則控制項會失敗。

您可以使用 TLS 來加密應用程式與 Amazon DocumentDB 叢集之間的連線。使用 TLS 有助於防止資料在應用程式和 Amazon DocumentDB 叢集之間傳輸時遭到攔截。Amazon DocumentDB 叢集的傳輸

中加密會使用與叢集相關聯的叢集參數群組中的 TLS 參數進行管理。當啟用傳輸中的加密時，需要使用 TLS 的安全連線來連線到叢集。建議使用下列 TLS 參數：tls1.2+、tls1.3+和 fips-140-3。

修補

如需有關變更 Amazon DocumentDB 叢集 TLS 設定的資訊，請參閱《Amazon DocumentDB 開發人員指南》中的[加密傳輸中的資料](#)。

DynamoDB 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon DynamoDB 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【DynamoDB.1】DynamoDB 資料表應隨著需求自動擴展容量

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::DynamoDB::Table

AWS Config 規則：[dynamodb-autoscaling-enabled](#)

排程類型：定期

參數：

參數	說明	Type	有效的自訂值	Security Hub CSPM 預設值
minProvisionedReadCapacity	DynamoDB 自動擴展的佈建讀取容量單位數目下限	Integer	1 至 40000	無預設值
targetReadUtilization	讀取容量的目標使用率百分比	Integer	20 至 90	無預設值

參數	說明	Type	有效的自訂值	Security Hub CSPM 預設值
minProvisionedWriteCapacity	DynamoDB 自動擴展的佈建寫入容量單位數目下限	Integer	1 至 40000	無預設值
targetWriteUtilization	寫入容量的目標使用率百分比	Integer	20 至 90	無預設值

此控制項會檢查 Amazon DynamoDB 資料表是否可以視需要擴展其讀取和寫入容量。如果資料表不使用隨需容量模式或已設定自動擴展的佈建模式，則控制項會失敗。根據預設，此控制項只需要設定其中一個模式，而不考慮讀取或寫入容量的特定層級。或者，您可以提供自訂參數值，以要求特定層級的讀取和寫入容量或目標使用率。

隨需擴展容量可避免限流例外狀況，有助於維持應用程式的可用性。使用隨需容量模式的 DynamoDB 資料表僅受到 DynamoDB 輸送量預設資料表配額的限制。若要提高這些配額，您可以向 [提交支援票證](#) 支援。使用佈建模式搭配自動擴展的 DynamoDB 資料表會動態調整佈建輸送量容量，以回應流量模式。如需 DynamoDB 請求限流的詳細資訊，請參閱《Amazon DynamoDB 開發人員指南》中的[請求限流和高載容量](#)。

修補

若要在容量模式中對現有資料表啟用 DynamoDB 自動擴展，請參閱《Amazon [DynamoDB 開發人員指南](#)》中的[在現有資料表上啟用 DynamoDB 自動擴展](#)。DynamoDB

【DynamoDB.2】DynamoDB 資料表應該啟用point-in-time復原

相關需求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

類別：復原 > 恢復 > 備份已啟用

嚴重性：中

資源類型：AWS::DynamoDB::Table

AWS Config 規則：[dynamodb-pitr-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已為 Amazon DynamoDB 資料表啟用 point-in-time 復原 (PITR)。

備份可協助您更快地從安全事件中復原。它們也會強化您系統的彈性。DynamoDB point-in-time 復原可自動備份 DynamoDB 資料表。它可縮短從意外刪除或寫入操作中復原的時間。已啟用 PITR 的 DynamoDB 資料表可以還原到過去 35 天內的任何時間點。

修補

若要將 DynamoDB 資料表還原至某個時間點，請參閱《Amazon [DynamoDB 開發人員指南](#)》中的 [將 DynamoDB 資料表還原至某個時間點](#)。 DynamoDB

【DynamoDB.3】DynamoDB Accelerator (DAX) 叢集應靜態加密

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest 加密

嚴重性：中

資源類型：AWS::DAX::Cluster

AWS Config 規則：[dax-encryption-enabled](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon DynamoDB Accelerator (DAX) 叢集是否靜態加密。如果 DAX 叢集未靜態加密，則控制項會失敗。

加密靜態資料可降低未驗證的使用者存取磁碟上儲存的資料的風險 AWS。加密新增另一組存取控制，以限制未經授權的使用者存取資料的能力。例如，需要 API 許可才能解密資料，才能讀取資料。

修補

建立叢集後，您無法啟用或停用靜態加密。您必須重新建立叢集，才能啟用靜態加密。如需如何在啟用靜態加密的情況下建立 DAX 叢集的詳細說明，請參閱《Amazon DynamoDB 開發人員指南》中的 [使用啟用靜態加密 AWS 管理主控台](#)。

【DynamoDB.4】DynamoDB 資料表應存在於備份計畫中

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

類別：Recover > Resilience > Backups enabled

嚴重性：中

資源類型：AWS::DynamoDB::Table

AWS Config 規則：[dynamodb-resources-protected-by-backup-plan](#)

排程類型：定期

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
backupVaultLockCheck	如果 參數設定為 true 且資源使用保存 AWS Backup 庫鎖定，則控制項會產生 PASSED 問題清單。	Boolean	true 或 false *	無預設值

此控制項會評估備份計畫是否涵蓋處於 ACTIVE 狀態的 Amazon DynamoDB 資料表。如果備份計畫未涵蓋 DynamoDB 資料表，則控制項會失敗。如果您將 backupVaultLockCheck 參數設定為等於 true，則只有在 DynamoDB 資料表備份在 AWS Backup 鎖定的保存庫中時，控制項才會通過。

AWS Backup 是一種全受管備份服務，可協助您集中和自動化跨的資料備份 AWS 服務。透過 AWS Backup，您可以建立備份計畫來定義備份需求，例如備份資料的頻率，以及保留這些備份的時間長度。在備份計畫中包含 DynamoDB 資料表可協助您保護資料免於意外遺失或刪除。

修補

若要將 DynamoDB 資料表新增至 AWS Backup 備份計畫，請參閱《AWS Backup 開發人員指南》中的[將資源指派給備份計畫](#)。

【DynamoDB.5】DynamoDB 資料表應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::DynamoDB::Table

AWS Config rule：tagged-dynamodb-table (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon DynamoDB 資料表是否具有具有參數中定義之特定金鑰的標籤requiredTagKeys。如果資料表沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果資料表未標記任何索引鍵，則會失敗。系統會aws:忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#)一般參考。

修補

若要將標籤新增至 DynamoDB 資料表，請參閱《Amazon [DynamoDB 開發人員指南](#)》中的在 [DynamoDB 中標記資源](#)。 DynamoDB

【DynamoDB.6】DynamoDB 資料表應該已啟用刪除保護

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

類別：保護 > 資料保護 > 資料刪除保護

嚴重性：中

資源類型：AWS::DynamoDB::Table

AWS Config 規則：[dynamodb-table-deletion-protection-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon DynamoDB 資料表是否已啟用刪除保護。如果 DynamoDB 資料表未啟用刪除保護，則控制項會失敗。

您可以使用刪除保護屬性來保護 DynamoDB 資料表免於意外刪除。為資料表啟用此屬性有助於確保管理員在定期資料表管理操作期間不會意外刪除資料表。這有助於防止對正常業務操作造成中斷。

修補

若要啟用 DynamoDB 資料表的刪除保護，請參閱《Amazon DynamoDB 開發人員指南》中的[使用刪除保護](#)。

【DynamoDB.7】DynamoDB Accelerator 叢集應在傳輸中加密

相關要求：NIST.800-53.r5 AC-17、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、PCI DSS v4.0.1/4.2.1

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::DAX::Cluster

AWS Config 規則：[dax-tls-endpoint-encryption](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon DynamoDB Accelerator (DAX) 叢集是否在傳輸中加密，且端點加密類型設定為 TLS。如果 DAX 叢集未在傳輸中加密，則控制項會失敗。

HTTPS (TLS) 可用來防止潛在攻擊者使用中間人攻擊或類似的攻擊手法來竊聽或操控網路流量。您應該只允許透過 TLS 的加密連線存取 DAX 叢集。不過，加密傳輸中的資料可能會影響效能。您應該在開啟加密的情況下測試應用程式，以了解效能設定檔和 TLS 的影響。

修補

您無法在建立 DAX 叢集之後變更 TLS 加密設定。若要加密現有的 DAX 叢集，請建立啟用傳輸中加密的新叢集，將應用程式的流量轉移到該叢集，然後刪除舊叢集。如需詳細資訊，請參閱《Amazon DynamoDB 開發人員指南》中的[使用刪除保護](#)。

Amazon EC2 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Elastic Compute Cloud (Amazon EC2) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【EC2.1】 Amazon EBS 快照不應設定為可公開還原

相關要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：AWS::::Account

AWS Config 規則：[ebs-snapshot-public-restorable-check](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon Elastic Block Store 快照是否設定為可公開還原。如果將所有 Amazon EBS 快照設定為可還原，則控制項會失敗。

EBS 快照用於在特定時間點將 EBS 磁碟區上的資料備份至 Amazon S3。您可以使用快照來還原 EBS 磁碟區的先前狀態。公開共享快照很少會有人願意接受。通常公開共享快照的決定都是錯誤的，或者並未完全了解其中含義。這項檢查有助於確保所有這些共享都是完整的規劃並且有意的。

修補

若要將公有 EBS 快照設為私有，請參閱《Amazon EC2 使用者指南》中的[共用快照](#)。針對動作、修改許可，選擇私有。

【EC2.2】VPC 預設安全群組不應允許傳入或傳出流量

相關要求：CIS AWS Foundations Benchmark v5.0.0/5.5、PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/2.1、CIS AWS Foundations Benchmark v1.2.0/4.3、CIS AWS Foundations Benchmark v1.4.0/5.3、CIS AWS Foundations Benchmark v3.0.0/5.4、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7)、NIST-1NIST.800-53.r5 SC-710 NIST.800-53.r5 SC-7

類別：保護 > 安全網路組態

嚴重性：高

資源類型：AWS::EC2::SecurityGroup

AWS Config 規則：[vpc-default-security-group-closed](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 VPC 的預設安全群組是否允許傳入或傳出流量。如果安全群組允許傳入或傳出流量，則控制項會失敗。

[預設安全群組](#)的規則允許所有來自指派至相同安全群組網路界面 (及其相關聯執行個體) 的傳出和傳入流量。建議您不要使用預設安全群組。由於您無法刪除預設安全群組，建議您變更預設安全群組的規則設定，限制傳入和傳出流量。這可以避免在意外地為資源 (例如 EC2 執行個體) 設定預設安全群組時產生意外的流量。

修補

若要修復此問題，請先建立新的最低權限安全群組。如需說明，請參閱《Amazon VPC 使用者指南》中的[建立安全群組](#)。然後，將新的安全群組指派給您的 EC2 執行個體。如需說明，請參閱《Amazon EC2 使用者指南》中的[變更執行個體的安全群組](#)。

將新的安全群組指派給資源之後，請從預設安全群組中移除所有傳入和傳出規則。如需說明，請參閱《Amazon VPC 使用者指南》中的[設定安全群組規則](#)。

【EC2.3】連接的 Amazon EBS 磁碟區應靜態加密

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::EC2::Volume

AWS Config 規則：[encrypted-volumes](#)

排程類型：變更已觸發

參數：無

此控制項會檢查處於連接狀態的 EBS 磁碟區是否已進行加密。如要通過此檢查，EBS 磁碟區必須為使用中狀態且經過加密。如果沒有連接 EBS 磁碟區，則其便不在此檢查的範圍內。

為了為您 EBS 磁碟區上的敏感資料新增多一層的安全，建議您啟用靜態 EBS 加密。Amazon EBS 加密提供 EBS 資源的直接加密解決方案，使您無須建置、維護和保全您自己的金鑰管理基礎設施。它會在建立加密的磁碟區和快照時使用 KMS 金鑰。

若要進一步了解 Amazon EBS 加密，請參閱《[Amazon EC2 使用者指南](#)》中的 [Amazon EBS 加密](#)。
Amazon EC2

修補

無法直接加密現有的未加密磁碟區或快照。您只能在建立磁碟區或快照時進行加密。

如果您預設啟用加密，Amazon EBS 會使用 Amazon EBS 加密的預設金鑰來加密產生的新磁碟區或快照。即使您沒有啟用預設加密，您可以在建立獨立的磁碟區或快照時啟用加密。在這兩種情況下，您可以覆寫 Amazon EBS 加密的預設金鑰，並選擇對稱客戶受管金鑰。

如需詳細資訊，請參閱《[Amazon EC2 使用者指南](#)》中的 [建立 Amazon EBS 磁碟區](#)、[Amazon EC2 複製 Amazon EBS 快照](#)。

【EC2.4】已停止的 EC2 執行個體應在指定的期間之後移除

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

類別：識別 > 清查

嚴重性：中

資源類型：AWS::EC2::Instance

AWS Config rule：ec2-stopped-instance-days-check (自訂 Security Hub CSPM 規則)

排程類型：定期

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
AllowedDays	在產生失敗的問題清單之前，允許 EC2 執行個體處於停止狀態的天數。	Integer	1 至 365	30

此控制項會檢查 Amazon EC2 執行個體是否已停止超過允許的天數。如果 EC2 執行個體停止的時間超過允許的最長期間，則控制項會失敗。除非您提供最長允許時段的自訂參數值，否則 Security Hub CSPM 會使用預設值 30 天。

當 EC2 執行個體長時間未執行時，會產生安全風險，因為執行個體並未主動維護（分析、修補、更新）。如果稍後啟動，缺乏適當的維護可能會導致您 AWS 環境中的意外問題。若要安全地將 EC2 執行個體長時間維持在非作用中狀態，請定期啟動它以進行維護，然後在維護後將其停止。理想情況下，這應該是自動化程序。

Note

此控制項會使用執行個體StateTransitionReason的 時間戳記，評估 EC2 執行個體已停止的天數。當 StateTransitionReason 不包含時間戳記（例如執行個體因內部錯誤而停止）時，控制項會改用執行個體的啟動時間。在此情況下，如果啟動時間早於允許的最長期間，控制項會產生 FAILED 問題清單。

修補

若要終止非作用中的 EC2 執行個體，請參閱《Amazon EC2 使用者指南》中的[終止執行個體](#)。

【EC2.6】應在所有 VPC 中啟用 VPCs 流程記錄

相關要求：CIS AWS Foundations Benchmark v5.0.0/3.7、CIS AWS Foundations Benchmark v1.2.0/2.9、CIS AWS Foundations Benchmark v1.4.0/3.9、CIS AWS Foundations Benchmark v3.0.0/3.7、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5AU-3、NIST.800-53.r5 AU-6(3)CA-7、NIST.800-5.r5 SI-7 3.1.2010.3.310.3.410.3.510.3.6

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::EC2::VPC

AWS Config 規則：[vpc-flow-logs-enabled](#)

排程類型：定期

參數：

- trafficType : REJECT (不可自訂)

此控制項會檢查是否已找到並啟用 VPC VPCs 流程日誌。流量類型設定為 Reject。如果您帳戶中的 VPC 未啟用 VPCs 流程日誌，則控制項會失敗。

Note

此控制項不會檢查是否已透過的 Amazon Security Lake 啟用 Amazon VPC 流程日誌 AWS 帳戶。

使用 VPC 流程日誌功能，您可以擷取進出 VPC 中網路介面之 IP 地址流量的相關資訊。建立流程日誌之後，您可以在 CloudWatch Logs 中檢視和擷取其資料。若要降低成本，您也可以將流程日誌傳送至 Amazon S3。

Security Hub CSPM 建議您為 VPCs 的封包拒絕啟用流程記錄。流程日誌可讓您了解周遊 VPC 的網路流量，並可偵測異常流量或在安全工作流程期間提供洞見。

根據預設，記錄包含 IP 地址流程不同元件的值，包括來源、目的地和通訊協定。如需日誌欄位的詳細資訊和說明，請參閱《Amazon [VPC 使用者指南](#)》中的 [VPC 流程日誌](#)。

修補

若要建立 VPC 流程日誌，請參閱《Amazon VPC 使用者指南》中的[建立流程日誌](#)。開啟 Amazon VPC 主控台後，選擇您的 VPCs。針對篩選條件，選擇拒絕或全部。

【EC2.7】應啟用 EBS 預設加密

相關要求：CIS AWS Foundations Benchmark v5.0.0/5.1.1、CIS AWS Foundations Benchmark v1.4.0/2.2.1、CIS AWS Foundations Benchmark v3.0.0/2.2.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.80-5.r5) SI-7)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS:::Account

AWS Config 規則：[ec2-ebs-encryption-by-default](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon Elastic Block Store (Amazon EBS) 磁碟區是否預設啟用帳戶層級加密。如果未針對 EBS 磁碟區啟用帳戶層級加密，則控制項會失敗。

為您的帳戶啟用加密時，Amazon EBS 磁碟區和快照複本會靜態加密。這會為您的資料新增額外的保護層。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[預設加密](#)。

修補

若要設定 Amazon EBS 磁碟區的預設加密，請參閱《Amazon EC2 使用者指南》中的[預設加密](#)。

【EC2.8】EC2 執行個體應使用執行個體中繼資料服務第 2 版 (IMDSv2)

相關要求：CIS AWS Foundations Benchmark v5.0.0/5.7、CIS AWS Foundations Benchmark v3.0.0/5.6、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、PCI DSS v4.0.1/2.2.6

類別：保護 > 網路安全

嚴重性：高

資源類型：AWS::EC2::Instance

AWS Config 規則：[ec2-imdsv2-check](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 EC2 執行個體中繼資料版本是否已使用執行個體中繼資料服務第 2 版 (IMDSv2) 設定。如果 HttpTokens 設定為 IMDSv2 所需的 `required`，則控制項會通過。如果設定為 `optional`，則控制項會失敗。

您可以使用執行個體中繼資料來設定或管理執行中的執行個體。IMDS 可讓您存取暫時、經常輪換的登入資料。這些登入資料無需手動或以程式設計方式對執行個體進行硬式編碼或分發敏感登入資料。IMDS 會在本機連接至每個 EC2 執行個體。它在 169.254.169.254 的特殊 "link local" IP 地址上執行。此 IP 地址只能由在執行個體上執行的軟體存取。

IMDS 第 2 版為下列類型的漏洞新增了新的保護。這些漏洞可用來嘗試存取 IMDS。

- 開啟網站應用程式防火牆
- 開啟反向代理
- 伺服器端請求偽造 (SSRF) 漏洞
- 開啟第 3 層防火牆和網路位址轉譯 (NAT)

Security Hub CSPM 建議您使用 IMDSv2 設定 EC2 執行個體。IMDSv2

修補

若要使用 IMDSv2 設定 EC2 執行個體，請參閱《Amazon EC2 使用者指南》中的[需要 IMDSv2 的建議路徑](#)。Amazon EC2

【EC2.9】 Amazon EC2 執行個體不應具有公有 IPv4 地址

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全網路組態 > 資源不可公開存取

嚴重性：高

資源類型：AWS::EC2::Instance

AWS Config 規則：[ec2-instance-no-public-ip](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 EC2 執行個體是否具有公有 IP 地址。如果 EC2 執行個體組態項目中存在 publicIp 欄位，則控制項會失敗。此控制項僅適用於 IPv4 地址。

公有 IPv4 地址是可從網際網路連線的 IP 地址。如果您使用公有 IP 地址啟動執行個體，則可以從網際網路存取 EC2 執行個體。私有 IPv4 地址是無法從網際網路連線的 IP 地址。您可以使用私有 IPv4 地址，在相同 VPC 或連線私有網路中的 EC2 執行個體之間進行通訊。

IPv6 地址是全域唯一的，因此可以從網際網路存取。不過，根據預設，所有子網路的 IPv6 定址屬性都設為 false。如需 IPv6 的詳細資訊，請參閱《Amazon [VPC 使用者指南](#)》中的 [VPC 中的 IP 定址](#)。

如果您有合法的使用案例來維護具有公有 IP 地址的 EC2 執行個體，則可以隱藏此控制項的問題清單。如需前端架構選項的詳細資訊，請參閱[AWS 架構部落格](#)或[這是我的架構系列](#) AWS 影片系列。

修補

使用非預設 VPC，讓執行個體預設不會獲指派公有 IP 地址。

當您在預設 VPC 中啟動 EC2 執行個體時，會為其指派公有 IP 地址。當您在非預設 VPC 中啟動 EC2 執行個體時，子網路組態會判斷它是否收到公有 IP 地址。子網路具有 屬性，可判斷子網路中的新 EC2 執行個體是否從公有 IPv4 地址集區接收公有 IP 地址。

您可以將自動指派的公有 IP 地址與 EC2 執行個體取消關聯。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[公有 IPv4 地址和外部 DNS 主機名稱](#)。

【EC2.10】 Amazon EC2 應設定為使用為 Amazon EC2 服務建立的 VPC 端點

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全網路組態 > API 私有存取

嚴重性：中

資源類型：AWS::EC2::VPC

AWS Config 規則：[service-vpc-endpoint-enabled](#)

排程類型：定期

參數：

- `serviceName` : `ec2` (不可自訂)

此控制項會檢查是否已為每個 VPC 建立 Amazon EC2 的服務端點。如果 VPC 沒有為 Amazon EC2 服務建立的 VPC 端點，則控制項會失敗。

此控制項會評估單一帳戶中的資源。它無法描述帳戶外部的資源。由於 AWS Config 和 Security Hub CSPM 不會執行跨帳戶檢查，因此您會看到跨帳戶共用 VPCs FAILED 問題清單。Security Hub CSPM 建議您隱藏這些 FAILED 調查結果。

Note

此控制項會評估標準端點服務名稱，且目前無法辨識 FIPS 變異端點服務名稱（例如 `com.amazonaws.us-east-1.ec2-fips`）。使用 Amazon EC2 的 FIPS 端點的 VPCs 可能會產生 FAILED 問題清單，即使已設定透過 VPC 端點連線至服務。

若要改善 VPC 的安全狀態，您可以將 Amazon EC2 設定為使用介面 VPC 端點。介面端點採用技術 AWS PrivateLink，可讓您私下存取 Amazon EC2 API 操作。它將 VPC 和 Amazon EC2 之間的所有網路流量限制在 Amazon 網路。由於端點僅在相同區域內受支援，因此您無法在不同區域中的 VPC 和服務之間建立端點。這可防止對其他區域的意外 Amazon EC2 API 呼叫。

若要進一步了解如何為 Amazon EC2 建立 VPC 端點，請參閱《[Amazon EC2 使用者指南](#)》中的 [Amazon EC2 和介面 VPC 端點](#)。Amazon EC2

修補

若要從 Amazon VPC 主控台建立介面端點至 Amazon EC2，請參閱《AWS PrivateLink 指南》中的 [建立 VPC 端點](#)。針對服務名稱，選擇 `com.amazonaws.region.ec2`。

您也可以建立端點政策並將其連接至 VPC 端點，以控制對 Amazon EC2 API 的存取。如需建立 VPC 端點政策的說明，請參閱《Amazon EC2 使用者指南》中的 [建立端點政策](#)。

【EC2.12】 應移除未使用的 Amazon EC2 EIPs

相關要求：PCI DSS v3.2.1/2.4、NIST.800-53.r5 CM-8(1)

類別：保護 > 安全網路組態

嚴重性：低

資源類型：AWS::EC2::EIP

AWS Config 規則：[eip-attached](#)

排程類型：變更已觸發

參數：無

此控制項會檢查配置給 VPC 的彈性 IP (EIP) 地址是否連接到 EC2 執行個體或使用中的彈性網路介面 (ENIs)。

失敗的問題清單表示您可能有未使用的 EC2 EIPs。

這可協助您在持卡人資料環境 (CDE) 中維持 EIPs 的準確資產清查。

修補

若要釋出未使用的 EIP，請參閱《Amazon EC2 使用者指南》中的[釋出彈性 IP 地址](#)。

【EC2.13】 安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 22

相關要求：CIS AWS Foundations Benchmark v1.2.0/4.1、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CM-7、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(7)、NIST.

類別：保護 > 安全網路組態

嚴重性：高

資源類型：AWS::EC2::SecurityGroup

AWS Config 規則：[restricted-ssh](#)

排程類型：已觸發和定期變更

參數：無

此控制項會檢查 Amazon EC2 安全群組是否允許從 0.0.0.0/0 或 ::/0 傳入連接埠 22。如果安全群組允許從 0.0.0.0/0 或 ::/0 傳入連接埠 22，則控制項會失敗。

安全群組提供 AWS 資源的輸入和輸出網路流量狀態篩選條件。不建議安全群組允許連接埠 22 不受限制的輸入存取。移除與遠端主控台服務 (如 SSH) 的不受限連線能力可降低伺服器暴露在風險中的機會。

修補

若要禁止傳入連接埠 22，請移除允許與 VPC 關聯之每個安全群組進行此類存取的規則。如需說明，請參閱《Amazon EC2 使用者指南》中的[更新安全群組規則](#)。在 Amazon EC2 主控台中選取安全群組後，選擇動作、編輯傳入規則。移除允許存取連接埠 22 的規則。

【EC2.14】 安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389

相關要求：CIS AWS Foundations Benchmark v1.2.0/4.2、PCI DSS v4.0.1/1.3.1

類別：保護 > 安全網路組態

嚴重性：高

資源類型：AWS::EC2::SecurityGroup

AWS Config rule：[restricted-common-ports](#) (建立的規則為 restricted-rdp)

排程類型：已觸發和定期變更

參數：無

此控制項會檢查 Amazon EC2 安全群組是否允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389。如果安全群組允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389，則控制項會失敗。

安全群組提供 AWS 資源的輸入和輸出網路流量狀態篩選條件。不建議安全群組允許連接埠 3389 不受限制的輸入存取。移除與遠端主控台服務 (如 RDP) 的不受限連線能力可降低伺服器暴露在風險中的機會。

修補

若要禁止傳入連接埠 3389，請移除規則，允許對與 VPC 相關聯的每個安全群組進行此類存取。如需說明，請參閱《Amazon VPC 使用者指南》中的[更新安全群組規則](#)。在 Amazon VPC 主控台中選取安全群組後，選擇動作、編輯傳入規則。移除允許存取連接埠 3389 的規則。

【EC2.15】 Amazon EC2 子網路不應自動指派公有 IP 地址

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 網路安全

嚴重性：中

資源類型：AWS::EC2::Subnet

AWS Config 規則：[subnet-auto-assign-public-ip-disabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon Virtual Private Cloud (Amazon VPC) 子網路是否已設定為自動指派公有 IP 地址。如果子網路設定為自動指派公有 IPv4 或 IPv6 地址，則控制項會失敗。

子網路具有屬性，可判斷網路介面是否自動接收公有 IPv4 和 IPv6 地址。對於 IPv4，此屬性 TRUE 針對預設子網路和非 FALSE 預設子網路設定為（透過 EC2 啟動執行個體精靈建立的非預設子網路除外，其中設定為 TRUE）。對於 IPv6，此屬性預設為所有子網路 FALSE 的。啟用這些屬性時，在子網路中啟動的執行個體會自動在其主要網路界面上接收對應的 IP 地址 (IPv4 或 IPv6)。

修補

若要將子網路設定為不指派公有 IP 地址，請參閱《Amazon VPC 使用者指南》中的[修改子網路的 IP 定址屬性](#)。

【EC2.16】 應該移除未使用的網路存取控制清單

相關要求：NIST.800-53.r5 CM-8(1)、NIST.800-171.r2 3.4.7、PCI DSS v4.0.1/1.2.7

類別：保護 > 網路安全

嚴重性：低

資源類型：AWS::EC2::NetworkAcl

AWS Config 規則：[vpc-network-acl-unused-check](#)

排程類型：變更已觸發

參數：無

此控制項會檢查虛擬私有雲端 (VPC) 中是否有任何未使用的網路存取控制清單 (網路 ACLs)。如果網路 ACL 未與子網路建立關聯，則控制項會失敗。控制項不會為未使用的預設網路 ACL 產生問題清單。

控制項會檢查資源的項目組態，AWS::EC2::NetworkAcl並判斷網路 ACL 的關係。

如果唯一關係是網路 ACL 的 VPC，則控制項會失敗。

如果列出其他關係，則控制項會通過。

修補

如需刪除未使用網路 ACL 的說明，請參閱《Amazon VPC 使用者指南》中的[刪除網路 ACL](#)。您無法刪除與子網路相關聯的預設網路 ACL 或 ACL。

【EC2.17】 Amazon EC2 執行個體不應使用多個 ENIs

相關要求：NIST.800-53.r5 AC-4(21)

類別：保護 > 網路安全

嚴重性：低

資源類型：AWS::EC2::Instance

AWS Config 規則：[ec2-instance-multiple-eni-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 EC2 執行個體是否使用多個彈性網路界面 (ENIs) 或彈性布料轉接器 (EFAs)。如果使用單一網路轉接器，則此控制項會通過。控制項包含選用參數清單，以識別允許的 ENIs。如果屬於 Amazon EKS 叢集的 EC2 執行個體使用多個 ENI，則此控制項也會失敗。如果您的 EC2 執行個體需要有多個 ENIs 做為 Amazon EKS 叢集的一部分，您可以隱藏這些控制問題清單。

多個 ENIs 可能會導致雙主目錄執行個體，這表示具有多個子網路的執行個體。這可能會增加網路安全複雜性，並導致意外的網路路徑和存取。

修補

若要分離網路介面與 EC2 執行個體，請參閱《Amazon EC2 使用者指南》中的[分離網路介面與執行個體](#)。

【EC2.18】安全群組應僅允許授權連接埠不受限制的傳入流量

相關要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)、NIST.800-171.r2 3.1.3、NIST.800-171.r2 3.1.20、NIST-1020.10

類別：保護 > 安全網路組態 > 安全群組組態

嚴重性：高

資源類型：AWS::EC2::SecurityGroup

AWS Config 規則：[vpc-sg-open-only-to-authorized-ports](#)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
authorize dTcpPorts	授權的 TCP 連接埠清單	IntegerList (最少 1 個項目，最多 32 個項目)	1 至 65535	[80,443]
authorize dUdpPorts	授權 UDP 連接埠的清單	IntegerList (最少 1 個項目，最多 32 個項目)	1 至 65535	無預設值

此控制項會檢查 Amazon EC2 安全群組是否允許來自未經授權連接埠的無限制傳入流量。控制狀態的判斷方式如下：

- 如果您使用的預設值 `authorizedTcpPorts`，則如果安全群組允許來自連接埠 80 和 443 以外的任何連接埠的無限制傳入流量，則控制項會失敗。
- 如果您為 `authorizedTcpPorts` 或提供自訂值 `authorizedUdpPorts`，則如果安全群組允許來自任何未列出連接埠的無限制傳入流量，則控制項會失敗。

安全群組提供傳入和傳出網路流量到的狀態篩選 AWS。安全群組規則應遵循最低權限存取的主體。無限制存取 (IP 地址尾碼為 /0) 會增加惡意活動的機會，例如駭客入侵、denial-of-service 攻擊和資料遺失。除非特別允許連接埠，否則連接埠應拒絕不受限制的存取。

修補

若要修改安全群組，請參閱《Amazon VPC 使用者指南》中的[使用安全群組](#)。

【EC2.19】安全群組不應允許無限制存取高風險的連接埠

相關需求：NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-7、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7 3.1.20

類別：保護 > 受限制的網路存取

嚴重性：嚴重

資源類型：AWS::EC2::SecurityGroup

AWS Config rule：[restricted-common-ports](#) (建立的規則為 vpc-sg-restricted-common-ports)

排程類型：變更已觸發和定期

參數："blockedPorts":

"20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,5600"
(不可自訂)

此控制項會檢查 Amazon EC2 安全群組的無限制傳入流量是否可供被視為高風險的指定連接埠存取。如果安全群組中的任何規則允許從 '0.0.0.0/0' 或 ':::0' 傳入流量到這些連接埠，則此控制會失敗。

安全群組提供 AWS 資源的輸入和輸出網路流量狀態篩選條件。無限制存取 (0.0.0.0/0) 會增加惡意活動的機會，例如駭客入侵、denial-of-service 攻擊和資料遺失。安全群組不應允許無限制的傳入存取下列連接埠：

- 20、21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)

- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)
- 1433、1434 (MSSQL)
- 3000 (Go、Node.js 和 Ruby Web 開發架構)
- 3306 (mySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (Python Web 開發架構)
- 5432 (postgresql)
- 5500 (fcg-addr-srvr1)
- 5601 (OpenSearch 儀表板)
- 8080 (代理)
- 8088 (舊版 HTTP 連接埠)
- 8888 (替代 HTTP 連接埠)
- 9200 或 9300 (OpenSearch)

修補

若要從安全群組刪除規則，請參閱《Amazon EC2 使用者指南》中的[從安全群組刪除規則](#)。

【EC2.20】 用於 an AWS Site-to-Site VPN 連線的兩個 VPN 通道都應啟動

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)、NIST.800-171.r2 3.1.13、NIST.800-171.r2 3.1.20

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::EC2::VPNConnection

AWS Config 規則：[vpc-vpn-2-tunnels-up](#)

排程類型：已觸發變更

參數：無

VPN 通道是一種加密連結，其中資料可以從客戶網路傳入或傳出 an AWS Site-to-Site VPN 連接 AWS。每個 VPN 連接包含兩個 VPN 通道，您可以同時使用這些通道以獲得高可用性。確保兩個 VPN 通道都適用於 VPN 連線，對於確認 AWS VPC 和遠端網路之間的安全且高可用性連線至關重要。

此控制項會檢查 AWS Site-to-Site VPN 通道都處於 UP 狀態。如果一個或兩個通道處於 DOWN 狀態，則控制項會失敗。

修補

若要修改 VPN 通道選項，請參閱[Site-to-Site使用者指南》中的修改站台對站台 VPN 通道選項](#)。AWS Site-to-Site

【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389

相關要求：CIS AWS Foundations Benchmark v5.0.0/5.2、CIS AWS Foundations Benchmark v1.4.0/5.1、CIS AWS Foundations Benchmark v3.0.0/5.1、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-7、NIST.800-53.r5 SC-7(5)、NIST.800-53.r5 SC-7 3.1.20

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::EC2::NetworkACL

AWS Config 規則：[nacl-no-unrestricted-ssh-rdp](#)

排程類型：已觸發變更

參數：無

此控制項會檢查網路存取控制清單（網路 ACL）是否允許無限制存取 SSH/RDP 輸入流量的預設 TCP 連接埠。如果網路 ACL 傳入項目允許 TCP 連接埠 22 或 3389 的來源 CIDR 區塊為 '0.0.0.0/0' 或 '：：/0'，則控制項會失敗。控制項不會產生預設網路 ACL 的問題清單。

存取遠端伺服器管理連接埠，例如連接埠 22 (SSH) 和連接埠 3389 (RDP)，不應公開存取，因為這可能會允許意外存取 VPC 中的資源。

修補

若要編輯網路 ACL 流量規則，請參閱《Amazon VPC 使用者指南》[中的使用網路 ACLs](#)。

【EC2.22】應移除未使用的 Amazon EC2 安全群組

類別：識別 > 清查

嚴重性：中

資源類型：AWS::EC2::NetworkInterface、AWS::EC2::SecurityGroup

AWS Config 規則：[ec2-security-group-attached-to-eni-periodic](#)

排程類型：定期

參數：無

此控制項會檢查安全群組是否連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體或彈性網路界面。如果安全群組未與 Amazon EC2 執行個體或彈性網路介面建立關聯，則控制項會失敗。

Important

2023 年 9 月 20 日，Security Hub CSPM 已從 AWS 基礎安全最佳實務和 NIST SP 800-53 修訂版 5 標準中移除此控制項。此控制項仍是 AWS Control Tower 服務受管標準的一部分。如果安全群組連接到 EC2 執行個體或彈性網路界面，此控制項會產生傳遞的問題清單。不過，對於某些使用案例，未連接的安全群組不會構成安全風險。您可以使用其他 EC2 控制項，例如 EC2.2、EC2.13、EC2.14、EC2.18 和 EC2.19，來監控您的安全群組。

修補

若要建立、指派和刪除安全群組，請參閱《Amazon [EC2 使用者指南](#)》中的 [EC2 執行個體的安全群組](#)。Amazon EC2

【EC2.23】Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求

相關需求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

類別：保護 > 安全網路組態

嚴重性：高

資源類型：AWS::EC2::TransitGateway

AWS Config 規則：[ec2-transit-gateway-auto-vpc-attach-disabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 EC2 傳輸閘道是否自動接受共用 VPC 連接。對於自動接受共用 VPC 連接請求的傳輸閘道，此控制失敗。

開啟 會將傳輸閘道AutoAcceptSharedAttachments設定為自動接受任何跨帳戶 VPC 連接請求，而無需驗證請求或連接來源的帳戶。若要遵循授權和身分驗證的最佳實務，建議您關閉此功能，以確保只接受授權的 VPC 連接請求。

修補

若要修改傳輸閘道，請參閱《Amazon VPC 開發人員指南》中的[修改傳輸閘道](#)。

【EC2.24】不應使用 Amazon EC2 全虛擬化執行個體類型

相關需求：NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：AWS::EC2::Instance

AWS Config 規則：[ec2-paravirtual-instance-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 EC2 執行個體的虛擬化類型是否為全虛擬化。如果 EC2 執行個體virtualizationType的 設定為 ，則控制項會失敗paravirtual。

Linux Amazon Machine Image (AMIs) 使用兩種虛擬化類型之一：全虛擬化 (PV) 或硬體虛擬機器 (HVM)。PV 和 HVM AMI 之間的主要區別在於開機的方式以及是否可以利用特殊的硬體延伸 (CPU、網路和儲存) 來獲得更好的效能。

歷史上，在許多情況下，PV 訪客比 HVM 訪客具有更好的效能，但由於 HVM 虛擬化中的增強以及 HVM AMI 之 PV 驅動程式的可用性，這已不再成立。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [Linux AMI 虛擬化類型](#)。

修補

若要將 EC2 執行個體更新為新的執行個體類型，請參閱《Amazon EC2 使用者指南》中的[變更執行個體類型](#)。

【EC2.25】 Amazon EC2 啟動範本不應將公IPs 指派給網路介面

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全網路組態 > 不可公開存取的資源

嚴重性：高

資源類型：AWS::EC2::LaunchTemplate

AWS Config 規則：[ec2-launch-template-public-ip-disabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EC2 啟動範本是否設定為在啟動時將公有 IP 地址指派給網路介面。如果 EC2 啟動範本設定為將公有 IP 地址指派給網路介面，或至少有一個具有公有 IP 地址的網路介面，則控制項會失敗。

公有 IP 地址是從網際網路連線的地址。如果您使用公有 IP 地址設定網路介面，則可以從網際網路存取與這些網路介面相關聯的資源。EC2 資源不應公開存取，因為這可能會允許意外存取您的工作負載。

修補

若要更新 EC2 啟動範本，請參閱《Amazon EC2 Auto Scaling 使用者指南》中的[變更預設網路介面設定](#)。

【EC2.28】 備份計畫應涵蓋 EBS 磁碟區

類別：復原 > 恢復 > 備份已啟用

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

嚴重性：低

資源類型：AWS::EC2::Volume

AWS Config 規則：[ebs-resources-protected-by-backup-plan](#)

排程類型：定期

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
backupVaultLockCheck	如果 參數設定為 true 且資源使用 AWS Backup 保存庫鎖定，則控制項會產生 PASSED 問題清單。	Boolean	true 或 false *	無預設值

此控制項會評估備份計畫是否涵蓋處於 in-use 狀態的 Amazon EBS 磁碟區。如果備份計畫未涵蓋 EBS 磁碟區，則控制項會失敗。如果您將 backupVaultLockCheck 參數設定為等於 true，則只有在 AWS Backup 鎖定的保存庫中備份 EBS 磁碟區時，控制項才會通過。

備份可協助您更快地從安全事件中復原。它們也會強化您系統的彈性。在備份計畫中包含 Amazon EBS 磁碟區可協助您保護資料免於意外遺失或刪除。

修補

若要將 Amazon EBS 磁碟區新增至 AWS Backup 備份計畫，請參閱《AWS Backup 開發人員指南》中的[將資源指派給備份計畫](#)。

【EC2.33】EC2 傳輸閘道附件應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::TransitGatewayAttachment

AWS Config rule：tagged-ec2-transitgatewayattachment (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1-6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 傳輸閘道連接是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果傳輸閘道連接沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果傳輸閘道附件未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 傳輸閘道連接，請參閱 [《Amazon EC2 使用者指南》中的標記您的 Amazon EC2 資源](#)。

【EC2.34】EC2 傳輸閘道路由表應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::TransitGatewayRouteTable

AWS Config rule：tagged-ec2-transitgatewayroutetable (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	無預設值

此控制項會檢查 Amazon EC2 傳輸閘道路由表是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果傳輸閘道路由表沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果傳輸閘道路由表未標記任何索引鍵，則 會失敗。系統會忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 傳輸閘道路由表，請參閱 [《Amazon EC2 使用者指南》](#) 中的標記您的 [Amazon EC2 資源](#)。Amazon EC2

【EC2.35】 EC2 網路介面應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::NetworkInterface

AWS Config rule：tagged-ec2-networkinterface (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1-6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 網路介面是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果網路介面沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果網路介面未標記任何索引鍵，則 控制會失敗。系統會 aws: 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 網路介面，請參閱 [《Amazon EC2 使用者指南》中的標記您的 Amazon EC2 資源](#)。

【EC2.36】 EC2 客戶閘道應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::CustomerGateway

AWS Config rule：tagged-ec2-customergateway (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 客戶閘道是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果客戶閘道沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果客戶閘道未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 客戶端，請參閱《[Amazon EC2 使用者指南](#)》中的[標記您的 Amazon EC2 資源](#)。

【EC2.37】 EC2 彈性 IP 地址應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::EIP

AWS Config rule：tagged-ec2-eip (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 彈性 IP 地址是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果彈性 IP 地址沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤金鑰是否存在，如果彈性 IP 地址未加上任何金鑰的標籤，則會失敗。系統會 aws: 忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱[什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 彈性 IP 地址，請參閱《[Amazon EC2 使用者指南](#)》中的[標記您的 Amazon EC2 資源](#)。

【EC2.38】應標記 EC2 執行個體

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::Instance

AWS Config rule：tagged-ec2-instance（自訂 Security Hub CSPM 規則）

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 執行個體是否具有具有參數 中定義之特定金鑰的標籤 `requiredTagKeys`。如果執行個體沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果執行個體未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 執行個體，請參閱 [《Amazon EC2 使用者指南》中的標記您的](#) Amazon EC2 資源。

【EC2.39】 EC2 網際網路閘道應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::InternetGateway

AWS Config rule：tagged-ec2-internetgateway (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 網際網路閘道是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果網際網路閘道沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果網際網路閘道未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 網際網路閘道，請參閱 [《Amazon EC2 使用者指南》](#) 中的 [標記您的 Amazon EC2 資源](#)。

【EC2.40】EC2 NAT 閘道應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::NatGateway

AWS Config rule：tagged-ec2-natgateway (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 網路位址轉譯 (NAT) 閘道是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果 NAT 閘道沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果 NAT 閘道未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 NAT 閘道，請參閱 [《Amazon EC2 使用者指南》中的標記您的 Amazon EC2 資源](#)。

【EC2.41】 EC2 網路 ACLs 應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::NetworkACL

AWS Config rule：tagged-ec2-networkacl (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 網路存取控制清單 (網路 ACL) 是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果網路 ACL 沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果網路 ACL 未標記任何索引鍵，則失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體 (使用者或角色) 和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱[什麼是 ABAC AWS ?](#) IAM 使用者指南中的 。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 網路 ACL，請參閱 [《Amazon EC2 使用者指南》](#) 中的標記您的 Amazon EC2 資源。Amazon EC2

【EC2.42】 EC2 路由表應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::RouteTable

AWS Config rule：tagged-ec2-routetable (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 路由表是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果路由表沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果路由表未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱[什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 路由表，請參閱《[Amazon EC2 使用者指南](#)》中的[標記您的 Amazon EC2 資源](#)。

【EC2.43】 EC2 安全群組應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::SecurityGroup

AWS Config rule：tagged-ec2-securitygroup (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 安全群組是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果安全群組沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果安全群組未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱[什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 安全群組，請參閱 [《Amazon EC2 使用者指南》中的標記您的 Amazon EC2 資源](#)。

【EC2.44】EC2 子網路應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::Subnet

AWS Config rule：tagged-ec2-subnet (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 子網路是否具有具有參數 中定義之特定金鑰的標籤 `requiredTagKeys`。如果子網路沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果子網路未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 子網路，請參閱 [《Amazon EC2 使用者指南》中的標記您的](#) Amazon EC2 資源。

【EC2.45】 EC2 磁碟區應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::Volume

AWS Config rule：tagged-ec2-volume (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	無預設值

此控制項會檢查 Amazon EC2 磁碟區是否具有含參數中定義之特定金鑰的標籤 `requiredTagKeys`。如果磁碟區沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果磁碟區未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 磁碟區，請參閱 [《Amazon EC2 使用者指南》中的標記您的 Amazon EC2 資源](#)。

【EC2.46】 Amazon VPCs應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::VPC

AWS Config rule : tagged-ec2-vpc (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1-6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon Virtual Private Cloud (Amazon VPC) 是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果 Amazon VPC 沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果 Amazon VPC 未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 VPC，請參閱 [《Amazon EC2 使用者指南》](#) 中的 [標記您的 Amazon EC2 資源](#)。

【EC2.47】 Amazon VPC 端點服務應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::VPCEndpointService

AWS Config rule：tagged-ec2-vpcendpointservice (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon VPC 端點服務是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果端點服務沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果端點服務未標記任何索引鍵，則 會失敗。系統會 aws: 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Amazon VPC 端點服務，請參閱 [《指南》中的設定端點服務一節中的管理標籤](https://docs.aws.amazon.com/vpc/latest/privatelink/configure-endpoint-service.html)。
<https://docs.aws.amazon.com/vpc/latest/privatelink/configure-endpoint-service.html> AWS PrivateLink

【EC2.48】 Amazon VPC 流程日誌應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::FlowLog

AWS Config rule：tagged-ec2-flowlog (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon VPC 流程日誌是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果流程日誌沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果流程日誌未標記任何索引鍵，則 會失敗。系統會 aws: 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Amazon VPC 流程日誌，請參閱《Amazon VPC 使用者指南》中的[標記流程日誌](#)。

【EC2.49】 Amazon VPC 互連連線應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::VPCPeeringConnection

AWS Config rule：tagged-ec2-vpcpeeringconnection (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon VPC 互連連線是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果對等連線沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果對等連線未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知

的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱[什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Amazon VPC 對等互連，請參閱《[Amazon EC2 使用者指南](#)》中的[標記您的 Amazon EC2 資源](#)。

【EC2.50】 EC2 VPN 閘道應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::VPNGateway

AWS Config rule：tagged-ec2-vpngateway (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 VPN 閘道是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果 VPN 閘道沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控

制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤金鑰是否存在，如果 VPN 閘道未標記任何金鑰，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 VPN 閘道，請參閱 [《Amazon EC2 使用者指南》中的標記您的 Amazon EC2 資源](#)。

【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄

相關要求：NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.8000-5.r5)、AU-6NIST.5 AU-9 CA-7 NIST.800-53.r5 SC-7 SI-3 SI-4 SI-7 3.1.12 3.1.2010.2.1

類別：識別 > 記錄日誌

嚴重性：低

資源類型：AWS::EC2::ClientVpnEndpoint

AWS Config 規則：[ec2-client-vpn-connection-log-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 AWS Client VPN 端點是否已啟用用戶端連線記錄。如果端點未啟用用戶端連線記錄，則控制項會失敗。

Client VPN 端點可讓遠端用戶端安全地連線至其中 Virtual Private Cloud (VPC) 中的資源 AWS。連線日誌可讓您追蹤 VPN 端點上的使用者活動，並提供可見性。啟用連線日誌記錄時，您可以在日誌群組中指定日誌串流的名稱。如果您未指定日誌串流，Client VPN 服務會為您建立一個。

修補

若要啟用連線記錄，請參閱《AWS Client VPN 管理員指南》中的[啟用現有 Client VPN 端點的連線記錄](#)。

【EC2.52】 EC2 傳輸閘道應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::TransitGateway

AWS Config rule：tagged-ec2-transitgateway (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon EC2 傳輸閘道是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果傳輸閘道沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果傳輸閘道未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知

的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱[什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EC2 傳輸閘道，請參閱《[Amazon EC2 使用者指南](#)》中的[標記您的 Amazon EC2 資源](#)。

【EC2.53】 EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠

相關要求：CIS AWS Foundations Benchmark v5.0.0/5.3、CIS AWS Foundations Benchmark v3.0.0/5.2、PCI DSS v4.0.1/1.3.1

類別：保護 > 安全網路組態 > 安全群組組態

嚴重性：高

資源類型：AWS::EC2::SecurityGroup

AWS Config 規則：[vpc-sg-port-restriction-check](#)

排程類型：定期

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
ipType	IP 版本	String	無法自訂	IPv4
restrictPorts	應拒絕輸入流量的連接埠清單	IntegerList	無法自訂	22, 3389

此控制項會檢查 Amazon EC2 安全群組是否允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠（連接埠 22 和 3389）。如果安全群組允許從 0.0.0.0/0 傳入連接埠 22 或 3389，則控制項會失敗。

安全群組提供 AWS 資源的輸入和輸出網路流量狀態篩選條件。我們建議安全群組不允許使用 TDP (6)、UDP (17) 或 ALL (-1) 通訊協定，不受限制地存取遠端伺服器管理連接埠，例如 SSH 對連接埠 22 和 RDP 對連接埠 3389。允許公開存取這些連接埠會增加資源攻擊面和資源入侵的風險。

修補

若要更新 EC2 安全群組規則以禁止將流量傳入指定的連接埠，請參閱《Amazon EC2 使用者指南》中的[更新安全群組規則](#)。在 Amazon EC2 主控台中選取安全群組後，選擇動作、編輯傳入規則。移除允許存取連接埠 22 或連接埠 3389 的規則。

【EC2.54】 EC2 安全群組不應允許從 ::/0 傳入遠端伺服器管理連接埠

相關要求：CIS AWS Foundations Benchmark v5.0.0/5.4、CIS AWS Foundations Benchmark v3.0.0/5.3、PCI DSS v4.0.1/1.3.1

類別：保護 > 安全網路組態 > 安全群組組態

嚴重性：高

資源類型：AWS::EC2::SecurityGroup

AWS Config 規則：[vpc-sg-port-restriction-check](#)

排程類型：定期

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
ipType	IP 版本	String	無法自訂	IPv6
restrictPorts	應拒絕輸入流量的連接埠清單	IntegerList	無法自訂	22, 3389

此控制項會檢查 Amazon EC2 安全群組是否允許從 ::/0 傳入遠端伺服器管理連接埠（連接埠 22 和 3389）。如果安全群組允許從 ::/0 傳入連接埠 22 或 3389，則控制項會失敗。

安全群組提供 AWS 資源的輸入和輸出網路流量狀態篩選條件。我們建議安全群組不允許使用 TDP (6)、UDP (17) 或 ALL (-1) 通訊協定，不受限制地存取遠端伺服器管理連接埠，例如 SSH 對連接埠 22 和 RDP 對連接埠 3389。允許公開存取這些連接埠會增加資源攻擊面和資源入侵的風險。

修補

若要更新 EC2 安全群組規則以禁止將流量傳入指定的連接埠，請參閱《Amazon EC2 使用者指南》中的[更新安全群組規則](#)。在 Amazon EC2 主控台中選取安全群組後，選擇動作、編輯傳入規則。移除允許存取連接埠 22 或連接埠 3389 的規則。

【EC2.55】 VPCs應使用 ECR API 的介面端點進行設定

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全存取控制 > 存取控制

嚴重性：中

資源類型：AWS::EC2::VPC、AWS::EC2::VPCEndpoint

AWS Config 規則：[vpc-endpoint-enabled](#)

排程類型：定期

參數：

參數	必要	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
serviceNames	必要	控制項評估的服務名稱	String	無法自訂	ecr.api
vpcIds	選用	VPC 端點的 Amazon VPC IDs 逗號分隔清單。如果提	StringList	使用一或多個 VPC IDs 自訂	無預設值

參數	必要	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
		供，則如果 serviceName 參數中 指定的服務 沒有其中一 個 VPC 端 點，則控制 項會失敗。			

此控制項會檢查您管理的虛擬私有雲端 (VPC) 是否有 Amazon ECR API 的介面 VPC 端點。如果 VPC 沒有 ECR API 的介面 VPC 端點，則控制項會失敗。此控制項會評估單一帳戶中的資源。

AWS PrivateLink 可讓客戶 AWS 以高可用性和可擴展的方式存取上託管的服務，同時保留 AWS 網路內的所有網路流量。服務使用者可以從 VPC 或其內部部署私下存取由 PrivateLink 提供支援的服務，而無需使用公 IPs，也不需要流量周遊網際網路。

修補

若要設定 VPC 端點，請參閱《AWS PrivateLink 指南》中的[AWS 服務 使用介面 VPC 端點存取](#)。

【EC2.56】 VPCs應使用 Docker 登錄檔的介面端點進行設定

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全存取控制 > 存取控制

嚴重性：中

資源類型：AWS::EC2::VPC、AWS::EC2::VPCEndpoint

AWS Config 規則：[vpc-endpoint-enabled](#)

排程類型：定期

參數：

參數	必要	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
serviceNames	必要	控制項評估的服務名稱	String	無法自訂	ecr.dkr
vpcIds	選用	VPC 端點的 Amazon VPC IDs 逗號分隔清單。如果提供，則如果 serviceName 參數中指定的服務沒有其中一個 VPC 端點，則控制項會失敗。	StringList	使用一或多個 VPC IDs 自訂	無預設值

此控制項會檢查您管理的虛擬私有雲端 (VPC) 是否有 Docker 登錄檔的介面 VPC 端點。如果 VPC 沒有 Docker 登錄檔的介面 VPC 端點，則控制項會失敗。此控制項會評估單一帳戶中的資源。

AWS PrivateLink 可讓客戶 AWS 以高可用性和可擴展的方式存取上託管的服務，同時保留 AWS 網路內的所有網路流量。服務使用者可以從 VPC 或其內部部署私下存取由 PrivateLink 提供支援的服務，而無需使用公 IPs，也不需要流量周遊網際網路。

修補

若要設定 VPC 端點，請參閱《AWS PrivateLink 指南》中的[AWS 服務 使用介面 VPC 端點存取](#)。

【EC2.57】 VPCs應使用 Systems Manager 的介面端點進行設定

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全存取控制 > 存取控制

嚴重性：中

資源類型：AWS::EC2::VPC、AWS::EC2::VPCEndpoint

AWS Config 規則：[vpc-endpoint-enabled](#)

排程類型：定期

參數：

參數	必要	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
serviceName	必要	控制項評估的服務名稱	String	無法自訂	ssm
vpcIds	選用	VPC 端點的 Amazon VPC IDs 逗號分隔清單。如果提供，則如果 serviceName 參數中指定的服務沒有其中一個 VPC 端點，則控制項會失敗。	StringList	使用一個或多個 VPC IDs 自訂	無預設值

此控制項會檢查您管理的虛擬私有雲端 (VPC) 是否有介面 VPC 端點 AWS Systems Manager。如果 VPC 沒有 Systems Manager 的介面 VPC 端點，則控制項會失敗。此控制項會評估單一帳戶中的資源。

AWS PrivateLink 可讓客戶 AWS 以高可用性和可擴展的方式存取上託管的服務，同時保留 AWS 網路內的所有網路流量。服務使用者可以從 VPC 或其內部部署私下存取由 PrivateLink 提供支援的服務，而無需使用公 IPs，也不需要流量周遊網際網路。

修補

若要設定 VPC 端點，請參閱《AWS PrivateLink 指南》中的[AWS 服務 使用介面 VPC 端點存取](#)。

【EC2.58】VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(15)、NIST.800-53.r5 SC-7、

類別：保護 > 安全存取控制 > 存取控制

嚴重性：中

資源類型：AWS::EC2::VPC、AWS::EC2::VPCEndpoint

AWS Config 規則：[vpc-endpoint-enabled](#)

排程類型：定期

參數：

參數	必要	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
serviceName	必要	控制項評估的服務名稱	String	無法自訂	ssm-contacts
vpcIds	選用	VPC 端點的 Amazon VPC IDs 逗號分隔清單。如果提供，則如果 serviceName 參數中指定的服務	StringList	使用一或多個 VPC IDs 自訂	無預設值

參數	必要	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
		沒有其中一個 VPC 端點，則控制項會失敗。			

此控制項會檢查您管理的虛擬私有雲端 (VPC) 是否有 AWS Systems Manager Incident Manager Contacts 的介面 VPC 端點。如果 VPC 沒有 Systems Manager Incident Manager Contacts 的介面 VPC 端點，則控制項會失敗。此控制項會評估單一帳戶中的資源。

AWS PrivateLink 可讓客戶 AWS 以高可用性和可擴展的方式存取上託管的服務，同時保留 AWS 網路內的所有網路流量。服務使用者可以從 VPC 或其內部部署私下存取由 PrivateLink 提供支援的服務，而無需使用公 IPs，也不需要流量周遊網際網路。

修補

若要設定 VPC 端點，請參閱《AWS PrivateLink 指南》中的[AWS 服務 使用介面 VPC 端點存取](#)。

【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-75
NIST.800-53.r5 SC-7)

類別：保護 > 安全存取控制 > 存取控制

嚴重性：中

資源類型：AWS::EC2::VPC、AWS::EC2::VPCEndpoint

AWS Config 規則：[vpc-endpoint-enabled](#)

排程類型：定期

參數：

參數	必要	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
serviceNames	必要	控制項評估的服務名稱	String	無法自訂	ssm-incidents
vpcIds	選用	VPC 端點的 Amazon VPC IDs 逗號分隔清單。如果提供，則如果 serviceName 參數中指定的服務沒有其中一個 VPC 端點，則控制項會失敗。	StringList	使用一或多個 VPC IDs 自訂	無預設值

此控制項會檢查您管理的虛擬私有雲端 (VPC) 是否具有 AWS Systems Manager Incident Manager 的介面 VPC 端點。如果 VPC 沒有 Systems Manager Incident Manager 的介面 VPC 端點，則控制項會失敗。此控制項會評估單一帳戶中的資源。

AWS PrivateLink 可讓客戶 AWS 以高可用性和可擴展的方式存取上託管的服務，同時保留 AWS 網路內的所有網路流量。服務使用者可以從 VPC 或其內部部署私下存取由 PrivateLink 提供支援的服務，而無需使用公IPs，也不需要流量周遊網際網路。

修補

若要設定 VPC 端點，請參閱《AWS PrivateLink 指南》中的[AWS 服務 使用介面 VPC 端點存取](#)。

【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 (IMDSv2)

相關要求：PCI DSS v4.0.1/2.2.6

類別：保護 > 網路安全

嚴重性：低

資源類型：AWS::EC2::LaunchTemplate

AWS Config 規則：[ec2-launch-template-imdsv2-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已使用執行個體中繼資料服務第 2 版 (IMDSv2) 設定 Amazon EC2 啟動範本。IMDSv2 如果設定為 HttpTokens，則控制項會失敗 optional。

在支援的軟體版本上執行資源可確保最佳效能、安全性和最新功能的存取。定期更新可防範漏洞，這有助於確保穩定且有效率的使用者體驗。

修補

若要在 EC2 啟動範本上要求 IMDSv2，請參閱《Amazon EC2 使用者指南》中的[設定執行個體中繼資料服務選項](#)。

【EC2.171】 EC2 VPN 連線應該已啟用記錄

相關要求：CIS AWS Foundations Benchmark v3.0.0/5.3、PCI DSS v4.0.1/10.4.2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::EC2::VPNConnection

AWS Config 規則：[ec2-vpn-connection-logging-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查這兩個通道是否已啟用 AWS Site-to-Site Amazon CloudWatch Logs。如果 Site-to-Site 通道都未啟用 CloudWatch Logs，則控制項會失敗。

AWS Site-to-Site 日誌可讓您更深入了解 Site-to-Site VPN 部署。透過此功能，您可以存取站台對站台 VPN 連接日誌，其中提供 IP 安全性 (IPsec) 通道建立、網際網路金鑰交換 (IKE) 交涉，以及失效對等

偵測 (DPD) 通訊協定訊息的詳細資料。Site-to-Site日誌可以發佈到 CloudWatch Logs。此功能為客戶提供一個一致的方式，來存取和分析其所有站台對站台 VPN 連接的詳細日誌。

修補

若要在 EC2 VPN 連接上啟用通道記錄，請參閱[AWS 《Site-to-Site VPN 使用者指南》中的 Site-to-Site VPN 日誌](#)。AWS Site-to-Site

【EC2.172】 EC2 VPC 封鎖公開存取設定應封鎖網際網路閘道流量

類別：保護 > 安全網路組態 > 不可公開存取的資源

嚴重性：中

資源類型：AWS::EC2::VPCBlockPublicAccessOptions

AWS Config rule：ec2-vpc-bpa-internet-gateway-blocked (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
vpcBpaInternetGatewayBlockMode	VPC BPA 選項模式的字串值。	列舉	block-bidirectional, block-ingress	無預設值

此控制項會檢查 Amazon EC2 VPC 封鎖公開存取 (BPA) 設定是否設定為封鎖 中所有 Amazon VPCs網際網路閘道流量 AWS 帳戶。如果未將 VPC BPA 設定設定為封鎖網際網路閘道流量，則控制項會失敗。若要傳遞控制項，VPC BPA InternetGatewayBlockMode 必須設定為 block-bidirectional或 block-ingress。如果vpcBpaInternetGatewayBlockMode提供 參數，則只有在 的 VPC BPA 值InternetGatewayBlockMode符合 參數時，控制項才會通過。

在 中為您的帳戶設定 VPC BPA 設定，AWS 區域 可讓您封鎖在該區域中擁有VPCs 和子網路中的資源，使其無法透過網際網路閘道和僅限輸出網際網路閘道從網際網路到達或到達。如果您需要特定的

VPCs和子網路才能從網際網路連線或存取，您可以透過設定 VPC BPA 排除來排除它們。如需建立和刪除排除的指示，請參閱《Amazon VPC 使用者指南》中的[建立和刪除排除](#)。

修補

若要在帳戶層級啟用雙向 BPA，請參閱《Amazon VPC 使用者指南》中的[為您的帳戶啟用 BPA 雙向模式](#)。若要啟用僅限輸入 BPA，請參閱[將 VPC BPA 模式變更為僅限輸入](#)。若要在組織層級啟用 VPC BPA，請參閱[在組織層級啟用 VPC BPA](#)。

【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::EC2::SpotFleet

AWS Config 規則：[ec2-spot-fleet-request-ct-encryption-at-rest](#)

排程類型：已觸發變更

參數：無

此控制項會檢查指定啟動參數的 Amazon EC2 Spot Fleet 請求是否設定為為所有連接至 EC2 執行個體的 Amazon Elastic Block Store (Amazon EBS) 磁碟區啟用加密。如果 Spot Fleet 請求指定啟動參數，且未啟用請求中指定的一或多個 EBS 磁碟區的加密，則控制項會失敗。

為了多一層安全性，您應該啟用 Amazon EBS 磁碟區的加密。然後，加密操作會在託管 Amazon EC2 執行個體的伺服器上進行，這有助於確保靜態資料和執行個體與其連接的 EBS 儲存體之間傳輸中資料的安全性。Amazon EBS 加密是一種直接的加密解決方案，適用於與 EC2 執行個體相關聯的 EBS 資源。透過 EBS 加密，您不需要建置、維護和保護自己的金鑰管理基礎設施。建立加密磁碟區 AWS KMS keys 時，EBS 加密會使用。

備註

此控制項不會為使用啟動範本的 Amazon EC2 Spot Fleet 請求產生問題清單。它也不會為未明確指定 encrypted 參數值的 Spot Fleet 請求產生問題清單。

修補

無法直接加密現有的未加密 Amazon EBS 磁碟區。您只能在建立磁碟區時加密新磁碟區。

不過，如果您預設啟用加密，Amazon EBS 會使用 EBS 加密的預設金鑰來加密新的磁碟區。如果您未預設啟用加密，您可以在建立個別磁碟區時啟用加密。在這兩種情況下，您可以覆寫 EBS 加密的預設金鑰，並選擇客戶受管的 AWS KMS key。如需 EBS 加密的詳細資訊，請參閱《[Amazon EBS 使用者指南](#)》中的 [Amazon EBS 加密](#)。

如需有關建立 Amazon EC2 Spot 機群請求的資訊，請參閱《Amazon Elastic Compute Cloud 使用者指南》中的[建立 Spot 機群](#)。

【EC2.174】 EC2 DHCP 選項集應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::DHCPOptions

AWS Config 規則：[ec2-dhcp-options-tagged](#)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤金鑰清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 DHCP 選項集是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果選項集沒有任何標籤索引鍵，或者它沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果選項集沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws: 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都是由必要的標籤索引鍵和選用的標籤值所組成。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多 存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需有關將標籤新增至 Amazon EC2 DHCP 選項集的資訊，請參閱《[Amazon EC2 使用者指南](#)》中的 [標記您的 Amazon EC2 資源](#)。

【EC2.175】 EC2 啟動範本應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::LaunchTemplate

AWS Config 規則：[ec2-launch-template-tagged](#)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤金鑰清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 啟動範本是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果啟動範本沒有任何標籤索引鍵，或它沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果啟動範本沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws: 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都是由必要的標籤索引鍵和選用的標籤值所組成。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和

篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多 存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需有關將標籤新增至 Amazon EC2 啟動範本的資訊，請參閱《[Amazon EC2 使用者指南](#)》中的[標記您的 Amazon EC2 資源](#)。

【EC2.176】 EC2 字首清單應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::PrefixList

AWS Config 規則：[ec2-prefix-list-tagged](#)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤金鑰清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 字首清單是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果字首清單沒有任何標籤索引鍵，或者它沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果

字首清單沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 `aws:` 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都是由必要的標籤索引鍵和選用的標籤值所組成。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需有關將標籤新增至 Amazon EC2 字首清單的資訊，請參閱《[Amazon EC2 使用者指南](#)》中的[標記您的 Amazon EC2 資源](#)。

【EC2.177】應標記 EC2 流量鏡像工作階段

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::TrafficMirrorSession

AWS Config 規則：[ec2-traffic-mirror-session-tagged](#)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤金鑰清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 流量鏡像工作階段是否具有 `requiredKeyTags` 參數指定的標籤索引鍵。如果工作階段沒有任何標籤索引鍵，或沒有 `requiredKeyTags` 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 `requiredKeyTags` 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果工作階段沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 `aws:` 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都是由必要的標籤索引鍵和選用的標籤值所組成。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

 Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需有關將標籤新增至 Amazon EC2 流量鏡像工作階段的資訊，請參閱《[Amazon EC2 使用者指南](#)》中的[標記您的 Amazon EC2 資源](#)。Amazon EC2

【EC2.178】應標記 EC2 流量鏡像篩選條件

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::TrafficMirrorFilter

AWS Config 規則：[ec2-traffic-mirror-filter-tagged](#)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤金鑰清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 流量鏡像篩選條件是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果篩選條件沒有任何標籤索引鍵，或者它沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果篩選條件沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws: 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都是由必要的標籤索引鍵和選用的標籤值所組成。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需有關將標籤新增至 Amazon EC2 流量鏡像篩選條件的資訊，請參閱《[Amazon EC2 使用者指南](#)》中的[標記您的 Amazon EC2 資源](#)。Amazon EC2

【EC2.179】應標記 EC2 流量鏡像目標

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EC2::TrafficMirrorTarget

AWS Config 規則：[ec2-traffic-mirror-target-tagged](#)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤金鑰清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 流量鏡像目標是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果目標沒有任何標籤索引鍵，或沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果目標沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws: 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都是由必要的標籤索引鍵和選用的標籤值所組成。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱 [標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需將標籤新增至 Amazon EC2 流量鏡像目標的詳細資訊，請參閱《[Amazon EC2 使用者指南](#)》中的 [標記您的 Amazon EC2 資源](#)。Amazon EC2

【EC2.180】 EC2 網路介面應啟用來源/目的地檢查

類別：保護 > 網路安全

嚴重性：中

資源類型：AWS::EC2::NetworkInterface

AWS Config 規則：[ec2-enis-source-destination-check-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查是否針對由使用者管理的 Amazon EC2 彈性網路介面 (ENI) 啟用來源/目的地檢查。如果停用使用者受管 ENI 的來源/目的地檢查，則控制項會失敗。此控制項只會檢查下列 ENIs 類型：aws_codedstar_connections_managed、branch、efainterface、lambda 和 quicksight。

Amazon EC2 執行個體和連接的 ENIs 的來源/目的地檢查應該在整個 EC2 執行個體中一致地啟用和設定。每個 ENI 都有自己的來源/目的地檢查設定。如果已啟用來源/目的地檢查，Amazon EC2 會強制執行來源/目的地地址驗證，以確保執行個體是其接收的任何流量的來源或目的地。這透過防止資源處理意外流量和防止 IP 地址詐騙，提供額外的網路安全層。

 Note

如果您使用 EC2 執行個體做為 NAT 執行個體，且已停用其 ENI 的來源/目的地檢查，則可以改用 [NAT 閘道](#)。

修補

如需有關啟用 Amazon EC2 ENI 來源/目的地檢查的資訊，請參閱《Amazon EC2 使用者指南》中的[修改網路介面屬性](#)。

【EC2.181】 EC2 啟動範本應為連接的 EBS 磁碟區啟用加密

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::EC2::LaunchTemplate

AWS Config 規則：[ec2-launch-templates-ebs-volume-encrypted](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EC2 啟動範本是否啟用所有連接 EBS 磁碟區的加密。如果 EC2 啟動範本指定的任何 EBS False 磁碟區將加密參數設為 `false`，則控制項會失敗。

Amazon EBS 加密是直接加密解決方案，適用於與 Amazon EC2 執行個體相關聯的 EBS 資源。透過 EBS 加密，您不需要建置、維護和保護自己的金鑰管理基礎設施。建立加密磁碟區和快照 AWS KMS keys 時，EBS 加密會使用 `aws:kms` 加密。加密操作發生在託管 EC2 執行個體的伺服器上，這有助於確保 EC2 執行個體與其連接的 EBS 儲存體之間靜態資料和傳輸中資料的安全性。如需詳細資訊，請參閱「Amazon EBS 使用者指南」中的 [Amazon EBS 加密](#)。

您可以在手動啟動個別 EC2 執行個體期間啟用 EBS 加密。不過，使用 EC2 啟動範本和在這些範本中設定加密設定有幾個好處。您可以強制執行加密作為標準，並確保使用一致的加密設定。您也可以降低手動啟動執行個體時可能發生的錯誤和安全漏洞風險。

Note

當此控制項檢查 EC2 啟動範本時，只會評估範本明確指定的 EBS 加密設定。評估不包含繼承自帳戶層級 EBS 加密設定、AMI 區塊型設備映射或來源快照加密狀態的加密設定。

修補

建立 Amazon EC2 啟動範本之後，您就無法修改它。不過，您可以建立新的啟動範本版本，並變更該新範本版本中的加密設定。您也可以指定新版本做為啟動範本的預設版本。然後，如果您從啟動範本啟動 EC2 執行個體，但未指定範本版本，EC2 會在啟動執行個體時使用預設版本的設定。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的 [修改啟動範本](#)。

【EC2.182】 應為 Amazon EBS 快照啟用封鎖公開存取設定

類別：保護 > 安全網路組態 > 資源不可公開存取

嚴重性：高

資源類型：AWS::EC2::SnapshotBlockPublicAccess

AWS Config 規則：[ebs-snapshot-block-public-access](#)

排程類型：變更已觸發

參數：無

此控制項會檢查是否啟用帳戶層級封鎖公開存取，以防止與所有人共用 Amazon EBS 快照。如果未啟用封鎖公有存取來封鎖與所有人共用 Amazon EBS 快照，則控制項會失敗。

若要防止公開共用 Amazon EBS 快照，您可以啟用快照的封鎖公開存取。在區域中啟用快照的封鎖公開存取後，在該區域中公開共用快照的任何嘗試都會自動封鎖。這有助於提高快照的安全性，並保護快照資料免於未經授權的或意外的存取。

修補

若要啟用快照的封鎖公開存取，請參閱《[Amazon EBS 使用者指南](#)》中的設定 Amazon EBS 快照的封鎖公開存取。針對封鎖公開存取，選擇封鎖所有公開存取。

【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::EC2::VPNConnection

AWS Config 規則：[ec2-vpn-connection-ike-version-check](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 an AWS Site-to-Site VPN 連接是否設定為使用 IKEv2 通訊協定。如果 Site-to-Site VPN 連接允許 IKEv1 通訊協定或未明確限制所有 VPN 通道上的 IKEv2，則控制項會失敗。

相較於舊版 IKEv1 提供更強大的密碼編譯演算法和改善的安全功能，包括內建的 denial-of-service 攻擊防護和增強的身分驗證機制。IKEv1 在其金鑰交換程序中具有已知的漏洞和弱點，攻擊者可以利用這些漏洞和弱點來入侵 VPN 通道安全性。透過強制執行 IKEv2-only 的連線，您可以減少攻擊面，並確保 VPN 通訊使用現代的業界標準加密通訊協定，以更好地保護傳輸中的資料。

修補

若要更新 EC2 VPN 連接上 VPN 通道的 IKE 版本，請參閱[Site-to-Site 使用者指南](#)中的修改 AWS 站對站 VPN 通道選項。AWS Site-to-Site

Auto Scaling 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 Amazon EC2 Auto Scaling 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【AutoScaling.1】與負載平衡器相關聯的 Auto Scaling 群組應使用 ELB 運作狀態檢查

相關要求：PCI DSS v3.2.1/2.2、NIST.800-53.r5 CA-7、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 SI-2

類別：識別 > 清查

嚴重性：低

資源類型：AWS::AutoScaling::AutoScalingGroup

AWS Config 規則：[autoscaling-group-elb-healthcheck-required](#)

排程類型：已觸發變更

參數：無

此控制項會檢查與負載平衡器相關聯的 Amazon EC2 Auto Scaling 群組是否使用 Elastic Load Balancing (ELB) 運作狀態檢查。如果 Auto Scaling 群組不使用 ELB 運作狀態檢查，則控制項會失敗。

ELB 運作狀態檢查有助於確保 Auto Scaling 群組可以根據負載平衡器提供的其他測試來判斷執行個體的運作狀態。使用 Elastic Load Balancing 運作狀態檢查也有助於支援使用 EC2 Auto Scaling 群組的應用程式可用性。

修補

若要新增 Elastic Load Balancing 運作狀態檢查，請參閱《Amazon EC2 Auto Scaling 使用者指南》中的[新增 Elastic Load Balancing 運作狀態檢查](#)。

【AutoScaling.2】Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::AutoScaling::AutoScalingGroup

AWS Config 規則：[autoscaling-multiple-az](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
minAvailabilityZones	可用區域數目下限	列舉	2, 3, 4, 5, 6	2

此控制項會檢查 Amazon EC2 Auto Scaling 群組是否至少跨越指定數量的可用區域 (AZs)。如果 Auto Scaling 群組未至少跨越指定數量 AZs，則控制項會失敗。除非您提供最低 AZs 數量的自訂參數值，否則 Security Hub CSPM 會使用兩個 AZs 的預設值。

不跨越多個 AZs Auto Scaling 群組無法在另一個可用區域中啟動執行個體，以便在設定的單一可用區域無法使用時予以補償。不過，在某些使用案例中，可能會偏好具有單一可用區域的 Auto Scaling 群組，例如批次工作或需要將跨可用區域傳輸成本保持在最低限度。在這種情況下，您可以停用此控制項或隱藏其問題清單。

修補

若要將 AZs 新增至現有的 Auto Scaling 群組，請參閱《Amazon EC2 Auto Scaling 使用者指南》中的[新增和移除可用區域](#)。

【AutoScaling.3】 Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 (IMDSv2)

相關要求：NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/2.2.6

類別：保護 > 安全網路組態

嚴重性：高

資源類型：AWS::AutoScaling::LaunchConfiguration

AWS Config 規則：[autoscaling-launchconfig-requires-imsdv2](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EC2 Auto Scaling 群組啟動的所有執行個體上是否啟用 IMDSv2。Amazon EC2 Auto Scaling 如果執行個體中繼資料服務 (IMDS) 版本未包含在啟動組態中或設定為 `token optional`，則控制項會失敗，這是允許 IMDSv1 或 IMDSv2 的設定。

IMDS 提供執行個體的資料，可用來設定或管理執行中的執行個體。

IMDS 第 2 版新增了 IMDSv1 中無法使用的新保護，以進一步保護您的 EC2 執行個體。

修補

Auto Scaling 群組一次與一個啟動組態相關聯。您無法在建立啟動組態之後對其進行修改。若要變更 Auto Scaling 群組的啟動組態，請使用現有的啟動組態做為啟用 IMDSv2 的新啟動組態的基礎。如需詳細資訊，請參閱《Amazon EC2 使用者指南》中的[設定新執行個體的執行個體中繼資料選項](#)。

【AutoScaling.4】Auto Scaling 群組啟動組態的中繼資料回應跳轉限制不應大於 1

 Important

Security Hub CSPM 已於 2024 年 4 月淘汰此控制項。如需詳細資訊，請參閱[Security Hub CSPM 控制項的變更日誌](#)。

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

類別：保護 > 安全網路組態

嚴重性：高

資源類型：AWS::AutoScaling::LaunchConfiguration

AWS Config 規則：[autoscaling-launch-config-hop-limit](#)

排程類型：已觸發變更

參數：無

此控制項會檢查中繼資料字符可以移動的網路躍點數量。如果中繼資料回應跳轉限制大於 1，則控制項會失敗。

Instance Metadata Service (IMDS) 提供 Amazon EC2 執行個體的中繼資料資訊，對於應用程式組態很有用。將中繼資料服務的 HTTP PUT 回應限制為只有 EC2 執行個體可保護 IMDS 免於未經授權的使用。

IP 封包中的存留時間 (TTL) 欄位在每個躍點上減少一個。此減少項目可用來確保封包不會在 EC2 外部傳輸。IMDSv2 會保護可能已錯誤設定為開放路由器、第 3 層防火牆、VPNs、通道或 NAT 裝置的 EC2 執行個體，以防止未經授權的使用者擷取中繼資料。使用 IMDSv2 時，包含秘密字符的 PUT 回應無法在執行個體之外移動，因為預設中繼資料回應跳轉限制設定為 1。不過，如果此值大於 1，字符可能會離開 EC2 執行個體。

修補

若要修改現有啟動組態的中繼資料回應跳轉限制，請參閱《Amazon EC2 使用者指南》中的[修改現有執行個體的執行個體中繼資料選項](#)。

【Autoscaling.5】 使用 Auto Scaling 群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全網路組態 > 不可公開存取的資源

嚴重性：高

資源類型：AWS::AutoScaling::LaunchConfiguration

AWS Config 規則：[autoscaling-launch-config-public-ip-disabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Auto Scaling 群組相關聯的啟動組態是否將[公有 IP 地址](#)指派給群組的執行個體。如果相關聯的啟動組態指派公有 IP 地址，則控制項會失敗。

Auto Scaling 群組啟動組態中的 Amazon EC2 執行個體不應具有相關聯的公有 IP 地址，但在有限的邊緣情況下除外。Amazon EC2 執行個體應只能從負載平衡器後方存取，而不是直接公開至網際網路。

修補

Auto Scaling 群組一次與一個啟動組態相關聯。您無法在建立啟動組態之後對其進行修改。若要變更 Auto Scaling 群組的啟動組態，請使用現有啟動組態作為新啟動組態的基礎。然後更新 Auto Scaling 群組，以便使用新啟動組態。如需 step-by-step 說明，請參閱《Amazon EC2 [Auto Scaling 使用者指](#)

[南》中的變更 Auto Scaling 群組的啟動組態](#)。Amazon EC2 Auto Scaling 建立新的啟動組態時，請在其他組態下，針對進階詳細資訊、IP 地址類型，選擇不要將公有 IP 地址指派給任何執行個體。

變更啟動組態後，Auto Scaling 會使用新的組態選項啟動新的執行個體。現有的執行個體不受影響。若要更新現有的執行個體，建議您重新整理執行個體，或允許自動擴展，以根據您的終止政策逐漸將較舊的執行個體取代為較新的執行個體。如需更新 Auto Scaling 執行個體的詳細資訊，請參閱《Amazon EC2 [Auto Scaling 使用者指南](#)》中的[更新 Auto Scaling 執行個體](#)。Amazon EC2 Auto Scaling

【AutoScaling.6】Auto Scaling 群組應在多個可用區域中使用多個執行個體類型

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2(2)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::AutoScaling::AutoScalingGroup

AWS Config 規則：[autoscaling-multiple-instance-types](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EC2 Auto Scaling 群組是否使用多個執行個體類型。如果 Auto Scaling 群組只定義一個執行個體類型，則控制項會失敗。

您可以將應用程式部署於在多個可用區域執行的多種執行個體類型之間，以增強可用性。Security Hub CSPM 建議使用多個執行個體類型，以便在您選擇的可用區域中執行個體容量不足時 Auto Scaling 群組可以啟動另一個執行個體類型。

修補

若要建立具有多個執行個體類型的 Auto Scaling 群組，請參閱《Amazon EC2 [Auto Scaling 使用者指南](#)》中的[具有多個執行個體類型和購買選項的 Auto Scaling 群組](#)。Amazon EC2 Auto Scaling

【AutoScaling.9】Amazon EC2 Auto Scaling 群組應使用 Amazon EC2 啟動範本

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

類別：識別 > 資源組態

嚴重性：中

資源類型：AWS::AutoScaling::AutoScalingGroup

AWS Config 規則：[autoscaling-launch-template](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已從 Amazon EC2 EC2 Auto Scaling 群組。如果未使用啟動範本建立 Amazon EC2 Auto Scaling 群組，或未在混合執行個體政策中指定啟動範本，則此控制項會失敗。

您可以從 EC2 啟動範本或啟動組態建立 EC2 Auto Scaling 群組。不過，使用啟動範本建立 Auto Scaling 群組可確保您可以存取最新的功能和改進。

修補

若要使用 EC2 啟動範本建立 Auto Scaling 群組，請參閱《Amazon EC2 [Auto Scaling 使用者指南](#)》中的[使用啟動範本建立 Auto Scaling 群組](#)。Amazon EC2 Auto Scaling 如需有關如何以啟動範本取代啟動組態的資訊，請參閱《Amazon EC2 使用者指南》中的[以啟動範本取代啟動組態](#)。

【AutoScaling.10】應標記 EC2 Auto Scaling 群組

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::AutoScaling::AutoScalingGroup

AWS Config rule：tagged-autoscaling-autoscalinggroup (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EC2 Auto Scaling 群組是否具有具有參數 中定義之特定金鑰的標籤 `requiredTagKeys`。如果 Auto Scaling 群組沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果 Auto Scaling 群組未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Auto Scaling 群組，請參閱《Amazon EC2 [Auto Scaling 使用者指南](#)》中的 [標籤 Auto Scaling 群組和執行個體](#)。Amazon EC2 Auto Scaling

Amazon ECR 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 Amazon Elastic Container Registry (Amazon ECR) 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【ECR.1】 ECR 私有儲存庫應設定映像掃描

相關要求：NIST.800-53.r5 RA-5、PCI DSS v4.0.1/6.2.3、PCI DSS v4.0.1/6.2.4

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：高

資源類型：AWS::ECR::Repository

AWS Config 規則：[ecr-private-image-scanning-enabled](#)

排程類型：定期

參數：無

此控制項會檢查私有 Amazon ECR 儲存庫是否已設定映像掃描。如果私有 ECR 儲存庫未設定為在推送或連續掃描時掃描，則控制項會失敗。

ECR 映像掃描有助於識別容器映像中的軟體漏洞。在 ECR 儲存庫上設定映像掃描會新增一層驗證，以確保所存放映像的完整性和安全性。

修補

若要設定 ECR 儲存庫的影像掃描，請參閱《Amazon Elastic Container Registry 使用者指南》中的[影像掃描](#)。

【ECR.2】 ECR 私有儲存庫應設定標籤不可變性

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-8(1)

類別：識別 > 庫存 > 標記

嚴重性：中

資源類型：AWS::ECR::Repository

AWS Config 規則：[ecr-private-tag-immutability-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查私有 ECR 儲存庫是否已啟用標籤不可變性。如果私有 ECR 儲存庫已停用標籤不可變性，則此控制項會失敗。如果標籤不可變性已啟用且值為 `IMMUTABLE`，則此規則會通過 `IMMUTABLE`。

Amazon ECR 標籤抗擾性可讓客戶依賴影像的描述性標籤作為追蹤和唯一識別影像的可靠機制。不可變標籤是靜態的，這表示每個標籤都是指唯一的影像。這可改善可靠性和可擴展性，因為使用靜態標籤一律會導致部署相同的映像。設定時，標籤不可變性可防止標籤遭到覆寫，從而減少攻擊面。

修補

若要建立已設定不可變標籤的儲存庫，或更新現有儲存庫的影像標籤可變性設定，請參閱《Amazon Elastic Container Registry 使用者指南》中的[影像標籤可變性](#)。

【ECR.3】 ECR 儲存庫應至少設定一個生命週期政策

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

類別：識別 > 資源組態

嚴重性：中

資源類型：AWS::ECR::Repository

AWS Config 規則：[ecr-private-lifecycle-policy-configured](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon ECR 儲存庫是否已設定至少一個生命週期政策。如果 ECR 儲存庫未設定任何生命週期政策，則此控制會失敗。

Amazon ECR 生命週期政策可讓您指定儲存庫中映像的生命週期管理。透過設定生命週期政策，您可以根據存留期或計數自動清除未使用的映像和映像過期。自動化這些任務可協助您避免意外使用儲存庫中過時的映像。

修補

若要設定生命週期政策，請參閱《Amazon Elastic Container Registry 使用者指南》中的[建立生命週期政策預覽](#)。

【ECR.4】 ECR 公有儲存庫應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::ECR::PublicRepository

AWS Config rule：tagged-ecr-publicrepository (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon ECR 公有儲存庫是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果公有儲存庫沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果公有儲存庫未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《[標記您的 AWS 資源](#)》中的 [標記您的 AWS 資源](#) 一般參考。

修補

若要將標籤新增至 ECR 公有儲存庫，請參閱《[Amazon Elastic Container Registry 使用者指南](#)》中的 [標記 Amazon ECR 公有儲存庫](#)。

【ECR.5】 ECR 儲存庫應使用客戶受管加密 AWS KMS keys

相關要求：NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 SI-7(6)、NIST.800-53.r5 AU-9

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::ECR::Repository

AWS Config 規則：[ecr-repository-cmk-encryption-enabled](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
kmsKeyArns	AWS KMS keys 要包含在評估中的 Amazon Resource Name (ARNs)清單。如果 ECR 儲存庫未在清單中使用 KMS 金鑰加密，則控制項會產生FAILED問題清單。	StringList (最多 10 個項目)	現有 KMS 金鑰的 1–10 ARNs。例如：arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab	無預設值

此控制項會檢查 Amazon ECR 儲存庫是否使用客戶受管的靜態加密 AWS KMS key。如果未使用客戶受管 KMS 金鑰加密 ECR 儲存庫，則控制項會失敗。您可以選擇性地為控制項指定要包含在評估中的 KMS 金鑰清單。

根據預設，Amazon ECR 會使用 AES-256 演算法，使用 Amazon S3 受管金鑰 (SSE-S3) 加密儲存庫資料。如需其他控制，您可以設定 Amazon ECR 改用 AWS KMS key (SSE-KMS 或 DSSE-KMS) 來加密資料。KMS 金鑰可以是：Amazon ECR 為您建立和管理 AWS 受管金鑰的，並具有別名 `aws/ecr`，或您在 中建立和管理的客戶受管金鑰 AWS 帳戶。使用客戶受管 KMS 金鑰，您可以完全控制金鑰。這包括定義和維護金鑰政策、管理授予、輪換密碼編譯材料、指派標籤、建立別名，以及啟用和停用金鑰。

 Note

AWS KMS 支援跨帳戶存取 KMS 金鑰。如果 ECR 儲存庫使用另一個帳戶擁有的 KMS 金鑰加密，則此控制項不會在評估儲存庫時執行跨帳戶檢查。控制項不會評估 Amazon ECR 在為儲存庫執行密碼編譯操作時是否可以存取和使用金鑰。

修補

您無法變更現有 ECR 儲存庫的加密設定。不過，您可以為後續建立的 ECR 儲存庫指定不同的加密設定。Amazon ECR 支援對個別儲存庫使用不同的加密設定。

如需 ECR 儲存庫加密選項的詳細資訊，請參閱《Amazon ECR 使用者指南》中的[靜態加密](#)。如需客戶受管的詳細資訊 AWS KMS keys，請參閱《AWS Key Management Service 開發人員指南[AWS KMS keys](#)》中的。

Amazon ECS 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 Amazon Elastic Container Service (Amazon ECS) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【ECS.1】 Amazon ECS 任務定義應具有安全的聯網模式和使用使用者定義 Important

Security Hub CSPM 已於 2026 年 3 月淘汰此控制。如需詳細資訊，請參閱[Security Hub CSPM 控制項的變更日誌](#)。您可以參考下列控制項來評估特殊權限組態、網路模式組態和使用使用者組態：

- [【ECS.4】 ECS 容器應以非特殊權限執行](#)
- [【ECS.17】 ECS 任務定義不應使用主機網路模式](#)
- [【ECS.20】 ECS 任務定義應在 Linux 容器定義中設定非根使用者](#)
- [【ECS.21】 ECS 任務定義應在 Windows 容器定義中設定非管理員使用者](#)

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

類別：保護 > 安全存取管理

嚴重性：高

資源類型：AWS::ECS::TaskDefinition

AWS Config 規則：[ecs-task-definition-user-for-host-mode-check](#)

排程類型：變更已觸發

參數：

- SkipInactiveTaskDefinitions：true (不可自訂)

此控制項會檢查具有主機聯網模式的作用中 Amazon ECS 任務定義是否具有 privileged 或 user 容器定義。對於主機網路模式和容器定義為 privileged=false、空白和 或空白的任務定義 user=root，控制項會失敗。

此控制項只會評估 Amazon ECS 任務定義的最新作用中修訂。

此控制的目的是確保在您執行使用主機網路模式的任務時，刻意定義存取。如果任務定義具有更高的權限，是因為您已選擇該組態。當任務定義已啟用主機聯網，而且您未選擇提升的權限時，此控制項會檢查是否有非預期的權限提升。

修補

如需有關如何更新任務定義的資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的[更新任務定義](#)。

當您更新任務定義時，不會更新從上一個任務定義啟動的執行中任務。若要更新執行中的任務，您必須使用新的任務定義重新部署任務。

【ECS.2】 ECS 服務不應自動為其指派公有 IP 地址

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全網路組態 > 資源不可公開存取

嚴重性：高

資源類型：AWS::ECS::Service

AWS Config rule : `ecs-service-assign-public-ip-disabled` (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon ECS 服務是否設定為自動指派公有 IP 地址。如果 `AssignPublicIP` 為 `ENABLED`，則此控制項會失敗。如果 `AssignPublicIP` 是 `DISABLED`，則此控制項會通過。

公有 IP 地址是從網際網路連線的 IP 地址。如果您使用公有 IP 地址啟動 Amazon ECS 執行個體，則可以從網際網路存取 Amazon ECS 執行個體。Amazon ECS 服務不應公開存取，因為這可能會允許意外存取您的容器應用程式伺服器。

修補

首先，您必須為叢集建立使用 `awsvpc` 網路模式的任務定義，並為指定 `FARGATErequiresCompatibilities`。然後，針對運算組態，選擇啟動類型和 `FARGATE`。最後，在聯網欄位中，關閉公有 IP 以停用服務的自動公有 IP 指派。

【ECS.3】 ECS 任務定義不應共用主機的程序命名空間

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

類別：識別 > 資源組態

嚴重性：高

資源類型：AWS::ECS::TaskDefinition

AWS Config 規則：[ecs-task-definition-pid-mode-check](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon ECS 任務定義是否設定為與其容器共用主機的程序命名空間。如果任務定義與在其上執行的容器共用主機的程序命名空間，則控制項會失敗。此控制項只會評估 Amazon ECS 任務定義的最新作用中修訂。

程序 ID (PID) 命名空間可在程序之間進行區隔。它可防止系統程序可見，並允許重複使用 PIDs，包括 PID 1。如果主機的 PID 命名空間與容器共用，則可讓容器查看主機系統上的所有程序。這可減少主機

和容器之間程序層級隔離的好處。這些情況可能會導致未經授權存取主機本身的程序，包括操作和終止它們的能力。客戶不應與在其上執行的容器共用主機的程序命名空間。

修補

若要在任務定義pidMode上設定，請參閱《Amazon Elastic Container Service 開發人員指南》中的[任務定義參數](#)。

【ECS.4】ECS 容器應以非特殊權限執行

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

類別：保護 > 安全存取管理 > 根使用者存取限制

嚴重性：高

資源類型：AWS::ECS::TaskDefinition

AWS Config 規則：[ecs-containers-nonprivileged](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon ECS 任務定義之容器定義中的 privileged 參數是否設定為 true。如果此參數等於，則控制項會失敗true。此控制項只會評估 Amazon ECS 任務定義的最新作用中修訂。

我們建議您從 ECS 任務定義中移除提升的權限。當權限參數為 true，容器會在主機容器執行個體上獲得更高的權限（類似於根使用者）。

修補

若要在任務定義上設定 privileged 參數，請參閱《Amazon Elastic Container Service 開發人員指南》中的[進階容器定義參數](#)。

【ECS.5】ECS 任務定義應將容器設定為僅限對根檔案系統的唯一讀存取

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

類別：保護 > 安全存取管理

嚴重性：高

資源類型：AWS::ECS::TaskDefinition

AWS Config 規則：[ecs-containers-readonly-access](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 ECS 任務定義是否將容器設定為僅限對掛載根檔案系統的唯一存取。如果 ECS 任務定義之容器定義中的 `readonlyRootFilesystem` 參數設定為 `false`，或該參數不存在於任務定義內的容器定義中，則控制項會失敗。此控制項只會評估 Amazon ECS 任務定義的最新作用中修訂。

如果 `readonlyRootFilesystem` 參數在 Amazon ECS 任務定義 `true` 中設定為 `true`，則 ECS 容器會獲得其根檔案系統的唯一存取權。這樣可以減少安全攻擊向量，因為如果沒有對檔案系統資料夾和目錄具有讀寫許可的明確磁碟區掛載，則無法竄改或寫入容器執行個體的根檔案系統。啟用此選項也會遵循最低權限原則。

Note

Windows 容器不支援 `readonlyRootFilesystem` 參數。`runtimePlatform` 設定為指定 `WINDOWS_SERVER` 作業系統系列的任務定義會標記為 `NOT_APPLICABLE`，而且不會為此控制項產生問題清單。

修補

若要授予 Amazon ECS 容器對其根檔案系統的唯一存取權，請將 `readonlyRootFilesystem` 參數新增至容器的任務定義，並將參數的值設定為 `true`。如需有關任務定義參數以及如何將其新增至任務定義的資訊，請參閱《[Amazon Elastic Container Service 開發人員指南](#)》中的 [Amazon ECS 任務定義](#) 和 [更新任務定義](#)。

【ECS.8】不應將秘密做為容器環境變數傳遞

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/8.6.2

類別：保護 > 安全開發 > 非硬式編碼的登入資料

嚴重性：高

資源類型：AWS::ECS::TaskDefinition

AWS Config 規則：[ecs-no-environment-secrets](#)

排程類型：變更已觸發

參

數：secretKeys：AWS_ACCESS_KEY_ID、AWS_SECRET_ACCESS_KEY、ECS_ENGINE_AUTH_DATA
(不可自訂)

此控制項會檢查容器定義 environment 參數中任何變數的索引鍵值是否包含 AWS_ACCESS_KEY_ID、AWS_SECRET_ACCESS_KEY 或 ECS_ENGINE_AUTH_DATA。如果任何容器定義中的單一環境變數等於 AWS_ACCESS_KEY_ID、或 AWS_SECRET_ACCESS_KEY，則此控制項會失敗 ECS_ENGINE_AUTH_DATA。此控制項不包含從 Amazon S3 等其他位置傳入的環境變數。此控制項只會評估 Amazon ECS 任務定義的最新作用中修訂。

AWS Systems Manager 參數存放區可協助您改善組織的安全狀態。我們建議您使用參數存放區來存放秘密和登入資料，而不是直接將秘密和登入資料傳遞到您的容器執行個體或硬式編碼到您的程式碼。

修補

若要使用 SSM 建立參數，請參閱 AWS Systems Manager 《使用者指南》中的 [建立 Systems Manager 參數](#)。如需建立指定秘密之任務定義的詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的 [使用 Secrets Manager 指定敏感資料](#)。

【ECS.9】ECS 任務定義應具有記錄組態

相關要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

類別：識別 > 記錄日誌

嚴重性：高

資源類型：AWS::ECS::TaskDefinition

AWS Config 規則：[ecs-task-definition-log-configuration](#)

排程類型：變更已觸發

參數：無

此控制項會檢查最新的作用中 Amazon ECS 任務定義是否已指定記錄組態。如果任務定義未定義 logConfiguration 屬性，或至少有一個容器定義中的值 logDriver 為 null，則控制項會失敗。

記錄可協助您維護 Amazon ECS 的可靠性、可用性和效能。從任務定義收集資料可提供可見性，這可協助您偵錯程序並尋找錯誤的根本原因。如果您使用的是不需要在 ECS 任務定義中定義的記錄解決方案（例如第三方記錄解決方案），您可以在確保正確擷取和交付您的日誌之後停用此控制項。

修補

若要定義 Amazon ECS 任務定義的日誌組態，請參閱《Amazon Elastic Container Service 開發人員指南》中的[在任務定義中指定日誌組態](#)。

【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行

相關要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：AWS::ECS::Service

AWS Config 規則：[ecs-fargate-latest-platform-version](#)

排程類型：變更已觸發

參數：

- latestLinuxVersion: 1.4.0（不可自訂）
- latestWindowsVersion: 1.0.0（不可自訂）

此控制項會檢查 Amazon ECS Fargate 服務是否正在執行最新的 Fargate 平台版本。如果平台版本不是最新的，則此控制項會失敗。

AWS Fargate 平台版本是指 Fargate 任務基礎設施的特定執行期環境，這是核心和容器執行期版本的組合。新的平台版本會隨著執行時間環境的演進而發佈。例如，可能會針對核心或作業系統更新、新功能、錯誤修正或安全性更新發行新版本。系統會為 Fargate 任務自動部署安全性更新與修補程式。如果發現影響平台版本的安全問題，請 AWS 修補平台版本。

修補

若要更新現有服務，包括其平台版本，請參閱《Amazon Elastic Container Service 開發人員指南》中的[更新服務](#)。

【ECS.12】 ECS 叢集應使用 Container Insights

相關要求：NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::ECS::Cluster

AWS Config 規則：[ecs-container-insights-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 ECS 叢集是否使用 Container Insights。如果未為叢集設定 Container Insights，則此控制項會失敗。

監控是維護 Amazon ECS 叢集可靠性、可用性和效能的重要部分。使用 CloudWatch Container Insights 來收集、彙整和摘要您容器化應用程式及微服務中的指標及日誌。CloudWatch 會自動收集 CPU、記憶體、磁碟和網路等許多資源的指標。Container Insights 還提供診斷資訊，例如容器重新啟動故障，協助您快速隔離和解決這些故障。您也可以為 Container Insights 收集的指標設定 CloudWatch 警示。

修補

若要使用 Container Insights，請參閱《Amazon CloudWatch 使用者指南》中的[更新服務](#)。

【ECS.13】 ECS 服務應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::ECS::Service

AWS Config rule：tagged-ecs-service (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon ECS 服務是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果服務沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果服務未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《[標記您的 AWS 資源](#)》中的 [標記您的 AWS 資源](#) 一般參考。

修補

若要將標籤新增至 ECS 服務，請參閱《[Amazon Elastic Container Service 開發人員指南](#)》中的標記 [Amazon ECS 資源](#)。

【ECS.14】ECS 叢集應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::ECS::Cluster

AWS Config rule：tagged-ecs-cluster (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon ECS 叢集是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果叢集沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果叢集未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#)AWS 一般參考。

修補

若要將標籤新增至 ECS 叢集，請參閱《[Amazon Elastic Container Service 開發人員指南](#)》中的標記 [Amazon ECS 資源](#)。

【ECS.15】 ECS 任務定義應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::ECS::TaskDefinition

AWS Config rule：tagged-ecs-taskdefinition (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon ECS 任務定義是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果任務定義沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果任務定義未標記任何索引鍵，則 會失敗。系統會 aws: 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 ECS 任務定義，請參閱 [《Amazon Elastic Container Service 開發人員指南》](#) 中的標記 [Amazon ECS 資源](#)。

【ECS.16】 ECS 任務集不應自動指派公有 IP 地址

相關要求：PCI DSS v4.0.1/1.4.4

類別：保護 > 安全網路組態 > 不可公開存取的資源

嚴重性：高

資源類型：AWS::ECS::TaskSet

AWS Config rule：ecs-taskset-assign-public-ip-disabled (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon ECS 任務集是否設定為自動指派公有 IP 地址。如果 AssignPublicIP 設定為 `ENABLED`，則控制項會失敗。

公有 IP 地址可從網際網路存取。如果您使用公有 IP 地址設定任務集，則可以從網際網路連線與任務集相關聯的資源。不應公開存取 ECS 任務集，因為這可能會允許意外存取您的容器應用程式伺服器。

修補

若要更新 ECS 任務集，使其不使用公有 IP 地址，請參閱 [《Amazon Elastic Container Service 開發人員指南》](#) 中的 [使用主控台更新 Amazon ECS 任務定義](#)。

【ECS.17】 ECS 任務定義不應使用主機網路模式

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::ECS::TaskDefinition

AWS Config 規則：[ecs-task-definition-network-mode-not-host](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon ECS 任務定義的最新作用中修訂是否使用host網路模式。如果 ECS 任務定義的最新作用中修訂使用host網路模式，則控制項會失敗。

使用host網路模式時，Amazon ECS 容器的聯網會直接繫結至執行容器的基礎主機。因此，此模式允許容器連線到主機上的私有迴路網路服務，並模擬主機。其他重大缺點是，使用host網路模式時無法重新映射容器連接埠，而且您無法在每個主機上執行多個任務的單一執行個體。

修補

如需 Amazon EC2 執行個體上託管之 Amazon EC2 任務的聯網模式和選項的相關資訊，請參閱 [《Amazon Elastic Container Service 開發人員指南》](#) 中的 [EC2 啟動類型的 Amazon ECS 任務聯網選項](#)。如需有關建立新的任務定義修訂和指定不同網路模式的資訊，請參閱該指南中的 [更新 Amazon ECS 任務定義](#)。

如果 Amazon ECS 任務定義是由 建立 AWS Batch，請參閱[AWS Batch 任務的網路模式](#)以了解網路模式和 AWS Batch 任務類型的典型用量，並選擇安全選項。

【ECS.18】 ECS 任務定義應針對 EFS 磁碟區使用傳輸中加密

類別：保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::ECS::TaskDefinition

AWS Config 規則：[ecs-task-definition-efs-encryption-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon ECS 任務定義的最新作用中修訂是否針對 EFS 磁碟區使用傳輸中加密。如果 ECS 任務定義的最新作用中修訂已停用 EFS 磁碟區的傳輸中加密，則控制項會失敗。

Amazon EFS 磁碟區提供簡單、可擴展且持久的共用檔案儲存，可用於 Amazon ECS 任務。Amazon EFS 支援使用 Transport Layer Security (TLS) 加密傳輸中的資料。當傳輸中的資料加密宣告為 EFS 檔案系統的掛載選項時，Amazon EFS 會在掛載檔案系統時與您的 EFS 檔案系統建立安全的 TLS 連線。

修補

如需使用 EFS 磁碟區為 Amazon ECS 任務定義啟用傳輸中加密的資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的[步驟 5：建立任務定義](#)。

【ECS.19】 ECS 容量提供者應啟用受管終止保護

類別：保護 > 資料保護

嚴重性：中

資源類型：AWS::ECS::CapacityProvider

AWS Config 規則：[ecs-capacity-provider-termination-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon ECS 容量提供者是否已啟用受管終止保護。如果未在 ECS 容量提供者上啟用受管終止保護，則控制項會失敗。

Amazon ECS 容量提供者會管理叢集中任務的基礎設施擴展。當您為容量使用 EC2 執行個體時，可以使用 Auto Scaling 群組管理 EC2 執行個體。受管終止保護可讓叢集自動擴展控制哪些執行個體會終止。使用受管終止保護時，Amazon ECS 只會終止沒有執行 Amazon ECS 任務的 EC2 執行個體。

Note

使用受管終止保護時，也必須使用受管擴展，否則受管終止保護無法運作。

修補

若要啟用 Amazon ECS 容量提供者的受管終止保護，請參閱《Amazon Elastic Container Service 開發人員指南》中的[更新 Amazon ECS 容量提供者的受管終止保護](#)。

【ECS.20】 ECS 任務定義應在 Linux 容器定義中設定非根使用者

類別：保護 > 安全存取管理 > 根使用者存取限制

嚴重性：中

資源類型：AWS::ECS::TaskDefinition

AWS Config 規則：[ecs-task-definition-linux-user-non-root](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon ECS 任務定義的最新作用中修訂是否將 Linux 容器設定為以非根使用者身分執行。如果任何容器的預設根使用者已設定或使用者組態不存在，則控制項會失敗。

當 Linux 容器以根權限執行時，會帶來數個重大的安全風險。根使用者在容器內具有不受限制的存取。這種更高的存取會增加容器逸出攻擊的風險，攻擊者可能會中斷容器隔離並存取基礎主機系統。如果以根身分執行的容器遭到入侵，攻擊者可能會利用它來存取或修改主機系統資源，進而影響其他容器或主機本身。此外，根存取可以啟用權限提升攻擊，讓攻擊者獲得容器預期範圍以外的額外許可。ECS 任務定義中的使用者參數可以多種格式指定使用者，包括使用者名稱、使用者 ID、含群組的使用者名稱或含群組 ID 的 UID。在設定任務定義時，請務必注意這些各種格式，以確保不會不小心授予根存取權。遵循最低權限原則，容器應使用非根使用者以最低必要許可執行。這種方法可大幅減少潛在的攻擊面，並減輕潛在安全漏洞的影響。

 Note

此控制項只會在任務定義中 `operatingSystemFamily` 將設定為 `LINUX` 或未設定 `operatingSystemFamily` 時，評估任務定義中的容器定義。如果任務定義中的任何容器定義 `user` 尚未設定或 `user` 設定為預設根使用者，控制項將產生評估任務定義的 `FAILED` 調查結果。Linux 容器的預設根使用者為 `"root"` 和 `"0"`。

修補

如需有關建立新的 Amazon ECS 任務定義修訂和更新容器定義中 `user` 參數的資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的[更新 Amazon ECS 任務定義](#)。

【ECS.21】 ECS 任務定義應在 Windows 容器定義中設定非管理員使用者

類別：保護 > 安全存取管理 > 根使用者存取限制

嚴重性：中

資源類型：AWS::ECS::TaskDefinition

AWS Config 規則：[ecs-task-definition-windows-user-non-admin](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon ECS 任務定義的最新作用中修訂是否將 Windows 容器設定為以非預設管理員的使用者身分執行。如果任何容器的預設管理員設定為使用者或使用者組態不存在，則控制項會失敗。

當 Windows 容器以管理員權限執行時，會帶來數個重大的安全風險。管理員在容器內具有不受限制的存取。這種更高的存取會增加容器逸出攻擊的風險，攻擊者可能會中斷容器隔離並存取基礎主機系統。

Note

此控制項只會在任務定義中 `operatingSystemFamily` 將設定為 `WINDOWS_SERVER` 或未 `operatingSystemFamily` 設定為時，評估任務定義中的容器定義。如果任務定義中的任何容器定義 `user` 尚未設定或 `user` 設定為 `WINDOWS_SERVER` 容器的預設管理員，則控制項將產生已評估任務定義的 FAILED 調查結果 "containeradministrator"。

修補

如需有關建立新的 Amazon ECS 任務定義修訂和更新容器定義中 `user` 參數的資訊，請參閱 [《Amazon Elastic Container Service 開發人員指南》](#) 中的 [更新 Amazon ECS 任務定義](#)。

Amazon EFS 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 Amazon Elastic File System (Amazon EFS) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【EFS.1】彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS

相關要求：CIS AWS Foundations Benchmark v5.0.0/2.3.1、CIS AWS Foundations Benchmark v3.0.0/2.4.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest 加密

嚴重性：中

資源類型：AWS::EFS::FileSystem

AWS Config 規則：[efs-encrypted-check](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon Elastic File System 是否設定為使用 加密檔案資料 AWS KMS。檢查會在下列情況下失敗。

- Encrypted 在[DescribeFileSystems](#)回應false中設定為。
- [DescribeFileSystems](#) 回應中的KmsKeyId金鑰與 的 KmsKeyId 參數不相符[efs-encrypted-check](#)。

請注意，此控制項不會針對 使用 KmsKeyId 參數[efs-encrypted-check](#)。其只會檢查 Encrypted 的值。

若要為 Amazon EFS 中的敏感資料增加一層安全性，您應該建立加密的檔案系統。Amazon EFS 支援靜態檔案系統的加密。您可以在建立 Amazon EFS 檔案系統時啟用靜態資料的加密。若要進一步了解 Amazon EFS 加密，請參閱《Amazon Amazon Elastic File System 使用者指南》中的 Amazon [EFS 中的資料加密](#)。

修補

如需如何加密新 Amazon EFS 檔案系統的詳細資訊，請參閱《Amazon Elastic File System 使用者指南》中的[加密靜態資料](#)。

【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 備份

嚴重性：中

資源類型：AWS::EFS::FileSystem

AWS Config 規則：[efs-in-backup-plan](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon Elastic File System (Amazon EFS) 檔案系統是否新增至 中的備份計劃 AWS Backup。如果備份計畫中未包含 Amazon EFS 檔案系統，則控制項會失敗。

在備份計畫中包含 EFS 檔案系統可協助您保護資料免於刪除和資料遺失。

修補

若要啟用現有 Amazon EFS 檔案系統的自動備份，請參閱《AWS Backup 開發人員指南》中的[入門 4：建立 Amazon EFS 自動備份](#)。

【EFS.3】 EFS 存取點應強制執行根目錄

相關需求：NIST.800-53.r5 AC-6(10)

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::EFS::AccessPoint

AWS Config 規則：[efs-access-point-enforce-root-directory](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EFS 存取點是否已設定為強制執行根目錄。如果 的 Path 值設為 / (檔案系統的預設根目錄)，則控制項會失敗。

強制執行根目錄時，使用存取點的 NFS 用戶端會使用存取點上設定的根目錄，而不是檔案系統的根目錄。強制執行存取點的根目錄有助於透過確保存取點的使用者只能存取指定子目錄的檔案來限制資料存取。

修補

如需如何強制執行 Amazon EFS 存取點根目錄的說明，請參閱《Amazon Elastic File System 使用者指南》中的[使用存取點強制執行根目錄](#)。

【EFS.4】 EFS 存取點應強制執行使用者身分

相關要求：NIST.800-53.r5 AC-6(2)、PCI DSS v4.0.1/7.3.1

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::EFS::AccessPoint

AWS Config 規則：[efs-access-point-enforce-user-identity](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EFS 存取點是否設定為強制執行使用者身分。如果在建立 EFS 存取點時未定義 POSIX 使用者身分，則此控制項會失敗。

Amazon EFS 存取點是應用程式特定的 EFS 檔案系統進入點，此進入點可讓您更輕鬆地管理共用資料集的應用程式存取。存取點可以針對透過存取點發出的所有檔案系統請求，強制執行使用者身分 (包括使用者的 POSIX 群組)。存取點也可以針對檔案系統強制執行不同的根目錄，讓用戶端只能存取指定目錄或其子目錄中的資料。

修補

若要強制執行 Amazon EFS 存取點的使用者身分，請參閱《Amazon Elastic File System 使用者指南》中的[使用存取點強制執行使用者身分](#)。

【EFS.5】 EFS 存取點應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EFS::AccessPoint

AWS Config rule：tagged-efs-accesspoint (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EFS 存取點是否具有具有參數 中定義之特定金鑰的標籤 `requiredTagKeys`。如果存取點沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果存取點未標記任何索引鍵，則 控制會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EFS 存取點，請參閱 [《Amazon Elastic File System 使用者指南》中的標記 Amazon EFS 資源](#)。Amazon Elastic File System

【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯

類別：保護 > 網路安全 > 資源不可公開存取

嚴重性：中

資源類型：AWS::EFS::FileSystem

AWS Config 規則：[efs-mount-target-public-accessible](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon EFS 掛載目標是否與在啟動時指派公有 IP 地址的子網路相關聯。如果掛載目標與在啟動時指派公有 IP 地址的子網路相關聯，則控制項會失敗。

子網路具有屬性，可判斷網路介面是否自動接收公有 IPv4 和 IPv6 地址。對於 IPv4，對於 TRUE 預設子網路和非預設子網路 FALSE，此屬性設定為（透過 EC2 啟動執行個體精靈建立的非預設子網路除外，其設定為 TRUE）。對於 IPv6，此屬性預設為所有子網路 FALSE 的。啟用這些屬性時，在子網路中啟動的執行個體會自動在其主要網路界面上接收對應的 IP 地址 (IPv4 或 IPv6)。在已啟用此屬性的子網路中啟動的 Amazon EFS 掛載目標，具有指派給其主要網路介面的公有 IP 地址。

修補

若要將現有的掛載目標與不同的子網路建立關聯，您必須在子網路中建立新的掛載目標，該子網路不會在啟動時指派公有 IP 地址，然後移除舊的掛載目標。如需有關管理掛載目標的資訊，請參閱《Amazon Elastic File System 使用者指南》中的[建立和管理掛載目標和安全群組](#)。

【EFS.7】 EFS 檔案系統應該啟用自動備份

類別：復原 > 恢復 > 備份已啟用

嚴重性：中

資源類型：AWS::EFS::FileSystem

AWS Config 規則：[efs-automatic-backups-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EFS 檔案系統是否已啟用自動備份。如果 EFS 檔案系統未啟用自動備份，則此控制會失敗。

資料備份是系統、組態或應用程式資料的複本，與原始資料分開存放。啟用定期備份可協助您保護寶貴的資料，避免發生意外事件，例如系統故障、網路攻擊或意外刪除。擁有強大的備份策略也有助於更快速的復原、業務連續性和在面臨潛在的資料遺失時安心。

修補

如需有關使用 AWS Backup for EFS 檔案系統的資訊，請參閱《Amazon Elastic [File System 使用者指南](#)》中的[備份 EFS](#) 檔案系統。Amazon Elastic File System

【EFS.8】 EFS 檔案系統應靜態加密

相關要求：CIS AWS Foundations Benchmark v5.0.0/2.3.1

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::EFS::FileSystem

AWS Config 規則：[efs-file-system-ct-encrypted](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EFS 檔案系統是否使用 AWS Key Management Service () 加密資料AWS KMS。如果未加密檔案系統，則控制項會失敗。

靜態資料是指存放在持久性、非揮發性儲存體中任何持續時間的資料。加密靜態資料可協助您保護其機密性，進而降低未經授權的使用者可存取資料的風險。

修補

若要為新的 EFS 檔案系統啟用靜態加密，請參閱《Amazon Elastic File System 使用者指南》中的[加密靜態資料](#)。

Amazon EKS 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 Amazon Elastic Kubernetes Service (Amazon EKS) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【EKS.1】不應公開存取 EKS 叢集端點

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7 、

類別：保護 > 安全網路組態 > 資源不可公開存取

嚴重性：高

資源類型：AWS::EKS::Cluster

AWS Config 規則：[eks-endpoint-no-public-access](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon EKS 叢集端點是否可公開存取。如果 EKS 叢集具有可公開存取的端點，則控制項會失敗。

當您建立新的叢集時，Amazon EKS 會為您用來與叢集通訊的受管 Kubernetes API 伺服器建立端點。根據預設，此 API 伺服器端點可公開供網際網路使用。使用 AWS Identity and Access Management (IAM) 和原生 Kubernetes 角色型存取控制 (RBAC) 的組合來保護 API 伺服器的存取。透過移除對端點的公開存取，您可以避免意外暴露和存取叢集。

修補

若要修改現有 EKS 叢集的端點存取，請參閱《Amazon EKS 使用者指南》中的[修改叢集端點存取](#)。您可以在建立新 EKS 叢集時設定端點存取。如需建立新的 Amazon EKS 叢集的說明，請參閱《[Amazon EKS 使用者指南](#)》中的[建立 Amazon EKS 叢集](#)。

【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/12.3.4

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：高

資源類型：AWS::EKS::Cluster

AWS Config 規則：[eks-cluster-supported-version](#)

排程類型：變更已觸發

參數：

- `oldestVersionSupported`：1.33 (不可自訂)

此控制項會檢查 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集是否在標準支援 Kubernetes 版本上執行。如果 Amazon EKS 叢集在不支援或延伸支援版本上執行，則控制項會失敗。

如果您的應用程式不需要特定版本的 Kubernetes，建議您為叢集使用 EKS 支援的最新可用 Kubernetes 版本。如需詳細資訊，請參閱《[Amazon EKS 使用者指南](#)》中的[Amazon EKS Kubernetes 版本行事曆](#)和[了解 Amazon EKS 上的 Kubernetes 版本生命週期](#)。

修補

若要更新 EKS 叢集，請參閱《Amazon EKS 使用者指南》中的[將現有叢集更新為新的 Kubernetes 版本](#)。

【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密

相關要求：NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、PCI DSS v4.0.1/8.3.2

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::EKS::Cluster

AWS Config 規則：[eks-cluster-secrets-encrypted](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon EKS 叢集是否使用加密的 Kubernetes 秘密。如果叢集的 Kubernetes 秘密未加密，則控制項會失敗。

當您加密秘密時，您可以使用 AWS Key Management Service (AWS KMS) 金鑰，為您的叢集提供存放在等中的 Kubernetes 秘密的信封加密。此加密是 EBS 磁碟區加密的補充，該加密預設為針對存放在中作為 EKS 叢集一部分的 etcd 中的所有資料（包括秘密）啟用。對 EKS 叢集使用秘密加密可讓您使用您定義和管理的 KMS 金鑰加密 Kubernetes 秘密，為 Kubernetes 應用程式部署深度防禦策略。

修補

若要在 EKS 叢集上啟用秘密加密，請參閱《Amazon EKS 使用者指南》中的在[現有叢集上啟用秘密加密](#)。

【EKS.6】 EKS 叢集應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EKS::Cluster

AWS Config rule：tagged-eks-cluster（自訂 Security Hub CSPM 規則）

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1-6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EKS 叢集是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果叢集沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果叢集未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EKS 叢集，請參閱 [《Amazon EKS 使用者指南》中的標記 Amazon EKS 資源](#)。

【EKS.7】EKS 身分提供者組態應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::EKS::IdentityProviderConfig

AWS Config rule：tagged-eks-identityproviderconfig (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EKS 身分提供者組態是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果組態沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果組態未標記任何索引鍵，則 會失敗。系統會忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EKS 身分提供者組態，請參閱 [《Amazon EKS 使用者指南》](#) 中的標記 [Amazon EKS 資源](#)。

【EKS.8】 EKS 叢集應該啟用稽核記錄

相關要求：NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6NIST.5 AU-9 CA-7 NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.2.1

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::EKS::Cluster

AWS Config 規則：[eks-cluster-log-enabled](#)

排程類型：變更已觸發

參數：

- logTypes: audit (不可自訂)

此控制項會檢查 Amazon EKS 叢集是否已啟用稽核記錄。如果未為叢集啟用稽核記錄，則控制項會失敗。

Note

此控制項不會檢查是否已透過的 Amazon Security Lake 啟用 Amazon EKS 稽核記錄 AWS 帳戶。

EKS 控制平面記錄會將稽核和診斷日誌直接從 EKS 控制平面提供給帳戶中的 Amazon CloudWatch Logs。您可以選取所需的日誌類型，並將日誌做為日誌串流傳送至 CloudWatch 中每個 EKS 叢集的群組。記錄可提供 EKS 叢集存取和效能的可見性。透過將 EKS 叢集的 EKS 控制平面日誌傳送至 CloudWatch Logs，您可以在中央位置記錄操作以進行稽核和診斷。

修補

若要啟用 EKS 叢集的稽核日誌，請參閱《Amazon EKS 使用者指南》中的[啟用和停用控制平面日誌](#)。

【EKS.9】 EKS 節點群組應在支援的 Kubernetes 版本上執行

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：高

資源類型：AWS::EKS::Nodegroup

AWS Config 規則：[eks-nodegroup-supported-version-check](#)

排程類型：變更已觸發

參數：

- oldestVersionSupported : 1.33 (不可自訂)

此控制項會檢查 Amazon EKS 節點群組是否在標準支援 Kubernetes 版本上執行。如果 Amazon EKS 節點群組在不支援或延伸支援版本上執行，則控制項會失敗。

在不支援的 Kubernetes 版本上執行 EKS 節點群組，表示這些節點不會再收到來自的安全修補程式、錯誤修正或相容性更新 AWS。不支援的版本可能包含在較新版本中解決的已知漏洞，並且可能會在 Kubernetes 生態系統中遇到更新 AWS 服務、容器映像和第三方工具的相容性問題。如果您的應用程式不需要特定版本的 Kubernetes，建議您為節點群組使用 Amazon EKS 支援的最新可用 Kubernetes 版本。如需詳細資訊，請參閱《[Amazon EKS 使用者指南](#)》中的 [Amazon EKS Kubernetes 版本行事曆](#)和[了解節點更新的每個階段](#)。

修補

若要更新 EKS 節點群組，請參閱《Amazon EKS 使用者指南》中的[更新叢集的受管節點群組](#)。

ElastiCache 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon ElastiCache 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【ElastiCache.1】ElastiCache (Redis OSS) 叢集應該啟用自動備份

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

類別：Recover > Resilience > Backups enabled

嚴重性：高

資源類型：AWS::ElastiCache::CacheCluster、AWS:ElastiCache:ReplicationGroup

AWS Config 規則：[elasticache-redis-cluster-automatic-backup-check](#)

排程類型：定期

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
snapshotRetentionPeriod	最短快照保留期間，以天為單位	Integer	1 至 35	1

此控制項會評估 Amazon ElastiCache (Redis OSS) 叢集是否已啟用自動備份。如果 Redis OSS 叢集 SnapshotRetentionLimit 的小於指定的時段，則控制項會失敗。除非您提供快照保留期間的自訂參數值，否則 Security Hub CSPM 會使用預設值 1 天。

ElastiCache (Redis OSS) 叢集可以備份其資料。您可以使用備份來還原叢集或植入新的叢集。備份包含叢集的中繼資料，以及叢集中的所有資料。所有備份都會寫入 Amazon S3，以提供耐用的儲存體。您可以透過建立新的 ElastiCache 叢集並填入備份中的資料來還原資料。您可以使用 AWS 管理主控台、AWS CLI 和 ElastiCache API 來管理備份。

Note

此控制項也會評估 ElastiCache (Redis OSS 和 Valkey) 複寫群組。

修補

如需有關排程 ElastiCache 叢集自動備份的資訊，請參閱《Amazon ElastiCache 使用者指南》中的[排程自動備份](#)。

【ElastiCache.2】ElastiCache 叢集應該啟用自動次要版本升級

相關要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5) PCI DSS v4.0.1/6.3.3

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：高

資源類型：AWS::ElastiCache::CacheCluster

AWS Config 規則：[elasticache-auto-minor-version-upgrade-check](#)

排程類型：定期

參數：無

此控制項會評估 Amazon ElastiCache 是否自動將次要版本升級套用至快取叢集。如果快取叢集未自動套用次要版本升級，則控制項會失敗。

 Note

此控制項不適用於 ElastiCache Memcached 叢集。

自動次要版本升級是一項功能，您可以在 Amazon ElastiCache 中啟用此功能，以便在新的次要快取引擎版本可用時自動升級快取叢集。這些升級可能包括安全性修補程式和錯誤修正。隨時掌握修補程式安裝 up-to-date，是保護系統安全的重要步驟。

修補

若要自動將次要版本升級套用至現有的 ElastiCache 快取叢集，請參閱《Amazon [ElastiCache 使用者指南](#)》中的 [ElastiCache 版本管理](#)。Amazon ElastiCache

【ElastiCache.3】ElastiCache 複寫群組應該啟用自動容錯移轉

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::ElastiCache::ReplicationGroup

AWS Config 規則：[elasticache-repl-grp-auto-failover-enabled](#)

排程類型：定期

參數：無

此控制項會檢查 ElastiCache 複寫群組是否已啟用自動容錯移轉。如果複寫群組未啟用自動容錯移轉，則控制項會失敗。

為複寫群組啟用自動容錯移轉時，主節點的角色會自動容錯移轉至其中一個僅供讀取複本。此容錯移轉和複本提升可確保您可以在提升完成後繼續寫入新的主要節點，以減少發生故障時的整體停機時間。

修補

若要啟用現有 ElastiCache 複寫群組的自動容錯移轉，請參閱《Amazon [ElastiCache 使用者指南](#)》中的[修改 ElastiCache 叢集](#)。Amazon ElastiCache 如果您使用 ElastiCache 主控台，請將自動容錯移轉設定為已啟用。

【ElastiCache.4】ElastiCache 複寫群組應靜態加密

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::ElastiCache::ReplicationGroup

AWS Config 規則：[elasticache-repl-grp-encrypted-at-rest](#)

排程類型：定期

參數：無

此控制項會檢查 ElastiCache 複寫群組是否靜態加密。如果複寫群組未靜態加密，則控制項會失敗。

加密靜態資料可降低未經驗證的使用者存取儲存在磁碟上的資料的風險。ElastiCache (Redis OSS) 複寫群組應靜態加密，以增加一層安全性。

修補

若要在 ElastiCache 複寫群組上設定靜態加密，請參閱《Amazon ElastiCache 使用者指南》中的[啟用靜態加密](#)。

【ElastiCache.5】ElastiCache 複寫群組應在傳輸中加密

相關需求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5

SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-85.r5
NIST.800-53.r5 SC-8 SI-7

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::ElastiCache::ReplicationGroup

AWS Config 規則：[elasticache-repl-grp-encrypted-in-transit](#)

排程類型：定期

參數：無

此控制項會檢查 ElastiCache 複寫群組是否在傳輸中加密。如果複寫群組未在傳輸中加密，則控制項會失敗。

加密傳輸中的資料可降低未經授權的使用者可以竊聽網路流量的風險。在 ElastiCache 複寫群組上啟用傳輸中加密會在資料從一個位置移至另一個位置時加密資料，例如叢集中的節點之間，或叢集與您的應用程式之間。

修補

若要在 ElastiCache 複寫群組上設定傳輸中加密，請參閱《Amazon ElastiCache 使用者指南》中的[啟用傳輸中加密](#)。

【ElastiCache.6] 舊版的 ElastiCache (Redis OSS) 複寫群組應該已啟用 Redis OSS AUTH

相關要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5
AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、PCI DSS v4.0.1/8.3.1

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::ElastiCache::ReplicationGroup

AWS Config 規則：[elasticache-repl-grp-redis-auth-enabled](#)

排程類型：定期

參數：無

此控制項會檢查 ElastiCache (Redis OSS) 複寫群組是否已啟用 Redis OSS AUTH。如果複寫群組節點的 Redis OSS 版本低於 6.0 且未使用，則控制項 AuthToken 會失敗。

當您使用 Redis 身分驗證字符或密碼時，Redis 需要密碼，才能允許用戶端執行命令，以改善資料安全性。對於 Redis 6.0 和更新版本，建議使用角色型存取控制 (RBAC)。由於 Redis 6.0 之前的版本不支援 RBAC，因此此控制項只會評估無法使用 RBAC 功能的版本。

修補

若要在 ElastiCache (Redis OSS) 複寫群組上使用 Redis AUTH，請參閱《Amazon ElastiCache [使用者指南](#)》中的在現有 ElastiCache (Redis OSS) 叢集上修改 AUTH 字符。

【ElastiCache.7】ElastiCache 叢集不應使用預設子網路群組

相關需求：NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)

類別：保護 > 安全網路組態

嚴重性：高

資源類型：AWS::ElastiCache::CacheCluster

AWS Config 規則：[elasticache-subnet-group-check](#)

排程類型：定期

參數：無

此控制項會檢查 ElastiCache 叢集是否已設定自訂子網路群組。如果 ElastiCache 叢集 CacheSubnetGroupName 的值為 `default`，則控制項會失敗。

啟動 ElastiCache 叢集時，如果尚未存在子網路群組，則會建立預設子網路群組。預設群組使用來自預設虛擬私有雲端 (VPC) 的子網路。建議使用自訂子網路群組，這些群組會更嚴格限制叢集所在的子網路，以及叢集從子網路繼承的聯網。

修補

若要為 ElastiCache 叢集建立新的子網路群組，請參閱《Amazon ElastiCache 使用者指南》中的[建立子網路群組](#)。

Elastic Beanstalk 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 AWS Elastic Beanstalk 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【ElasticBeanstalk.1】Elastic Beanstalk 環境應啟用增強型運作狀態報告

相關要求：NIST.800-53.r5 CA-7，NIST.800-53.r5 SI-2

類別：偵測 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：AWS::ElasticBeanstalk::Environment

AWS Config 規則：[beanstalk-enhanced-health-reporting-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查您的環境是否啟用 AWS Elastic Beanstalk 增強型運作狀態報告。

Elastic Beanstalk 增強型運作狀態報告可更快速回應基礎基礎設施運作狀態的變化。這些變更可能會導致應用程式缺乏可用性。

Elastic Beanstalk 增強型運作狀態報告會提供狀態描述項，評估已識別問題的嚴重性，並找出可能的調查原因。Elastic Beanstalk 運作狀態代理程式包含在支援的 Amazon Machine Image (AMIs) 中，可評估環境 EC2 執行個體的日誌和指標。

如需詳細資訊，請參閱《AWS Elastic Beanstalk 開發人員指南》中的[增強型運作狀態報告和監控](#)。

修補

如需如何啟用增強型運作狀態報告的指示，請參閱《AWS Elastic Beanstalk 開發人員指南》中的[使用 Elastic Beanstalk 主控台啟用增強型運作狀態報告](#)。

【ElasticBeanstalk.2】應啟用 Elastic Beanstalk 受管平台更新

相關要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：高

資源類型：AWS::ElasticBeanstalk::Environment

AWS Config 規則：[elastic-beanstalk-managed-updates-enabled](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
UpdateLevel	版本更新層級	列舉	minor, patch	無預設值

此控制項會檢查是否針對 Elastic Beanstalk 環境啟用受管平台更新。如果未啟用受管平台更新，則控制項會失敗。根據預設，如果啟用任何類型的平台更新，控制項會通過。或者，您可以提供自訂參數值，以要求特定的更新層級。

啟用受管平台更新可確保已安裝環境的最新可用平台修正、更新和功能。隨時掌握修補程式安裝的最新資訊，是保護系統安全的重要步驟。

修補

若要啟用受管平台更新，請參閱《AWS Elastic Beanstalk 開發人員指南》中的[在受管平台更新下設定受管平台更新](#)。

【ElasticBeanstalk.3】Elastic Beanstalk 應將日誌串流至 CloudWatch

相關要求：PCI DSS v4.0.1/10.4.2

類別：識別 > 記錄日誌

嚴重性：高

資源類型：AWS::ElasticBeanstalk::Environment

AWS Config 規則：[elastic-beanstalk-logs-to-cloudwatch](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
Retention InDays	在過期前保留日誌事件的天數	列舉	1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365 , 400, 545, 731, 1827, 3653	無預設值

此控制項會檢查 Elastic Beanstalk 環境是否設定為將日誌傳送至 CloudWatch Logs。如果 Elastic Beanstalk 環境未設定為將日誌傳送至 CloudWatch Logs，則控制項會失敗。或者，如果您希望控制項僅在過期前保留指定天數的日誌時傳遞，您可以為 RetentionInDays 參數提供自訂值。

CloudWatch 可協助您收集和監控應用程式和基礎設施資源的各種指標。您也可以使用 CloudWatch 根據特定指標設定警示動作。我們建議您將 Elastic Beanstalk 與 CloudWatch 整合，以提高對 Elastic Beanstalk 環境的可見性。Elastic Beanstalk 日誌包括 eb-activity.log、從環境 nginx 或 Apache 代理伺服器存取日誌，以及特定於環境的日誌。

修補

若要將 Elastic Beanstalk 與 CloudWatch Logs 整合，請參閱《AWS Elastic Beanstalk 開發人員指南》中的[將執行個體日誌串流至 CloudWatch Logs](#)。

Elastic Load Balancing 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Elastic Load Balancing 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【ELB.1】 Application Load Balancer 應設定為將所有 HTTP 請求重新導向至 HTTPS

相關要求：PCI DSS v3.2.1/2.3、PCI DSS v3.2.1/4.1、NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-80.5
NIST.800-53.r5 SC-8 SI-7

類別：偵測 > 偵測服務

嚴重性：中

資源類型：AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config 規則：[alb-http-to-https-redirection-check](#)

排程類型：定期

參數：無

此控制項會檢查 Application Load Balancer 的所有 HTTP 接聽程式是否設定 HTTP 至 HTTPS 重新導向。如果 Application Load Balancer 的任何 HTTP 接聽程式未設定 HTTP 到 HTTPS 重新導向，則控制項會失敗。

開始使用 Application Load Balancer 之前，您必須新增一或多個接聽程式。接聽程式是使用已設定通訊協定和連接埠檢查連線請求的一種程序。接聽程式同時支援 HTTP 和 HTTPS 通訊協定。您可以使用 HTTPS 接聽程式，將加密和解密的工作卸載至負載平衡器。若要強制執行傳輸中加密，您應該搭配 Application Load Balancer 使用重新導向動作，將用戶端 HTTP 請求重新導向至連接埠 443 上的 HTTPS 請求。

若要進一步了解，請參閱《[Application Load Balancer 使用者指南](#)》中的 [Application Load Balancer 的接聽程式](#)。

修補

若要將 HTTP 請求重新導向至 HTTPS，您必須新增 Application Load Balancer 接聽程式規則或編輯現有規則。

如需新增規則的說明，請參閱《Application Load Balancer 使用者指南》中的[新增規則](#)。針對通訊協定：連接埠，選擇 HTTP，然後輸入 **80**。對於新增動作，重新導向至，選擇 HTTPS，然後輸入 **443**。

如需編輯現有規則的說明，請參閱《Application Load Balancer 使用者指南》中的[編輯規則](#)。針對通訊協定：連接埠，選擇 HTTP，然後輸入 **80**。對於新增動作，重新導向至，選擇 HTTPS，然後輸入 **443**。

【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用提供的憑證 AWS Certificate Manager

相關需求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5

SC-23(5)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(1)、NIST.8000NIST.800-53.r5 SC-85.55
NIST.800-53.r5 SC-8 SI-7

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::ElasticLoadBalancing::LoadBalancer

AWS Config 規則：[elb-acm-certificate-required](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Classic Load Balancer 是否使用 AWS Certificate Manager (ACM) 提供的 HTTPS/SSL 憑證。如果使用 HTTPS/SSL 接聽程式設定的 Classic Load Balancer 不使用 ACM 提供的憑證，則控制項會失敗。

若要建立憑證，您可以使用 ACM 或支援 SSL 和 TLS 通訊協定的工具，例如 OpenSSL。Security Hub CSPM 建議您使用 ACM 來建立或匯入負載平衡器的憑證。

ACM 與 Classic Load Balancer 整合，因此您可以在負載平衡器上部署憑證。您也應該自動續約這些憑證。

修補

如需有關如何將 ACM SSL/TLS 憑證與 Classic Load Balancer 建立關聯的資訊，請參閱 AWS 知識中心文章[如何將 ACM SSL/TLS 憑證與 Classic、Application 或 Network Load Balancer 建立關聯？](#)

【ELB.3】 Classic Load Balancer 接聽程式應使用 HTTPS 或 TLS 終止設定

相關要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5
IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5
SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(1)、NIST.8000NIST.800-53.r5 SC-85.r5
SC-850.5 NIST.800-53.r5 SC-8 SI-7 3.13.15

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::ElasticLoadBalancing::LoadBalancer

AWS Config 規則：[elb-tls-https-listeners-only](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Classic Load Balancer 接聽程式是否設定為使用 HTTPS 或 TLS 通訊協定進行前端（用戶端至負載平衡器）連線。如果 Classic Load Balancer 有接聽程式，則控制項適用。如果您的 Classic Load Balancer 未設定接聽程式，則控制項不會報告任何問題清單。

如果 Classic Load Balancer 接聽程式是針對前端連線使用 TLS 或 HTTPS 設定，則控制項會通過。

如果未使用 TLS 或 HTTPS 為前端連線設定接聽程式，則控制項會失敗。

開始使用負載平衡器之前，您必須新增一或多個接聽程式。接聽程式是使用已設定通訊協定和連接埠檢查連線請求的一種程序。接聽程式可以同時支援 HTTP 和 HTTPS/TLS 通訊協定。您應該一律使用 HTTPS 或 TLS 接聽程式，以便負載平衡器在傳輸中執行加密和解密工作。

修補

若要修復此問題，請更新您的接聽程式以使用 TLS 或 HTTPS 通訊協定。

將所有不合規接聽程式變更為 TLS/HTTPS 接聽程式

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格的 Load Balancing (負載平衡) 下方，選擇 Load Balancers (負載平衡器)。
3. 選取您的 Classic Load Balancer。
4. 在 Listeners (接聽程式) 標籤上，選擇 Edit (編輯)。
5. 對於未將 Load Balancer 通訊協定設定為 HTTPS 或 SSL 的所有接聽程式，請將設定變更為 HTTPS 或 SSL。
6. 對於所有修改過的接聽程式，在憑證索引標籤上，選擇變更預設值。
7. 對於 ACM 和 IAM 憑證，請選取憑證。
8. 選擇儲存為預設。
9. 更新所有接聽程式之後，請選擇儲存。

【ELB.4】 Application Load Balancer 應設定為捨棄無效的 http 標頭

相關要求：NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(2)、PCI DSS v4.0.1/6.2.4

類別：保護 > 網路安全

嚴重性：中

資源類型：AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config 規則：[alb-http-drop-invalid-header-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會評估 Application Load Balancer 是否設定為捨棄無效的 HTTP 標頭。如果 的 `routing.http.drop_invalid_header_fields.enabled` 設為 `false`，則控制項會失敗。

根據預設，Application Load Balancer 不會設定為捨棄無效的 HTTP 標頭值。移除這些標頭值可防止 HTTP 非同步攻擊。

 Note

如果您的帳戶中已啟用 ELB.12，我們建議您停用此控制項。如需詳細資訊，請參閱 [【ELB.12】Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)。

修補

若要修復此問題，請將負載平衡器設定為捨棄無效的標頭欄位。

若要設定負載平衡器以捨棄無效的標頭欄位

1. 前往 <https://console.aws.amazon.com/ec2/> 開啟 Amazon EC2 主控台。
2. 在導覽窗格上，選擇 Load balancers (負載平衡器)。
3. 選擇 Application Load Balancer。
4. 在動作中，選擇編輯屬性。
5. 在捨棄無效標頭欄位下，選擇啟用。
6. 選擇儲存。

【ELB.5】應啟用應用程式和 Classic Load Balancer 記錄

相關要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::ElasticLoadBalancing::LoadBalancer、
AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config 規則：[elb-logging-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Application Load Balancer 和 Classic Load Balancer 的記錄是否已啟用。如果 `access_logs.s3.enabled` 為 `false`，則控制項會失敗。

Elastic Load Balancing 提供存取日誌，可針對傳送到負載平衡器的請求，擷取其詳細資訊。每個日誌包含收到請求的時間、用戶端的 IP 地址、延遲、請求路徑和伺服器回應等資訊。您可以使用這些存取日誌來分析流量模式和排除問題。

若要進一步了解，請參閱 [Classic Load Balancer 使用者指南](#) 中的存取 Classic Load Balancer 的日誌。

修補

若要啟用存取日誌，請參閱 Application Load Balancer 使用者指南中的 [步驟 3：設定存取日誌](#)。

【ELB.6】應用程式、閘道和 Network Load Balancer 應啟用刪除保護

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5
CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config 規則：[elb-deletion-protection-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Application、Gateway 或 Network Load Balancer 是否已啟用刪除保護。如果停用刪除保護，則控制項會失敗。

啟用刪除保護，以保護 Application、Gateway 或 Network Load Balancer 免於刪除。

修補

為避免您的負載平衡器上遭意外刪除，您可以啟用刪除保護。您的負載平衡器的刪除保護預設為停用。

如果您為負載平衡器啟用刪除保護，您必須先停用刪除保護，才能刪除負載平衡器。

若要啟用 Application Load Balancer 的刪除保護，請參閱《Application Load Balancer 使用者指南》中的[刪除保護](#)。若要啟用 Gateway Load Balancer 的刪除保護，請參閱《Gateway Load Balancer 使用者指南》中的[刪除保護](#)。若要啟用 Network Load Balancer 的刪除保護，請參閱 Network Load Balancer 使用者指南中的[刪除保護](#)。

【ELB.7】 Classic Load Balancer 應啟用連線耗盡

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

類別：復原 > 恢復能力

嚴重性：低

資源類型：AWS::ElasticLoadBalancing::LoadBalancer

AWS Config rule：elb-connection-draining-enabled (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Classic Load Balancer 是否已啟用連線耗盡。

在 Classic Load Balancer 上啟用連線耗盡可確保負載平衡器停止將請求傳送至取消註冊或運作狀態不佳的執行個體。它會保持現有連線開啟。這對於 Auto Scaling 群組中的執行個體特別有用，以確保連線不會突然中斷。

修補

若要在 Classic Load Balancer 上啟用連線耗盡，請參閱 [Classic Load Balancer 使用者指南中的設定 Classic Load Balancer 的連線耗盡](#)。

【ELB.8】 具有 SSL AWS Config 接聽程式的 Classic Load Balancer 應使用預先定義的安全政策，該政策具有強烈驅動

相關要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-85.r5 SI-7 3.13.15

類別：保護 > 資料保護 > data-in-transit 加密

嚴重性：中

資源類型：AWS::ElasticLoadBalancing::LoadBalancer

AWS Config 規則：[elb-predefined-security-policy-ssl-check](#)

排程類型：已觸發變更

參數：

- predefinedPolicyName：ELBSecurityPolicy-TLS-1-2-2017-01 (不可自訂)

此控制項會檢查您的 Classic Load Balancer HTTPS/SSL 接聽程式是否使用預先定義的政策 ELBSecurityPolicy-TLS-1-2-2017-01。如果 Classic Load Balancer HTTPS/SSL 接聽程式不使用，則控制項會失敗 ELBSecurityPolicy-TLS-1-2-2017-01。

安全政策是 SSL 通訊協定、密碼和伺服器訂單偏好設定選項的組合。預先定義的政策控制在用戶端和負載平衡器之間的 SSL 交涉期間支援的加密、通訊協定和偏好設定順序。

使用 ELBSecurityPolicy-TLS-1-2-2017-01 可協助您符合需要停用特定版本 SSL 和 TLS 的合規和安全標準。如需詳細資訊，請參閱 [Classic Load Balancer 使用者指南中的 Classic Load Balancer 的預先定義 SSL 安全政策](#)。

修補

如需有關如何 ELBSecurityPolicy-TLS-1-2-2017-01 搭配 Classic Load Balancer 使用預先定義安全政策的資訊，請參閱 Classic Load Balancer 使用者指南中的 [設定安全設定](#)。

【ELB.9】 Classic Load Balancer 應啟用跨區域負載平衡

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::ElasticLoadBalancing::LoadBalancer

AWS Config 規則：[elb-cross-zone-load-balancing-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Classic Load Balancer (CLBs) 是否啟用跨區域負載平衡。如果未針對 CLB 啟用跨區域負載平衡，則控制項會失敗。

負載平衡器節點只會在其可用區域中的已註冊目標之間分配流量。停用跨區域負載平衡時，每個負載平衡器節點只會將流量分發到其可用區域內已註冊的目標。如果已註冊的目標數量在可用區域之間不同，流量將無法平均分配，且相較於另一個區域中的執行個體，一個區域中的執行個體最終可能會過度使用。啟用跨區域負載平衡後，Classic Load Balancer 的每個負載平衡器節點會將請求平均分配到所有已啟用可用區域中的已註冊執行個體。如需詳細資訊，請參閱《Elastic Load Balancing 使用者指南》中的[跨區域負載平衡](#)。

修補

若要在 Classic Load Balancer 中啟用跨區域負載平衡，請參閱 Classic Load Balancer 使用者指南中的[啟用跨區域負載平衡](#)。

【ELB.10】 Classic Load Balancer 應跨越多個可用區域

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::ElasticLoadBalancing::LoadBalancer

AWS Config 規則：[clb-multiple-az](#)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
minAvailabilityZones	可用區域數目下限	列舉	2, 3, 4, 5, 6	2

此控制項會檢查 Classic Load Balancer 是否已設定為至少跨越指定數量的可用區域 (AZs)。如果 Classic Load Balancer 未至少跨越指定數量 AZs，則控制項會失敗。除非您提供最低 AZs 數量的自訂參數值，否則 Security Hub CSPM 會使用兩個 AZs 的預設值。

Classic Load Balancer 可設定為在單一可用區域中或多個可用區域中，將傳入的請求分散至 Amazon EC2 執行個體。如果唯一設定的可用區域無法使用，則未跨越多個可用區域的 Classic Load Balancer 無法將流量重新導向至另一個可用區域中的目標。

修補

若要將可用區域新增至 Classic Load Balancer，請參閱 [Classic Load Balancer 使用者指南中的新增或移除 Classic Load Balancer 的子網路](#)。

【ELB.12】 Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式

相關要求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/6.2.4

類別：保護 > 資料保護 > 資料完整性

嚴重性：中

資源類型：AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config 規則：[alb-desync-mode-check](#)

排程類型：已觸發變更

參數：

- desyncMode : defensive, strictest (不可自訂)

此控制項會檢查 Application Load Balancer 是否設定為防禦性還是最嚴格的非同步緩解模式。如果 Application Load Balancer 未設定為防禦性或最嚴格的非同步緩解模式，則控制項會失敗。

HTTP Desync 問題可能導致請求走私，並讓應用程式容易受到請求佇列或快取中毒的影響。反之，這些漏洞可能會導致登入資料填充或執行未經授權的命令。使用防禦性或最嚴格的非同步緩解模式設定的 Application Load Balancer 可保護您的應用程式免於 HTTP Desync 可能導致安全問題。

修補

若要更新 Application Load Balancer 的取消同步緩解模式，請參閱《Application Load Balancer 使用者指南》中的[取消同步緩解模式](#)。

【ELB.13】 應用程式、網路和閘道負載平衡器應跨越多個可用區域

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config 規則：[elbv2-multiple-az](#)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
minAvailabilityZones	可用區域數目下限	列舉	2, 3, 4, 5, 6	2

此控制項會檢查 Elastic Load Balancer V2（應用程式、網路或閘道 Load Balancer）是否已從至少指定數量的可用區域 (AZs) 註冊執行個體。如果 Elastic Load Balancer V2 沒有在至少指定數量的 AZs 中註冊的執行個體，則控制項會失敗。除非您提供最低 AZs 數量的自訂參數值，否則 Security Hub CSPM 會使用兩個 AZs 的預設值。

Elastic Load Balancing 會自動將傳入流量分配到一或多個可用區域中的多個目標，例如 EC2 執行個體、容器和 IP 地址。當傳入流量隨著時間發生變化，Elastic Load Balancing 會擴展您的負載平衡器。建議至少設定兩個可用區域以確保服務的可用性，因為如果某個可用區域無法使用，Elastic Load Balancer 將能夠將流量導向另一個可用區域。設定多個可用區域有助於消除應用程式的單一故障點。

修補

若要將可用區域新增至 Application Load Balancer，請參閱《Application [Application Load Balancer](#) 中的 Application Load Balancer 的可用區域》。若要將可用區域新增至 Network Load Balancer，請參閱 [Network Load Balancer](#) 使用者指南中的 Network Load Balancer。若要將可用區域新增至閘道 Load Balancer，請參閱《[閘道 Load Balancer 使用者指南](#)》中的 [建立閘道負載平衡器](#)。

【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式

相關要求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/6.2.4

類別：保護 > 資料保護 > 資料完整性

嚴重性：中

資源類型：AWS::ElasticLoadBalancing::LoadBalancer

AWS Config 規則：[clb-desync-mode-check](#)

排程類型：已觸發變更

參數：

- desyncMode : defensive, strictest (不可自訂)

此控制項會檢查 Classic Load Balancer 是否設定為防禦性還是最嚴格的非同步緩解模式。如果 Classic Load Balancer 未設定為防禦性或最嚴格的非同步緩解模式，則控制項會失敗。

HTTP Desync 問題可能導致請求走私，並讓應用程式容易受到請求佇列或快取中毒的影響。反之，這些漏洞可能會導致登入資料遭到劫持或執行未經授權的命令。使用防禦性或最嚴格的非同步緩解模式設定的 Classic Load Balancer 可保護您的應用程式免於 HTTP Desync 可能導致安全問題。

修補

若要更新 Classic Load Balancer 上的非同步緩解模式，請參閱 Classic Load Balancer 使用者指南中的 [修改非同步緩解模式](#)。

【ELB.16】 Application Load Balancer 應與 AWS WAF Web ACL 建立關聯

相關要求：NIST.800-53.r5 AC-4(21)

類別：保護 > 保護服務

嚴重性：中

資源類型：AWS::ElasticLoadBalancingV2::LoadBalancer

AWS Config 規則：[alb-waf-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Application Load Balancer 是否與 AWS WAF Classic 或 AWS WAF Web 存取控制清單 (Web ACL) 相關聯。如果 AWS WAF 組態Enabled的欄位設定為 `false`，則控制項會失敗。

AWS WAF 是一種 Web 應用程式防火牆，可協助保護 Web 應用程式和 APIs 免受攻擊。您可以使用 AWS WAF 設定 Web ACL，這是一組規則，可根據您定義的可自訂 Web 安全規則和條件來允許、封鎖或計數 Web 請求。我們建議您將 Application Load Balancer 與 AWS WAF Web ACL 建立關聯，以協助保護它免受惡意攻擊。

修補

若要將 Application Load Balancer 與 Web ACL 建立關聯，請參閱《AWS WAF 開發人員指南》中的[將 Web ACL 與 AWS 資源建立關聯或取消關聯](#)。

【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策

相關需求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8 SI-7r

類別：保護 > 資料保護 > data-in-transit 加密

嚴重性：中

資源類型：AWS::ElasticLoadBalancingV2::Listener

AWS Config 規則：[elbv2-predefined-security-policy-ssl-check](#)

排程類型：已觸發變更

參數：sslPolicies：ELBSecurityPolicy-TLS13-1-3-2021-06, ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-2021-06, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09, ELBSecurityPolicy-TLS13-1-3-PQ-2025-09, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09, ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09 (不可自訂)

此控制項會檢查 Application Load Balancer 的 HTTPS 接聽程式或 Network Load Balancer 的 TLS 接聽程式是否設定為使用建議的安全政策來加密傳輸中的資料。如果負載平衡器的 HTTPS 或 TLS 接聽程式未設定為使用建議的安全政策，則控制項會失敗。

Elastic Load Balancing 使用稱為安全政策的 SSL 交涉組態，來交涉用戶端和負載平衡器之間的連線。安全政策會指定通訊協定和密碼的組合。通訊協定會在用戶端和伺服器之間建立安全連線。密碼是一種加密演算法，使用加密金鑰來建立編碼的訊息。在連線交涉程序期間，用戶端與負載平衡器會出示它們分別支援的加密和通訊協定的清單 (以偏好的順序)。使用建議的負載平衡器安全政策可協助您符合合規和安全標準。

修補

如需有關建議的安全性政策和如何更新接聽程式的資訊，請參閱 Elastic Load Balancing 使用者指南的下列章節：[Application Load Balancer 的安全政策](#)、[Network Load Balancer 的安全政策](#)、[更新 Application Load Balancer 的 HTTPS 接聽程式](#)，以及[更新 Network Load Balancer 的接聽程式](#)。

【ELB.18】應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::ElasticLoadBalancingV2::Listener

AWS Config 規則：[elbv2-listener-encryption-in-transit](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Application Load Balancer 或 Network Load Balancer 的接聽程式是否設定為使用安全通訊協定來加密傳輸中的資料。如果 Application Load Balancer 接聽程式未設定為使用 HTTPS 通訊協定，或 Network Load Balancer 接聽程式未設定為使用 TLS 通訊協定，則控制項會失敗。

若要加密用戶端和負載平衡器之間傳輸的資料，Elastic Load Balancer 接聽程式應設定為使用產業標準安全通訊協定：適用於 Application Load Balancer 的 HTTPS 或適用於 Network Load Balancer 的 TLS。否則，用戶端與負載平衡器之間傳輸的資料容易遭到攔截、竄改和未經授權的存取。接聽程式使用 HTTPS 或 TLS 符合安全最佳實務，有助於確保傳輸期間資料的機密性和完整性。這對處理敏感資訊的應用程式特別重要，或必須符合需要傳輸中資料加密的安全標準。

修補

如需為接聽程式設定安全通訊協定的相關資訊，請參閱 Elastic Load Balancing 使用者指南中的下列章節：[為 Application Load Balancer 建立 HTTPS 接聽程式](#)，並為 [Network Load Balancer 建立接聽程式](#)。

【ELB.21】應用程式和 Network Load Balancer 目標群組應使用加密的運作狀態檢查通訊協定

類別：保護 > 資料保護 > data-in-transit

嚴重性：中

資源類型：AWS::ElasticLoadBalancingV2::TargetGroup

AWS Config 規則：[elbv2-targetgroup-healthcheck-protocol-encrypted](#)

排程類型：已觸發變更

參數：無

此控制項會檢查應用程式和網路負載平衡器運作狀態檢查的目標群組是否使用加密的傳輸通訊協定。如果運作狀態檢查通訊協定不使用 HTTPS，則控制項會失敗。此控制項不適用於 Lambda 目標類型。

負載平衡器會將運作狀態檢查請求傳送至已註冊的目標，以判斷其狀態並相應地路由流量。目標群組態中指定的運作狀態檢查通訊協定會決定執行這些檢查的方式。當運作狀態檢查通訊協定使用 HTTP 等未加密通訊時，可以在傳輸期間攔截或操作請求和回應。這可讓攻擊者深入了解基礎設施組態、竄改運作狀態檢查結果，或進行會影響路由決策 man-in-the-middle 攻擊。使用 HTTPS 進行運作狀態檢查可在負載平衡器及其目標之間提供加密通訊，以保護運作狀態資訊的完整性和機密性。

修補

若要設定 Application Load Balancer 目標群組的加密運作狀態檢查，請參閱 Elastic Load Balancing 使用者指南中的[更新 Application Load Balancer 目標群組的運作狀態檢查設定](#)。若要設定 Network Load Balancer 目標群組的加密運作狀態檢查，請參閱《Elastic Load Balancing 使用者指南》中的[更新 Network Load Balancer 目標群組的運作狀態檢查設定](#)。

【ELB.22】 ELB 目標群組應使用加密傳輸通訊協定

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::ElasticLoadBalancingV2::TargetGroup

AWS Config 規則：[elbv2-targetgroup-protocol-encrypted](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Elastic Load Balancing 目標群組是否使用加密的傳輸通訊協定。此控制項不適用於目標類型為 Lambda 或 ALB 的目標群組，或使用 GENEVE 通訊協定的目標群組。如果目標群組不使用 HTTPS、TLS 或 QUIC 通訊協定，則控制項會失敗。

加密傳輸中的資料可保護資料不受未經授權的使用者攔截。使用未加密通訊協定 (HTTP、TCP、UDP) 的目標群組在沒有加密的情況下傳輸資料，因此容易遭到竊聽。使用加密通訊協定 (HTTPS、TLS、QUIC) 可確保負載平衡器和目標之間傳輸的資料受到保護。

修補

若要使用加密的通訊協定，您必須使用 HTTPS、TLS 或 QUIC 通訊協定建立新的目標群組。目標群組通訊協定無法在建立後修改。若要建立 Application Load Balancer 目標群組，請參閱 Elastic Load Balancing 使用者指南中的[為 Application Load Balancer 建立目標群組](#)。若要建立 Network Load Balancer 目標群組，請參閱 Elastic Load Balancing 使用者指南中的[為 Network Load Balancer 建立目標群組](#)。

適用於 Elasticsearch 的 Security Hub CSPM

這些 AWS Security Hub CSPM 控制項會評估 Elasticsearch 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【ES.1】 Elasticsearch 網域應該啟用靜態加密

相關要求：PCI DSS v3.2.1/3.4、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::Elasticsearch::Domain

AWS Config 規則：[elasticsearch-encrypted-at-rest](#)

排程類型：定期

參數：無

此控制項會檢查 Elasticsearch 網域是否已啟用靜態加密組態。如果未啟用靜態加密，則檢查會失敗。

為了為 OpenSearch 中的敏感資料增加一層安全性，您應該將 OpenSearch 設定為靜態加密。Elasticsearch 網域提供靜態資料的加密。此功能使用 AWS KMS 來存放和管理加密金鑰。為了執行加密，其會使用 256 位元金鑰的進階加密標準演算法 (AES-256)。

若要進一步了解 OpenSearch 靜態加密，請參閱《[Amazon OpenSearch Service 開發人員指南](#)》中的 [Amazon OpenSearch Service 靜態資料加密](#)。 OpenSearch

t.small 和 等特定執行個體類型 t.medium 不支援靜態資料加密。如需詳細資訊，請參閱《Amazon OpenSearch Service 開發人員指南》中的 [支援的執行個體類型](#)。

修補

若要為新的和現有的 Elasticsearch 網域啟用靜態加密，請參閱《Amazon OpenSearch Service 開發人員指南》中的 [啟用靜態資料加密](#)。

【ES.2】 不應公開存取 Elasticsearch 網域

相關要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4-4(21)、NIST.800-53.r5 AC-60 NIST.800-53.r5 SC-7

類別：保護 > 安全網路組態 > VPC 內的資源

嚴重性：嚴重

資源類型：AWS::Elasticsearch::Domain

AWS Config 規則：[elasticsearch-in-vpc-only](#)

排程類型：定期

參數：無

此控制項會檢查 Elasticsearch 網域是否位於 VPC 中。它不會評估 VPC 子網路路由組態來判斷公有存取。您應該確保 Elasticsearch 網域未連接到公有子網路。請參閱《Amazon OpenSearch Service 開發人員指南》中的[資源型政策](#)。您也應該確保您的 VPC 已根據建議的最佳實務進行設定。請參閱《Amazon [VPC 使用者指南](#)》中的[VPC 的安全最佳實務](#)。

部署在 VPC 內的 Elasticsearch 網域可以透過私有 AWS 網路與 VPC 資源通訊，而不需要周遊公有網際網路。此組態透過限制對傳輸中資料的存取來增加安全狀態。VPCs 提供多種網路控制，以安全存取 Elasticsearch 網域，包括網路 ACL 和安全群組。Security Hub CSPM 建議您將公有 Elasticsearch 網域遷移至 VPCs，以利用這些控制項。

修補

如果您建立了具備公有端點的網域，您稍後便無法將其置放於 VPC 內。反之，您必須建立新網域並遷移您的資料。反之亦然。如果您在 VPC 中建立了網域，該網域便無法擁有公有端點。您必須改為[建立另一個網域](#)或停用此控制項。

請參閱《[Amazon OpenSearch Service 開發人員指南](#)》中的在 VPC 中啟動 Amazon OpenSearch Service 網域。 OpenSearch

【ES.3】 Elasticsearch 網域應該加密節點之間傳送的資料

相關要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、PCI DSS v4.0.1/4.2.1

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::Elasticsearch::Domain

AWS Config 規則：[elasticsearch-node-to-node-encryption-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Elasticsearch 網域是否已啟用node-to-node加密。如果 Elasticsearch 網域未啟用node-to-node加密，則控制項會失敗。如果 Elasticsearch 版本不支援node-to-node加密檢查，控制項也會產生失敗的問題清單。

HTTPS (TLS) 可用來協助防止潛在攻擊者竊聽或使用 person-in-the-middle 或類似攻擊操縱網路流量。只能允許透過 HTTPS (TLS) 進行加密連線。啟用 Elasticsearch 網域的 node-to-node 加密，可確保叢集內通訊在傳輸中加密。

此組態可能會產生效能損失。在啟用此選項之前，您應該注意並測試效能權衡。

修補

如需有關在新的和現有的網域上啟用 node-to-node 加密的資訊，請參閱《Amazon OpenSearch Service 開發人員指南》中的[啟用 node-to-node 加密](#)。

【ES.4】應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-7

類別：識別 – 記錄日誌

嚴重性：中

資源類型：AWS::Elasticsearch::Domain

AWS Config 規則：[elasticsearch-logs-to-cloudwatch](#)

排程類型：已觸發變更

參數：

- logtype = 'error' (不可自訂)

此控制項會檢查 Elasticsearch 網域是否設定為將錯誤日誌傳送至 CloudWatch Logs。

您應該啟用 Elasticsearch 網域的錯誤日誌，並將這些日誌傳送至 CloudWatch Logs 以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。

修補

如需如何啟用日誌發佈的資訊，請參閱《Amazon OpenSearch Service 開發人員指南》中的[啟用日誌發佈（主控台）](#)。

【ES.5】 Elasticsearch 網域應該啟用稽核記錄

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.4.2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::Elasticsearch::Domain

AWS Config rule：elasticsearch-audit-logging-enabled (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

- cloudWatchLogsLogGroupArnList (不可自訂)。Security Hub CSPM 不會填入此參數。應為稽核日誌設定的 CloudWatch Logs 日誌群組逗號分隔清單。

NON_COMPLIANT 如果在此參數清單中未指定 Elasticsearch 網域的 CloudWatch Logs 日誌群組，則此規則為。

此控制項會檢查 Elasticsearch 網域是否已啟用稽核記錄。如果 Elasticsearch 網域未啟用稽核記錄，則此控制會失敗。

稽核日誌可高度自訂。它們可讓您追蹤 Elasticsearch 叢集上的使用者活動，包括身分驗證成功和失敗、對 OpenSearch 的請求、索引變更，以及傳入的搜尋查詢。

修補

如需啟用稽核日誌的詳細資訊，請參閱《Amazon OpenSearch Service 開發人員指南》中的[啟用稽核日誌](#)。

【ES.6】 Elasticsearch 網域應至少具有三個資料節點

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::Elasticsearch::Domain

AWS Config rule：elasticsearch-data-node-fault-tolerance (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Elasticsearch 網域是否已設定至少三個資料節點，且zoneAwarenessEnabled為true。

Elasticsearch 網域需要至少三個資料節點，以實現高可用性和容錯能力。部署具有至少三個資料節點的 Elasticsearch 網域可確保在節點失敗時執行叢集操作。

修補

修改 Elasticsearch 網域中的資料節點數量

1. 開啟位於 <https://console.aws.amazon.com/aos/> 的 Amazon OpenSearch Service 主控台。
2. 在網域下，選擇您要編輯的網域名稱。
3. 選擇 Edit domain (編輯網域)。
4. 在資料節點下，將節點數目設定為大於或等於 的數目3。

對於三個可用區域部署，將 設定為三個部署的倍數，以確保可用區域之間的分佈相等。

5. 選擇提交。

【ES.7】 Elasticsearch 網域應該至少設定三個專用主節點

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::Elasticsearch::Domain

AWS Config rule : elasticsearch-primary-node-fault-tolerance (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Elasticsearch 網域是否已設定至少三個專用主節點。如果網域不使用專用主節點，則此控制會失敗。如果 Elasticsearch 網域有五個專用主節點，則此控制項會通過。不過，使用超過三個主要節點可能不需要，以降低可用性風險，並會產生額外的成本。

Elasticsearch 網域需要至少三個專用主節點，以實現高可用性和容錯能力。專用主節點資源可能會在資料節點藍/綠部署期間受到壓力，因為還有其他節點需要管理。部署具有至少三個專用主節點的 Elasticsearch 網域，可確保在節點失敗時有足夠的主節點資源容量和叢集操作。

修補

修改 OpenSearch 網域中專用主節點的數量

1. 開啟位於 <https://console.aws.amazon.com/aos/> 的 Amazon OpenSearch Service 主控台。
2. 在網域下，選擇您要編輯的網域名稱。
3. 選擇 Edit domain (編輯網域)。
4. 在專用主節點下，將執行個體類型設定為所需的執行個體類型。
5. 將主節點數目設定為等於三個或大於三個。
6. 選擇提交。

【ES.8】 應使用最新的 TLS 安全政策加密與 Elasticsearch 網域的連線

相關要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(1)、NIST.NIST.800-53.r5 SC-855.r5 SI-7

類別：保護 > 資料保護 > data-in-transit

嚴重性：中

資源類型：AWS::Elasticsearch::Domain

AWS Config rule : elasticsearch-https-required (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Elasticsearch 網域端點是否設定為使用最新的 TLS 安全政策。如果 Elasticsearch 網域端點未設定為使用最新支援的政策，或未啟用 HTTPS 則控制項會失敗。目前支援的最新 TLS 安全政策為 Policy-Min-TLS-1-2-PFS-2023-10。

HTTPS (TLS) 可用來防止潛在攻擊者使用中間人攻擊或類似的攻擊手法來竊聽或操控網路流量。只能允許透過 HTTPS (TLS) 進行加密連線。加密傳輸中的資料可能會影響效能。您應該使用此功能測試應用程式，以了解效能描述檔和 TLS 的影響。TLS 1.2 提供相較於舊版 TLS 的數個安全性增強功能。

修補

若要啟用 TLS 加密，請使用 [UpdateDomainConfig](#) API 操作來設定 [DomainEndpointOptions](#) 物件。這會設定 TLSSecurityPolicy。

【ES.9】應標記 Elasticsearch 網域

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Elasticsearch::Domain

AWS Config rule：tagged-elasticsearch-domain (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	No default value

此控制項會檢查 Elasticsearch 網域是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果網域沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失

敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果網域未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Elasticsearch 網域，請參閱《Amazon OpenSearch Service 開發人員指南》中的 [使用標籤](#)。

Amazon EMR 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon EMR（先前稱為 Amazon Elastic MapReduce）服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址

相關要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v4.0.1/1.4.4、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4)、NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7

類別：保護 > 安全網路組態

嚴重性：高

資源類型：AWS::EMR::Cluster

AWS Config 規則：[emr-master-no-public-ip](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon EMR 叢集上的主節點是否具有公有 IP 地址。如果公有 IP 地址與任何主節點執行個體相關聯，則控制項會失敗。

公有 IP 地址是在執行個體 `NetworkInterfaces` 組態的 `PublicIp` 欄位中指定。此控制項只會檢查處於 `RUNNING` 或 `WAITING` 狀態的 Amazon EMR 叢集。

修補

在啟動期間，您可以控制預設或非預設子網路中的執行個體是否已指派公有 IPv4 地址。根據預設，預設子網路會將此屬性設定為 `true`。非預設子網路的 IPv4 公有定址屬性設定為 `false`，除非是由 Amazon EC2 啟動執行個體精靈建立。在這種情況下，屬性會設定為 `true`。

啟動後，您無法手動取消公有 IPv4 地址與執行個體的關聯。

若要修復失敗的問題清單，您必須在 VPC 中啟動新的叢集，其私有子網路的 IPv4 公有定址屬性設定為 `false`。如需指示，請參閱《Amazon EMR 管理指南》中的 [在 VPC 中啟動叢集](#)。

【EMR.2】應啟用 Amazon EMR 封鎖公開存取設定

相關要求：PCI DSS v4.0.1/1.4.4、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7

類別：保護 > 安全存取管理 > 資源不可公開存取

嚴重性：嚴重

資源類型：AWS::::Account

AWS Config 規則：[emr-block-public-access](#)

排程類型：定期

參數：無

此控制項會檢查您的帳戶是否已設定 Amazon EMR 封鎖公開存取。如果未啟用封鎖公開存取設定，或允許連接埠 22 以外的任何連接埠，則控制項會失敗。

如果叢集具有允許來自連接埠上公有 IP 地址的傳入流量的安全組態，Amazon EMR 封鎖公有存取會阻止您在公有子網路中啟動叢集。在您的 AWS 帳戶中的使用者啟動叢集時，Amazon EMR 會檢查叢集安全群組中的連接埠規則，並將其與您的傳入流量規則進行比較。如果安全群組具有開啟公有 IP 地址 IPv4 0.0.0.0/0 或 IPv6 ::/0 連接埠的傳入規則，且這些連接埠未指定為您帳戶的例外狀況，則 Amazon EMR 不會允許使用者建立叢集。

 Note

預設為啟用封鎖公開存取。為了增強帳戶保護，建議您保持啟用狀態。

修補

若要設定 Amazon EMR 的封鎖公開存取，請參閱 [《Amazon EMR 管理指南》中的使用 Amazon EMR 封鎖公開存取](#)。

【EMR.3】 Amazon EMR 安全組態應靜態加密

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CP-9(8)、NIST.800-53.r5 SI-12

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::EMR::SecurityConfiguration

AWS Config 規則：[emr-security-configuration-encryption-rest](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EMR 安全組態是否已啟用靜態加密。如果安全組態未啟用靜態加密，則控制項會失敗。

靜態資料是指存放在持久性、非揮發性儲存體中任何持續時間的資料。加密靜態資料可協助您保護其機密性，進而降低未經授權的使用者可存取資料的風險。

修補

若要在 Amazon EMR 安全組態中啟用靜態加密，請參閱 [《Amazon EMR 管理指南》中的設定資料加密](#)。

【EMR.4】 Amazon EMR 安全組態應在傳輸中加密

相關要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::EMR::SecurityConfiguration

AWS Config 規則：[emr-security-configuration-encryption-transit](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EMR 安全組態是否已啟用傳輸中加密。如果安全組態未啟用傳輸中的加密，則控制項會失敗。

傳輸中的資料是指從一個位置移動到另一個位置的資料，例如叢集中的節點之間，或叢集與您的應用程式之間。資料可能會跨網際網路或在私有網路中移動。加密傳輸中的資料可降低未經授權的使用者可以竊聽網路流量的風險。

修補

若要在 Amazon EMR 安全組態中啟用傳輸中加密，請參閱《Amazon EMR 管理指南》中的[設定資料加密](#)。

EventBridge 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon EventBridge 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【EventBridge.2] 應標記 EventBridge 事件匯流排

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Events::EventBus

AWS Config rule：tagged-events-eventbus (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon EventBridge 事件匯流排是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果事件匯流排沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果事件匯流排未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 EventBridge 事件匯流排，請參閱 [《Amazon EventBridge 使用者指南》中的 Amazon EventBridge 標籤](#)。 EventBridge

【EventBridge.3】EventBridge 自訂事件匯流排應連接以資源為基礎的政策

相關要求：NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)、PCI DSS v4.0.1/10.3.1

類別：保護 > 安全存取管理 > 資源不可公開存取

嚴重性：低

資源類型：AWS::Events::EventBus

AWS Config 規則：[custom-eventbus-policy-attached](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EventBridge 自訂事件匯流排是否已連接以資源為基礎的政策。如果自訂事件匯流排沒有以資源為基礎的政策，則此控制會失敗。

根據預設，EventBridge 自訂事件匯流排未連接以資源為基礎的政策。這可讓帳戶中的主體存取事件匯流排。透過將資源型政策連接到事件匯流排，您可以將事件匯流排的存取權限制在指定的帳戶，以及刻意將存取權授予另一個帳戶中的實體。

修補

若要將資源型政策連接至 EventBridge 自訂事件匯流排，請參閱《[Amazon EventBridge 使用者指南](#)》中的[為 Amazon EventBridge 使用資源型政策](#)。EventBridge

【EventBridge.4】EventBridge 全域端點應啟用事件複寫

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::Events::Endpoint

AWS Config 規則：[global-endpoint-event-replication-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon EventBridge 全域端點是否已啟用事件複寫。如果全域端點未啟用事件複寫，則控制項會失敗。

全域端點有助於讓您的應用程式具有區域容錯能力。若要開始，請將 Amazon Route 53 運作狀態檢查指派給端點。啟動容錯移轉時，運作狀態檢查會報告「運作狀態不良」狀態。在容錯移轉初始化的幾分鐘內，所有自訂事件都會路由至次要區域中的事件匯流排，並由該事件匯流排處理。當您使用全域端點時，您可以啟用事件複寫。事件複寫會使用受管規則，將所有自訂事件傳送至主要和次要區域中的事件匯流排。建議您在設定全域端點時啟用事件複寫。事件複寫可協助您確認已正確設定全域端點。需要事件複寫，才能從容錯移轉事件自動復原。如果您沒有啟用事件複寫，您必須先手動將 Route 53 運作狀態檢查重設為「運作狀態」，事件才會重新路由回主要區域。

Note

如果您使用的是自訂事件匯流排，則每個區域中都需要具有相同名稱和相同帳戶中的自訂甚至匯流排，容錯移轉才能正常運作。啟用事件複寫可能會增加您的每月成本。如需定價的詳細資訊，請參閱 [Amazon EventBridge 定價](#)。

修補

若要啟用 EventBridge 全域端點的事件複寫，請參閱《Amazon EventBridge 使用者指南》中的 [建立全域端點](#)。針對事件複寫，選取啟用事件複寫。

Amazon Fraud Detector 的 Security Hub CSPM 控制項

這些 Security Hub CSPM 控制項會評估 Amazon Fraud Detector 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【FraudDetector.1】Amazon Fraud Detector 實體類型應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::FraudDetector::EntityType

AWS Config 規則：frauddetector-entity-type-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon Fraud Detector 實體類型是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果實體類型沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果實體類型未標記任何索引鍵，則控制項會失敗。系統會 aws: 忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

將標籤新增至 Amazon Fraud Detector 實體類型（主控台）

- 開啟位於 <https://console.aws.amazon.com/frauddetector> 的 Amazon Fraud Detector 主控台。
- 在導覽窗格中，選擇實體。

3. 從清單中選擇實體類型。
4. 在實體類型標籤區段中，選擇管理標籤。
5. 選擇 Add new tag (新增標籤)。輸入標籤的金鑰和值。針對其他鍵/值對重複此步驟。
6. 當您完成新增標籤的作業時，請選擇 Save (儲存)。

【FraudDetector.2】Amazon Fraud Detector 標籤應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::FraudDetector::Label

AWS Config 規則：frauddetector-label-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon Fraud Detector 標籤是否具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果標籤沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果標籤未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

將標籤新增至 Amazon Fraud Detector 標籤 (主控台)

1. 開啟位於 <https://console.aws.amazon.com/frauddetector> 的 Amazon Fraud Detector 主控台。
2. 在導覽窗格中，選擇標籤。
3. 從清單中選擇標籤。
4. 在標籤區段中，選擇管理標籤。
5. 選擇 Add new tag (新增標籤)。輸入標籤的金鑰和值。針對其他鍵/值對重複此步驟。
6. 當您完成新增標籤的作業時，請選擇 Save (儲存)。

【FraudDetector.3】Amazon Fraud Detector 結果應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::FraudDetector::Outcome

AWS Config 規則：frauddetector-outcome-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	無預設值

此控制項會檢查 Amazon Fraud Detector 結果是否具有含參數 中定義之特定金鑰的標籤 `requiredKeyTags`。如果結果沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredKeyTags`。如果 `requiredKeyTags` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果結果未標記任何索引鍵，則失敗。系統會 `aws:忽略` 自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

將標籤新增至 Amazon Fraud Detector 結果（主控台）

1. 開啟位於 <https://console.aws.amazon.com/frauddetector> 的 Amazon Fraud Detector 主控台。
2. 在導覽窗格中，選擇結果。
3. 從清單中選擇結果。
4. 在結果標籤區段中，選擇管理標籤。
5. 選擇 Add new tag (新增標籤)。輸入標籤的金鑰和值。針對其他鍵/值對重複此步驟。
6. 當您完成新增標籤的作業時，請選擇 Save (儲存)。

【FraudDetector.4】Amazon Fraud Detector 變數應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::FraudDetector::Variable

AWS Config 規則：frauddetector-variable-tagged

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon Fraud Detector 變數是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果變數沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果變數未標記任何索引鍵，則會失敗。系統會 aws: 忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

將標籤新增至 Amazon Fraud Detector 變數（主控台）

1. 開啟位於 <https://console.aws.amazon.com/frauddetector> 的 Amazon Fraud Detector 主控台。

2. 在導覽窗格中，選擇變數。
3. 從清單中選擇變數。
4. 在變數標籤區段中，選擇管理標籤。
5. 選擇 Add new tag (新增標籤)。輸入標籤的金鑰和值。針對其他鍵/值對重複此步驟。
6. 當您完成新增標籤的作業時，請選擇 Save (儲存)。

Amazon FSx 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon FSx 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【FSx.1】FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::FSx::FileSystem

AWS Config 規則：[fsx-openzfs-copy-tags-enabled](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon FSx for OpenZFS 檔案系統是否設定為將標籤複製到備份和磁碟區。如果未將 OpenZFS 檔案系統設定為將標籤複製到備份和磁碟區，則控制項會失敗。

識別和清查您的 IT 資產是控管和安全性的重要層面。標籤可協助您以不同的方式分類 AWS 資源，例如依用途、擁有者或環境。當您有許多相同類型的資源時，這會很有用，因為您可以根據指派給該資源的標籤快速識別特定資源。

修補

如需有關設定 FSx for OpenZFS 檔案系統以將標籤複製到備份和磁碟區的資訊，請參閱《Amazon FSx for OpenZFS 使用者指南》中的[更新檔案系統](#)。

【FSx.2】FSx for Lustre 檔案系統應設定為將標籤複製到備份

相關需求：NIST.800-53.r5 CP-9、NIST.800-53.r5 CM-8

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::FSx::FileSystem

AWS Config 規則：[fsx-lustre-copy-tags-to-backups](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon FSx for Lustre 檔案系統是否設定為將標籤複製到備份和磁碟區。如果未將 Lustre 檔案系統設定為將標籤複製到備份和磁碟區，則控制項會失敗。

識別和清查您的 IT 資產是控管和安全性的主要層面。標籤可協助您以不同的方式分類 AWS 資源，例如依用途、擁有者或環境。當您有許多相同類型的資源時，這會很有用，因為您可以根據指派給該資源的標籤快速識別特定資源。

修補

如需有關設定 FSx for Lustre 檔案系統將標籤複製到備份的資訊，請參閱《Amazon FSx for Lustre 使用者指南》中的在[相同的 內複製備份 AWS 帳戶](#)。

【FSx.3】FSx for OpenZFS 檔案系統應設定為異地同步備份部署

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::FSx::FileSystem

AWS Config 規則：[fsx-openzfs-deployment-type-check](#)

排程類型：定期

參數：deploymentTypes: MULTI_AZ_1 (不可自訂)

此控制項會檢查 Amazon FSx for OpenZFS 檔案系統是否設定為使用多個可用區域（多可用區域）部署類型。如果未將檔案系統設定為使用異地同步備份部署類型，則控制項會失敗。

Amazon FSx for OpenZFS 支援多種檔案系統的部署類型：異地同步備份 (HA)、單一可用區 (HA) 和單一可用區（非 HA）。部署類型提供不同層級的可用性和持久性。多可用區域 (HA) 檔案系統是由跨兩個可用區域 (AZs) 分佈的高可用性 (HA) 對檔案伺服器組成。由於多可用區域 (HA) 部署類型提供的高可用性和持久性模型，因此我們建議對大多數生產工作負載使用。

修補

您可以設定 Amazon FSx for OpenZFS 檔案系統，以在建立檔案系統時使用異地同步備份部署類型。您無法變更現有 FSx for OpenZFS 檔案系統的部署類型。

如需有關 FSx for OpenZFS 檔案系統的部署類型和選項的資訊，請參閱《[Amazon FSx for OpenZFS 使用者指南](https://docs.aws.amazon.com/fsx/latest/OpenZFSGuide/managing-file-systems.html)》中的 [Amazon FSx for OpenZFS 和管理檔案系統資源的可用性和耐用性](https://docs.aws.amazon.com/fsx/latest/OpenZFSGuide/managing-file-systems.html)。 <https://docs.aws.amazon.com/fsx/latest/OpenZFSGuide/managing-file-systems.html> FSx OpenZFS

【FSx.4】FSx for NetApp ONTAP 檔案系統應設定為異地同步備份部署

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::FSx::FileSystem

AWS Config 規則：[fsx-ontap-deployment-type-check](#)

排程類型：定期

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
deploymentTypes	要包含在評估中的部署類型清單。如果檔案系統未設定為使用清單中指定的部署類型，則控制項會產生 FAILED 問題清單。	列舉	MULTI_AZ_1 , MULTI_AZ_2	MULTI_AZ_1 , MULTI_AZ_2

此控制項會檢查 Amazon FSx for NetApp ONTAP 檔案系統是否設定為使用多個可用區域（多可用區域）部署類型。如果未將檔案系統設定為使用異地同步備份部署類型，則控制項會失敗。您可以選擇性地指定要在評估中包含的部署類型清單。

Amazon FSx for NetApp ONTAP 支援多種檔案系統的部署類型：單一可用區 1、單一可用區 2、多可用區 1 和多可用區 2。部署類型提供不同層級的可用性和持久性。由於多可用區域部署類型提供的高可用性和持久性模型，我們建議對大多數生產工作負載使用異地同步備份部署類型。多可用區域檔案系統支援單一可用區域檔案系統的所有可用性和持久性功能。此外，它們旨在提供資料的持續可用性，即使可用區域 (AZ) 無法使用也一樣。

修補

您無法變更現有 Amazon FSx for NetApp ONTAP 檔案系統的部署類型。不過，您可以備份資料，然後在使用異地同步備份部署類型的新檔案系統上還原資料。

如需有關 FSx for ONTAP 檔案系統的部署類型和選項的資訊，請參閱《FSx for ONTAP 使用者指南》中的[可用性、耐用性和部署選項](#)以及[管理檔案系統](#)。

【FSx.5】FSx for Windows File Server 檔案系統應設定為異地同步備份部署

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::FSx::FileSystem

AWS Config 規則：[fsx-windows-deployment-type-check](#)

排程類型：定期

參數：deploymentTypes: MULTI_AZ_1（不可自訂）

此控制項會檢查 Amazon FSx for Windows File Server 檔案系統是否設定為使用多個可用區域（多可用區域）部署類型。如果未將檔案系統設定為使用異地同步備份部署類型，則控制項會失敗。

Amazon FSx for Windows File Server 支援兩種檔案系統的部署類型：單一可用區和多可用區。部署類型提供不同層級的可用性和持久性。單一可用區域檔案系統由單一 Windows 檔案伺服器執行個體和單一可用區域 (AZ) 內的一組儲存磁碟區組成。多可用區域檔案系統是由分散在兩個可用區域的 Windows 檔案伺服器的高可用性叢集組成。由於提供的高可用性和持久性模型，我們建議對大多數生產工作負載使用異地同步備份部署類型。

修補

您可以設定 Amazon FSx for Windows File Server 檔案系統，以在建立檔案系統時使用異地同步備份部署類型。您無法變更現有 FSx for Windows File Server 檔案系統的部署類型。

如需 FSx for Windows File Server 檔案系統的部署類型和選項的相關資訊，請參閱《[Amazon FSx for Windows File Server 使用者指南](#)》中的[可用性和耐用性：單一可用區域和多可用區域檔案系統和 Amazon FSx for Windows File Server 入門](#)。FSx

Global Accelerator 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 AWS Global Accelerator 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【GlobalAccelerator.1】應標記 Global Accelerator 加速器

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::GlobalAccelerator::Accelerator

AWS Config rule：tagged-globalaccelerator-accelerator (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS Global Accelerator 加速器是否具有具有參數 中定義之特定索引鍵的標籤requiredTagKeys。如果加速器沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制

項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果加速器未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Global Accelerator 全域加速器，請參閱《AWS Global Accelerator 開發人員指南》中的 [在中標記 AWS Global Accelerator](#)。

的 Security Hub CSPM 控制項 AWS Glue

這些 AWS Security Hub CSPM 控制項會評估 AWS Glue 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【Glue.1】AWS Glue 工作應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Glue::Job

AWS Config rule：tagged-glue-job (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Glue 任務是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果任務沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果任務未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 AWS Glue 任務，請參閱 AWS Glue 《使用者指南》 [AWS 中的標籤 AWS Glue](#)。

【Glue.3】AWS Glue 機器學習轉換應該靜態加密

類別：保護 > 資料保護 > data-at-rest 加密

嚴重性：中

資源類型：AWS::Glue::MLTransform

AWS Config 規則：[glue-ml-transform-encrypted-at-rest](#)

排程類型：已觸發變更

參數：否

此控制項會檢查 AWS Glue 機器學習轉換是否靜態加密。如果機器學習轉換未靜態加密，則控制項會失敗。

靜態資料是指存放在持久性、非揮發性儲存體中任何持續時間的資料。加密靜態資料可協助您保護其機密性，進而降低未經授權的使用者可存取資料的風險。

修補

若要設定 AWS Glue 機器學習轉換的加密，請參閱AWS Glue 《使用者指南》中的[使用機器學習轉換](#)。

【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：AWS::Glue::Job

AWS Config 規則：[glue-spark-job-supported-version](#)

排程類型：已觸發變更

參數：minimumSupportedGlueVersion：3.0 (不可自訂)

此控制項會檢查 AWS Glue for Spark 任務是否設定為在支援的 版本上執行 AWS Glue。如果 Spark 任務設定為在早於最低支援版本的 上執行 AWS Glue，則控制項會失敗。

Note

如果任務的組態項目 (CI) 中不存在 AWS Glue 版本 (GlueVersion) 屬性或為 null，則此控制項也會為 AWS Glue for Spark 任務產生FAILED問題清單。在這種情況下，問題清單包含下列註釋：GlueVersion is null or missing in glueetl job configuration。若要

解決這類 FAILED 問題清單，請將 `GlueVersion` 屬性新增至任務的組態。如需支援版本和執行時間環境的清單，請參閱 AWS Glue 《使用者指南》中的 [AWS Glue 版本](#)。

在目前版本的上執行 AWS Glue Spark 任務 AWS Glue，可以最佳化效能、安全性和對最新功能的存取 AWS Glue。它也可以協助防範安全漏洞。例如，可能會發佈新版本，以提供安全性更新、解決問題或引進新功能。

修補

如需將 Spark 任務遷移至支援版本的相關資訊 AWS Glue，請參閱 AWS Glue 《使用者指南》中的 [遷移 AWS Glue Spark 任務](#)。

Amazon GuardDuty 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon GuardDuty 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【GuardDuty.1】應啟用 GuardDuty

相關要求：NIST.800-53.r5 AC-2(12)，NIST.800-53.r5 AU-6(1)，NIST.800-53.r5 AU-6(5)，NIST.800-53.r5 CA-7、NIST.800-53.r5 CM-8(3)，NIST.800-53.r5 RA-3(4)，NIST.800-53.r5 SA-11(1)，NIST.800-53.r5 SA-11(6)，NIST.800-53.r5 SA-15(2)，NIST.800-53.r5 SA-15(8)，NIST.800-53.r5 SA-8(19)，NIST.800-53.r5 SA-8(21)，NIST.800-53.r5 SA-8(25)，NIST.800-53.r5 SC-5、NIST.800-53.r5 SC-5(1)，NIST.800-53.r5 SC-5(3)，NIST.800-53.r5 SI-20、NIST.800-53.r5 SI-3(8)，NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(1)，NIST.800-53.r5 SI-4(13)，NIST.800-53.r5 SI-4(2)，NIST.800-53.r5 SI-4(22)，NIST.800-53.r5 SI-4(25)，NIST.800-53.r5 SI-4(4)，NIST.800-53.r5 SI-4(5)，NIST.800-171.r2 3.4.2、NIST.800-171.r2 3.14.6，NIST.800-171.r2 3.14.7、PCI DSS 3.2.1/11.4 版，PCI DSS 4.0.1/11.5.1 版

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS:::Account

AWS Config 規則：[guardduty-enabled-centralized](#)

排程類型：定期

參數：無

此控制項會檢查您的 Amazon GuardDuty 帳戶和區域中是否已啟用 Amazon GuardDuty。

強烈建議您在所有支援的區域中啟用 GuardDuty AWS。這樣做可讓 GuardDuty 產生有關未經授權或異常活動的調查結果，即使在您未主動使用的區域中也是如此。這也允許 GuardDuty 監控全域 AWS 服務的 CloudTrail 事件，例如 IAM。

修補

若要啟用 GuardDuty，請參閱《Amazon [GuardDuty 使用者指南](#)》中的 GuardDuty 入門。Amazon GuardDuty

【GuardDuty.2】GuardDuty 篩選條件應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::GuardDuty::Filter

AWS Config rule：tagged-guardduty-filter (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	No default value

此控制項會檢查 Amazon GuardDuty 篩選條件是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果篩選條件沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果篩選條件未標記任何索引鍵，則 會失敗。系統會 aws: 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義

許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 AWS 服務，包括 AWS Billing，都可以存取標籤。如需更多標記最佳實務，請參閱《[標記您的 AWS 資源](#)》中的 AWS 一般參考。

修補

若要將標籤新增至 GuardDuty 篩選條件，請參閱《Amazon GuardDuty API 參考[TagResource](#)》中的。

【GuardDuty.3] GuardDuty IPSets 應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::GuardDuty::IPSet

AWS Config rule：tagged-guarddduty-ipset (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon GuardDuty IPSet 是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果 IPSet 沒有任何標籤索引鍵，或如果它沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤

索引鍵是否存在，如果 IPSet 未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 GuardDuty IPSet，請參閱《Amazon GuardDuty API 參考[TagResource](#)》中的。

【GuardDuty.4] GuardDuty 偵測器應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::GuardDuty::Detector

AWS Config rule：tagged-guarddduty-detector (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon GuardDuty 偵測器是否具有具有參數 中定義之特定金鑰的標籤 `requiredTagKeys`。如果偵測器沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果偵測器未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 GuardDuty 偵測器，請參閱《Amazon GuardDuty API 參考 [TagResource](#)》中的 。

【GuardDuty.5】應啟用 GuardDuty EKS 稽核日誌監控

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::GuardDuty::Detector

AWS Config 規則：[guardduty-eks-protection-audit-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否啟用 GuardDuty EKS 稽核日誌監控。對於獨立帳戶，如果帳戶中停用 GuardDuty EKS 稽核日誌監控，則控制項會失敗。在多帳戶環境中，如果委派的 GuardDuty 管理員帳戶和所有成員帳戶未啟用 EKS 稽核日誌監控，則控制項會失敗。

在多帳戶環境中，控制項只會在委派的 GuardDuty 管理員帳戶中產生問題清單。只有委派管理員才能啟用或停用組織中成員帳戶的 EKS 稽核日誌監控功能。GuardDuty 成員帳戶無法從其帳戶修改此組態。如果委派的 GuardDuty 管理員具有未啟用 GuardDuty EKS 稽核日誌監控的暫停成員帳戶，則此控制項會產生 FAILED 調查結果。若要接收 PASSED 問題清單，委派管理員必須在 GuardDuty 中取消這些暫停帳戶的關聯。

GuardDuty EKS 稽核日誌監控可協助您偵測 Amazon Elastic Kubernetes Service (Amazon EKS) 叢集中的潛在可疑活動。EKS 稽核日誌監控使用 Kubernetes 稽核日誌，從使用者、使用 Kubernetes API 的應用程式和控制平面，擷取依時間順序排列的活動。

修補

若要啟用 GuardDuty EKS 稽核日誌監控，請參閱《Amazon GuardDuty 使用者指南》中的 [EKS 稽核日誌監控](#)。

【GuardDuty.6】應啟用 GuardDuty Lambda 保護

相關要求：PCI DSS v4.0.1/11.5.1

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::GuardDuty::Detector

AWS Config 規則：[guardduty-lambda-protection-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否已啟用 GuardDuty Lambda 保護。對於獨立帳戶，如果在帳戶中停用 GuardDuty Lambda 保護，則控制項會失敗。在多帳戶環境中，如果委派的 GuardDuty 管理員帳戶和所有成員帳戶未啟用 Lambda 保護，則控制項會失敗。

在多帳戶環境中，控制項只會在委派的 GuardDuty 管理員帳戶中產生問題清單。只有委派管理員才能啟用或停用組織中成員帳戶的 Lambda 保護功能。GuardDuty 成員帳戶無法從其帳戶修改此組態。如果委派的 GuardDuty 管理員具有未啟用 GuardDuty Lambda 保護的暫停成員帳戶，則此控制項會產生 FAILED 調查結果。若要接收 PASSED 問題清單，委派管理員必須在 GuardDuty 中取消這些暫停帳戶的關聯。

GuardDuty Lambda 保護可協助您在叫用 AWS Lambda 函數時識別潛在的安全威脅。啟用 Lambda 保護之後，GuardDuty 會開始監控與中 Lambda 函數相關聯的 Lambda 網路活動日誌 AWS 帳戶。當叫

用 Lambda 函數且 GuardDuty 識別可疑的網路流量，指出 Lambda 函數中存在潛在惡意的程式碼片段時，GuardDuty 會產生問題清單。

修補

若要啟用 GuardDuty Lambda 保護，請參閱《Amazon GuardDuty 使用者指南》中的[設定 Lambda 保護](#)。

【GuardDuty.7】應啟用 GuardDuty EKS 執行期監控

相關要求：PCI DSS v4.0.1/11.5.1

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::GuardDuty::Detector

AWS Config 規則：[guardduty-eks-protection-runtime-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否已啟用具有自動代理程式管理的 GuardDuty EKS 執行期監控。對於獨立帳戶，如果在帳戶中停用具有自動代理程式管理的 GuardDuty EKS 執行期監控，則控制項會失敗。在多帳戶環境中，如果委派的 GuardDuty 管理員帳戶和所有成員帳戶未啟用自動代理程式管理的 EKS 執行期監控，則控制項會失敗。

在多帳戶環境中，控制項只會在委派的 GuardDuty 管理員帳戶中產生問題清單。只有委派管理員才能為組織中的成員帳戶啟用或停用具有自動代理程式管理的 EKS 執行期監控功能。GuardDuty 成員帳戶無法從其帳戶修改此組態。如果委派的 GuardDuty 管理員具有未啟用 GuardDuty EKS 執行期監控的暫停成員帳戶，則此控制項會產生 FAILED 調查結果。若要接收 PASSED 問題清單，委派管理員必須在 GuardDuty 中取消這些暫停帳戶的關聯。

Amazon GuardDuty 中的 EKS 保護提供威脅偵測涵蓋範圍，有助於保護 AWS 環境中的 Amazon EKS 叢集。EKS 執行期監控使用作業系統層級事件，協助您偵測 EKS 叢集內 EKS 節點和容器中的潛在威脅。

修補

若要使用自動代理程式管理啟用 EKS 執行期監控，請參閱《Amazon [GuardDuty 使用者指南](#)》中的[啟用 GuardDuty 執行期監控](#)。Amazon GuardDuty

【GuardDuty.8】應啟用 EC2 的 GuardDuty 惡意軟體防護

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::GuardDuty::Detector

AWS Config 規則：[guardduty-malware-protection-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否啟用 GuardDuty 惡意軟體防護。對於獨立帳戶，如果帳戶中停用 GuardDuty 惡意軟體防護，則控制項會失敗。在多帳戶環境中，如果委派的 GuardDuty 管理員帳戶和所有成員帳戶未啟用惡意軟體防護，則控制項會失敗。

在多帳戶環境中，控制項只會在委派的 GuardDuty 管理員帳戶中產生問題清單。只有委派管理員可以啟用或停用組織中成員帳戶的惡意軟體防護功能。GuardDuty 成員帳戶無法從其帳戶修改此組態。如果委派的 GuardDuty 管理員具有未啟用 GuardDuty 惡意軟體防護的暫停成員帳戶，則此控制項會產生 FAILED 調查結果。若要接收 PASSED 問題清單，委派管理員必須在 GuardDuty 中取消這些暫停帳戶的關聯。

GuardDuty Malware Protection for EC2 透過掃描連接到 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體和容器工作負載的 Amazon Elastic Block Store (Amazon EBS) 磁碟區，協助您偵測潛在的惡意軟體存在。惡意軟體防護提供掃描選項，您可以在掃描時決定是否要包含或排除特定 EC2 執行個體和容器工作負載。它還提供在 GuardDuty 帳戶中保留連接到 EC2 執行個體或容器工作負載之 EBS 磁碟區的快照的選項。只有在發現惡意軟體並產生惡意軟體防護調查結果時，才會保留快照。

修補

若要啟用 EC2 的 GuardDuty 惡意軟體防護，請參閱《Amazon [GuardDuty 使用者指南](#)》中的設定 [GuardDuty 起始的惡意軟體掃描](#)。Amazon GuardDuty

【GuardDuty.9】應啟用 GuardDuty RDS 保護

相關要求：PCI DSS v4.0.1/11.5.1

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::GuardDuty::Detector

AWS Config 規則：[guardduty-rds-protection-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否已啟用 GuardDuty RDS 保護。對於獨立帳戶，如果在帳戶中停用 GuardDuty RDS 保護，則控制項會失敗。在多帳戶環境中，如果委派的 GuardDuty 管理員帳戶和所有成員帳戶未啟用 RDS 保護，則控制項會失敗。

在多帳戶環境中，控制項只會在委派的 GuardDuty 管理員帳戶中產生問題清單。只有委派管理員才能啟用或停用組織中成員帳戶的 RDS 保護功能。GuardDuty 成員帳戶無法從其帳戶修改此組態。如果委派的 GuardDuty 管理員具有未啟用 GuardDuty RDS 保護的暫停成員帳戶，則此控制項會產生 FAILED 調查結果。若要接收 PASSED 問題清單，委派管理員必須在 GuardDuty 中取消這些暫停帳戶的關聯。

GuardDuty 中的 RDS 保護會分析和分析 RDS 登入活動，以找出對 Amazon Aurora 資料庫的潛在存取威脅 (Aurora MySQL 相容版本和 Aurora PostgreSQL 相容版本)。此功能可讓您識別潛在的可疑登入行為。RDS 保護不需要額外的基礎設施；專門為不影響資料庫執行個體的效能而設計。當 RDS 保護偵測到潛在的可疑或異常登入嘗試 (這表明資料庫存在安全威脅) 時，GuardDuty 會產生新的調查結果，其中包含可能被盜用之資料庫的詳細資訊。

修補

若要啟用 GuardDuty RDS 保護，請參閱《Amazon [GuardDuty 使用者指南](#)》中的 [GuardDuty RDS 保護](#)。Amazon GuardDuty

【GuardDuty.10】應啟用 GuardDuty S3 保護

相關要求：PCI DSS v4.0.1/11.5.1

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::GuardDuty::Detector

AWS Config 規則：[guardduty-s3-protection-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否已啟用 GuardDuty S3 保護。對於獨立帳戶，如果在帳戶中停用 GuardDuty S3 保護，則控制項會失敗。在多帳戶環境中，如果委派的 GuardDuty 管理員帳戶和所有成員帳戶未啟用 S3 保護，則控制項會失敗。

在多帳戶環境中，控制項只會在委派的 GuardDuty 管理員帳戶中產生問題清單。只有委派管理員才能啟用或停用組織中成員帳戶的 S3 保護功能。GuardDuty 成員帳戶無法從其帳戶修改此組態。如果委派的 GuardDuty 管理員具有未啟用 GuardDuty S3 保護的暫停成員帳戶，則此控制項會產生 FAILED 調查結果。若要接收 PASSED 問題清單，委派管理員必須在 GuardDuty 中取消這些暫停帳戶的關聯。

S3 保護可讓 GuardDuty 監控物件層級 API 操作，以識別 Amazon Simple Storage Service (Amazon S3) 儲存貯體中資料的潛在安全風險。GuardDuty 透過分析 AWS CloudTrail 管理事件和 CloudTrail S3 資料事件來監控對 S3 資源的威脅。S3

修補

若要啟用 GuardDuty S3 保護，請參閱《[Amazon S3 Amazon GuardDuty 使用者指南](#)》中的 [Amazon GuardDuty Amazon GuardDuty S3 保護](#)。

【GuardDuty.11】應啟用 GuardDuty 執行期監控

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::GuardDuty::Detector

AWS Config 規則：[guardduty-runtime-monitoring-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否在 Amazon GuardDuty 中啟用執行期監控。對於獨立帳戶，如果帳戶停用 GuardDuty 執行期監控，則控制項會失敗。在多帳戶環境中，如果委派的 GuardDuty 管理員帳戶和所有成員帳戶停用 GuardDuty 執行期監控，則控制項會失敗。

在多帳戶環境中，只有委派的 GuardDuty 管理員可以啟用或停用組織中帳戶的 GuardDuty 執行期監控。此外，只有 GuardDuty 管理員可以設定和管理 GuardDuty 用來監控組織中帳戶 AWS 工作負載和

資源的執行時間的安全代理程式。GuardDuty 成員帳戶無法為自己的帳戶啟用、設定或停用執行期監控。

GuardDuty 執行期監控會觀察和分析作業系統層級、聯網和檔案事件，以協助您偵測環境中特定 AWS 工作負載的潛在威脅。它使用 GuardDuty 安全代理程式來增加執行時間行為的可見性，例如檔案存取、程序執行、命令列引數和網路連線。您可以為要監控潛在威脅的每種資源類型啟用和管理安全代理程式，例如 Amazon EKS 叢集和 Amazon EC2 執行個體。

修補

如需有關設定和啟用 GuardDuty 執行期監控的資訊，請參閱《Amazon [GuardDuty 使用者指南](#)》中的 [GuardDuty 執行期監控](#)和[啟用 GuardDuty 執行期監控](#)。Amazon GuardDuty

【GuardDuty.12】應啟用 GuardDuty ECS 執行期監控

類別：偵測 > 偵測服務

嚴重性：中

資源類型：AWS::GuardDuty::Detector

AWS Config 規則：[guardduty-ecs-protection-runtime-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否已啟用 Amazon GuardDuty 自動化安全代理程式，以監控 Amazon ECS 叢集的執行時間 AWS Fargate。對於獨立帳戶，如果停用帳戶的安全代理程式，則控制項會失敗。在多帳戶環境中，如果委派的 GuardDuty 管理員帳戶和所有成員帳戶停用安全代理程式，則控制項會失敗。

在多帳戶環境中，此控制項只會在委派的 GuardDuty 管理員帳戶中產生調查結果。這是因為只有委派的 GuardDuty 管理員可以啟用或停用組織中帳戶的 ECS-Fargate 資源執行期監控。GuardDuty 成員帳戶無法對自己的帳戶執行此操作。此外，如果成員帳戶的 GuardDuty 暫停，且成員帳戶的 ECS-Fargate 資源的執行期監控已停用，則此控制項會產生 FAILED 調查結果。若要接收 PASSED 調查結果，GuardDuty 管理員必須使用 GuardDuty 取消暫停的成員帳戶與其管理員帳戶的關聯。

GuardDuty 執行期監控會觀察和分析作業系統層級、聯網和檔案事件，以協助您偵測環境中特定 AWS 工作負載的潛在威脅。它使用 GuardDuty 安全代理程式來增加執行時間行為的可見性，例如檔案存取、程序執行、命令列引數和網路連線。您可以為要監控潛在威脅的每種資源類型啟用和管理安全代理程式。這包括上的 Amazon ECS 叢集 AWS Fargate。

修補

若要啟用和管理 ECS-Fargate 資源的 GuardDuty 執行期監控的安全代理程式，您必須直接使用 GuardDuty。您無法為 ECS-Fargate 資源啟用或手動管理它。如需有關啟用和管理安全代理程式的資訊，請參閱 [《Amazon GuardDuty 使用者指南》中的 AWS Fargate \(僅限 Amazon ECS\) 支援和管理 \(僅限 Amazon ECS\) 的自動化安全代理程式的先決條件](#)。 [AWS Fargate](#) Amazon GuardDuty

【GuardDuty.13】應啟用 GuardDuty EC2 執行期監控

類別：偵測 > 偵測服務

嚴重性：中

資源類型：AWS::GuardDuty::Detector

AWS Config 規則：[guardduty-ec2-protection-runtime-enabled](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon GuardDuty 自動化安全代理程式是否已啟用 Amazon EC2 執行個體的執行期監控。對於獨立帳戶，如果停用帳戶的安全代理程式，則控制項會失敗。在多帳戶環境中，如果委派的 GuardDuty 管理員帳戶和所有成員帳戶停用安全代理程式，則控制項會失敗。

在多帳戶環境中，此控制項只會在委派的 GuardDuty 管理員帳戶中產生調查結果。這是因為只有委派的 GuardDuty 管理員可以為組織中的帳戶啟用或停用 Amazon EC2 執行個體的執行期監控。GuardDuty 成員帳戶無法對自己的帳戶執行此操作。此外，如果成員帳戶的 GuardDuty 暫停，且成員帳戶的 EC2 執行個體執行期監控已停用，則此控制項會產生 FAILED 調查結果。若要接收 PASSED 調查結果，GuardDuty 管理員必須使用 GuardDuty 取消暫停的成員帳戶與其管理員帳戶的關聯。

GuardDuty 執行期監控會觀察和分析作業系統層級、聯網和檔案事件，以協助您偵測環境中特定 AWS 工作負載的潛在威脅。它使用 GuardDuty 安全代理程式來增加執行時間行為的可見性，例如檔案存取、程序執行、命令列引數和網路連線。您可以為要監控潛在威脅的每種資源類型啟用和管理安全代理程式。這包括 Amazon EC2 執行個體。

修補

如需為 EC2 執行個體的 GuardDuty 執行期監控設定和管理自動化安全代理程式的相關資訊，請參閱 [《Amazon GuardDuty 使用者指南》中的 Amazon EC2 執行個體支援和啟用 Amazon EC2 執行個體的自動化安全代理程式的先決條件](#)。 [Amazon EC2](#) Amazon GuardDuty

的 Security Hub CSPM 控制項 AWS Identity and Access Management

這些 AWS Security Hub CSPM 控制項會評估 AWS Identity and Access Management (IAM) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【IAM.1】 IAM 政策不應允許完整的「*」管理權限

相關要求：CIS AWS Foundations Benchmark v1.2.0/1.22、CIS AWS Foundations Benchmark v1.4.0/1.16、NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6800-55.r5)、NIST-50.5)、NIST-50.50 NIST.800-53.r5 AC-6.

類別：保護 > 安全存取管理

嚴重性：高

資源類型：AWS::IAM::Policy

AWS Config 規則：[iam-policy-no-statements-with-admin-access](#)

排程類型：已觸發變更

參數：

- `excludePermissionBoundaryPolicy: true` (不可自訂)

此控制項會檢查預設版本的 IAM 政策 (也稱為客戶受管政策) 是否具有管理員存取權，方法是使用 "Effect": "Allow" 搭配 "Action": "*" 的陳述式 "Resource": "*"。如果您有具有此類陳述式的 IAM 政策，則控制項會失敗。

控制項只會檢查您建立的客戶受管政策。它不會檢查內嵌和 AWS 受管政策。

IAM 政策定義一組授予使用者、群組或角色的權限。遵循標準安全建議，AWS 建議您授予最低權限，這表示僅授予執行任務所需的許可。在您提供完整管理權限而非使用者需要的最低許可組時，您便會向潛在的不需要動作公開資源。

相較於允許完整的管理權限，建議您決定使用者需要做什麼，然後打造政策，讓使用者只執行這些任務。以最小的一組許可開始，然後依需要授予額外的許可更加安全。不要從太寬鬆的許可開始，稍後才嘗試限縮這些許可。

您應該移除具有陳述式的 IAM 政策，該陳述 "Effect": "Allow" 式具有 "Action": "*" 超過的 "Resource": "*"。

 Note

AWS Config 應在您使用 Security Hub CSPM 的所有區域中啟用。不過，可在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要修改您的 IAM 政策，使其不允許完整的「*」管理權限，請參閱 [《IAM 使用者指南》中的編輯 IAM 政策](#)。

【IAM.2】 IAM 使用者不應連接 IAM 政策

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.14、CIS AWS Foundations Benchmark v3.0.0/1.15、CIS AWS Foundations Benchmark v1.2.0/1.16、NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-66(3)、NIST.8000-17.r2

類別：保護 > 安全存取管理

嚴重性：低

資源類型：AWS::IAM::User

AWS Config 規則：[iam-user-no-policies-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查您的 IAM 使用者是否已連接政策。如果您的 IAM 使用者已連接政策，則控制項會失敗。相反地，IAM 使用者必須繼承 IAM 群組的許可或擔任角色。

根據預設，IAM 使用者、群組和角色無法存取 AWS 資源。IAM 政策會將權限授予使用者、群組或角色。我們建議您將 IAM 政策直接套用至群組和角色，而不是使用者。在群組或角色層級指派權限，會減少隨使用者數量成長而增加的存取管理複雜性。降低存取管理複雜性，可能會降低無意中讓委託人接收或保留過多權限的機會。

 Note

AWS Config 應在您使用 Security Hub CSPM 的所有區域中啟用。不過，可在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，您可以在記錄全域資源的區域以外的所有區域中停用此控制項。

修補

若要解決此問題，[請建立 IAM 群組](#)，並將政策連接至群組。然後，[將使用者新增至群組](#)。政策即會套用到群組中的每個使用者。若要移除直接連接到使用者的政策，請參閱《[IAM 使用者指南](#)》中的[新增和移除 IAM 身分許可](#)。

【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.13、CIS AWS Foundations Benchmark v3.0.0/1.14、CIS AWS Foundations Benchmark v1.4.0/1.14、CIS AWS Foundations Benchmark v1.2.0/1.4、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-2(3)、NIST.800-53.r5 AC-3(15)、PCI DSS v4.0.1/8.3.9、PCI DSS v4.0.1/8.6.3

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::IAM::User

AWS Config 規則：[access-keys-rotated](#)

排程類型：定期

參數：

- maxAccessKeyAge：90 (不可自訂)

此控制項會檢查作用中的存取金鑰是否會在 90 天內輪換。

我們強烈建議您不要產生和移除帳戶中的所有存取金鑰。反之，建議的最佳實務是建立一或多個 IAM 角色或使用[聯合](#) AWS IAM Identity Center。您可以使用這些方法來允許使用者存取 AWS 管理主控台和 AWS CLI。

每種方法都有其使用案例。對於具有現有中央目錄或計劃需要超過 IAM 使用者目前限制的企業而言，聯合通常更好。在 AWS 環境外部執行的應用程式需要存取金鑰，才能以程式設計方式存取 AWS 資源。

不過，如果需要程式設計存取的資源在內部執行 AWS，最佳實務是使用 IAM 角色。角色可讓您授予資源存取，而無須在組態中硬式編碼存取金鑰 ID 和私密存取金鑰。

若要進一步了解如何保護您的存取金鑰和帳戶，請參閱《》中的[管理 AWS 存取金鑰的最佳實務](#) AWS 一般參考。另請參閱部落格文章 [在使用程式設計存取 AWS 帳戶時保護的指導方針](#)。

如果您已有存取金鑰，Security Hub CSPM 建議您每 90 天輪換存取金鑰。輪換存取金鑰可降低使用與被盜用或已終止帳戶相關聯存取金鑰的機會。這也能確保無法使用可能遺失、毀損或遭竊的舊金鑰存取資料。請在您輪換存取金鑰後一律更新應用程式。

存取金鑰由存取金鑰 ID 和私密存取金鑰組成。它們用於簽署您提出的程式設計請求 AWS。使用者需要自己的存取金鑰，才能使用個別的 API 操作 AWS，從 AWS CLI、Tools for Windows PowerShell、AWS SDKs 或直接 HTTP 呼叫對進行程式設計呼叫 AWS 服務。

如果您的組織使用 AWS IAM Identity Center (IAM Identity Center)，您的使用者可以登入 Active Directory、內建的 IAM Identity Center 目錄，或[連線至 IAM Identity Center 的其他身分提供者 \(IdP\)](#)。然後，它們可以映射到 IAM 角色，使他們能夠執行 AWS CLI 命令或呼叫 AWS API 操作，而無需存取金鑰。若要進一步了解，請參閱 AWS Command Line Interface 《使用者指南》中的[設定 AWS CLI 以使用 AWS IAM Identity Center](#)。

Note

AWS Config 應在您使用 Security Hub CSPM 的所有區域中啟用。不過，可在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要輪換超過 90 天的存取金鑰，請參閱《IAM 使用者指南》中的[輪換存取金鑰](#)。對於存取金鑰存留期大於 90 天的任何使用者，請遵循指示。

【IAM.4】 IAM 根使用者存取金鑰不應存在

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.3、CIS AWS Foundations Benchmark v3.0.0/1.4、CIS AWS Foundations Benchmark v1.4.0/1.4、CIS AWS Foundations Benchmark

v1.2.0/1.12、PCI DSS v3.2.1/2.1、PCI DSS v3.2.1/2.2、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6

類別：保護 > 安全存取管理

嚴重性：嚴重

資源類型：AWS:::Account

AWS Config 規則：[iam-root-access-key-check](#)

排程類型：定期

參數：無

此控制項會檢查根使用者存取金鑰是否存在。

根使用者是 中最高權限的使用者 AWS 帳戶。AWS 存取金鑰提供對指定帳戶的程式設計存取。

Security Hub CSPM 建議您移除與根使用者相關聯的所有存取金鑰。這限制了可用於入侵您帳戶的向量。這也會鼓勵建立和使用擁有最低權限的角色類型帳戶。

修補

若要刪除根使用者存取金鑰，請參閱《IAM 使用者指南》中的[刪除根使用者的存取金鑰](#)。若要從 AWS 帳戶 中刪除根使用者存取金鑰 AWS GovCloud (US)，請參閱AWS GovCloud (US) 《使用者指南》中的[刪除我的 AWS GovCloud \(US\) 帳戶根使用者存取金鑰](#)。

[IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.9、CIS AWS Foundations Benchmark v3.0.0/1.10、CIS AWS Foundations Benchmark v1.4.0/1.10、CIS AWS Foundations Benchmark v1.2.0/1.2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-2(2)、NIST.800-5.r5 IA-2(6)、NIST.800-5.r5)、PCI-IA-200.

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::IAM::User

AWS Config 規則：[mfa-enabled-for-iam-console-access](#)

排程類型：定期

參數：無

此控制項會檢查是否針對使用主控台密碼的所有 IAM 使用者啟用 AWS 多重驗證 (MFA)。

Multi-Factor authentication (MFA) 在使用者名稱和密碼之外，多增加一層保護。啟用 MFA 後，當使用者登入 AWS 網站時，系統會提示他們輸入其使用者名稱和密碼。此外，系統會提示他們從 AWS MFA 裝置輸入驗證碼。

我們建議您為擁有主控台密碼的所有帳戶啟用 MFA。MFA 的設計旨在為主控台存取提供更高的安全。身分驗證委託人必須擁有發出時效性金鑰的裝置，並且必須擁有登入資料的知識。

 Note

AWS Config 應在您使用 Security Hub CSPM 的所有區域中啟用。不過，可在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要為 IAM 使用者新增 MFA，請參閱《IAM 使用者指南》中的[在中使用多重要素驗證 \(MFA\) AWS](#)。

[IAM.6] 應為根使用者啟用硬體 MFA

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.5、CIS AWS Foundations Benchmark v3.0.0/1.6、CIS AWS Foundations Benchmark v1.4.0/1.6、CIS AWS Foundations Benchmark v1.2.0/1.14、PCI DSS v3.2.1/8.3.1、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-22(2)、NIST.8000-5. IA-2

類別：保護 > 安全存取管理

嚴重性：嚴重

資源類型：AWS:::Account

AWS Config 規則：[root-account-hardware-mfa-enabled](#)

排程類型：定期

參數：無

此控制項會檢查您的 AWS 帳戶 是否已啟用使用硬體多重要素驗證 (MFA) 裝置，以根使用者憑證登入。如果未啟用硬體 MFA 或允許使用根使用者登入資料登入虛擬 MFA 裝置，則控制項會失敗。

虛擬 MFA 可能無法提供與硬體 MFA 裝置相同層級的安全。建議您只在等待硬體購買核准或硬體送達時使用虛擬 MFA 裝置。若要進一步了解，請參閱《IAM 使用者指南》中的[指派虛擬 MFA 裝置（主控台）](#)。

Note

Security Hub CSPM 會根據 中根使用者憑證（登入設定檔）的存在來評估此控制項 AWS 帳戶。在下列情況下，控制項會產生 PASSED 問題清單：

- 根使用者登入資料存在於帳戶中，且已啟用根使用者的硬體 MFA。
- 根使用者憑證不存在於帳戶中。

如果根使用者登入資料存在於帳戶中，且根使用者未啟用硬體 MFA，則控制項會產生 FAILED 問題清單。

修補

如需有關為根使用者啟用硬體 MFA 的資訊，請參閱《IAM 使用者指南》中的 [的多重要素驗證 AWS 帳戶根使用者](#)。

【IAM.7】 IAM 使用者的密碼政策應具有強大的組態

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-2(3)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-5(1)、NIST.800-171.r2 3.5.2、NIST.800-171.r2 3.5.7、NIST.800-171.r2 3.5.8、PCI DSS v4.0.1/8.3.6、PCI DSS v4.0.1/8.3.7、PCI v4.0.98.3.10

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：[iam-password-policy](#)

排程類型：定期

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
RequireUppercaseCharacters	密碼中至少需要一個大寫字元	Boolean	true 或 false *	true
RequireLowercaseCharacters	密碼中至少需要一個小寫字元	Boolean	true 或 false *	true
RequireSymbols	密碼中至少需要一個符號	Boolean	true 或 false *	true
RequireNumbers	密碼中至少需要一個數字	Boolean	true 或 false *	true
MinimumPasswordLength	密碼中的字元數下限	Integer	8 至 128	8
PasswordReusePrevention	重複使用舊密碼之前的密碼輪換次數	Integer	12 至 24	無預設值
MaxPasswordAge	密碼過期前的天數	Integer	1 至 90	無預設值

此控制項會檢查 IAM 使用者的帳戶密碼政策是否使用強式組態。如果密碼政策不使用強式組態，則控制項會失敗。除非您提供自訂參數值，否則 Security Hub CSPM 會使用上表中提及的預設值。PasswordReusePrevention 和 MaxPasswordAge 參數沒有預設值，因此如果您排除這些參數，Security Hub CSPM 會在評估此控制項時忽略密碼輪換次數和密碼存留期。

若要存取 AWS 管理主控台，IAM 使用者需要密碼。最佳實務是，Security Hub CSPM 強烈建議您使用聯合，而不是建立 IAM 使用者。聯合允許使用者使用其現有的公司登入資料來登入 AWS 管理主控

台。使用 AWS IAM Identity Center (IAM Identity Center) 建立或聯合使用者，然後在帳戶中擔任 IAM 角色。

若要進一步了解身分提供者和聯合身分，請參閱《IAM 使用者指南》中的[身分提供者和聯合身分](#)。若要進一步了解 IAM Identity Center，請參閱 [AWS IAM Identity Center 使用者指南](#)。

如果您需要使用 IAM 使用者，Security Hub CSPM 建議您強制建立強式使用者密碼。您可以在 [上設定密碼政策 AWS 帳戶](#)，以指定密碼的複雜性要求和強制性輪換期間。當您建立或變更密碼政策時，會在下次使用者變更其密碼時強制執行大部分的密碼政策設定。某些設定會立即強制執行。

修補

若要更新密碼政策，請參閱《[IAM 使用者指南](#)》中的[為 IAM 使用者設定帳戶密碼政策](#)。

【IAM.8】應移除未使用的 IAM 使用者登入資料

相關要求：CIS AWS Foundations Benchmark v1.2.0/1.3、NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-2(3)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-171.r2 3.1.2、PCI v3.2.1/8.1.4、PCI v4.02.1.6。

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::IAM::User

AWS Config 規則：[iam-user-unused-credentials-check](#)

排程類型：定期

參數：

- maxCredentialUsageAge : 90 (不可自訂)

此控制項會檢查您的 IAM 使用者是否有密碼或作用中的存取金鑰，而這些金鑰已在 90 天內未使用。

IAM 使用者可以使用不同類型的登入資料來存取 AWS 資源，例如密碼或存取金鑰。

Security Hub CSPM 建議您移除或停用所有未使用 90 天或更長時間的登入資料。停用或移除不必要的登入資料，可以減少使用與被盜用或放棄帳戶相關聯登入資料的機會。

 Note

AWS Config 應在您使用 Security Hub CSPM 的所有區域中啟用。不過，可在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

當您在 IAM 主控台中檢視使用者資訊時，有存取金鑰存留期、密碼存留期和上次活動的資料欄。如果上述任一欄的值大於 90 天，請將這些使用者的登入資料設定為非作用中。

您也可以使用[登入資料報告](#)來監控使用者，並識別 90 天或更長時間內沒有活動的使用者。您可以從 IAM 主控台下載 .csv 格式的登入資料報告。

識別非作用中帳戶或未使用的登入資料後，請停用它們。如需說明，請參閱 [《IAM 使用者指南》中的建立、變更或刪除 IAM 使用者密碼（主控台）](#)。

【IAM.9】 應為根使用者啟用 MFA

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.4、PCI DSS v3.2.1/8.3.1、PCI DSS v4.0.1/8.4.2、CIS AWS Foundations Benchmark v3.0.0/1.5、CIS AWS Foundations Benchmark v1.4.0/1.5、CIS AWS Foundations Benchmark v1.2.0/1.13、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-5 IA-2

類別：保護 > 安全存取管理

嚴重性：嚴重

資源類型：AWS::::Account

AWS Config 規則：[root-account-mfa-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否已啟用多重要素驗證 (MFA)，AWS 帳戶 讓 的 IAM 根使用者登入 AWS 管理主控台。如果未為帳戶的根使用者啟用 MFA，則控制項會失敗。

的 IAM 根使用者 AWS 帳戶 具有帳戶中所有 服務和資源的完整存取權。如果已啟用 MFA，使用者必須輸入其 AWS MFA 裝置的使用者名稱、密碼和驗證碼，才能登入 AWS 管理主控台。MFA 在使用者名稱和密碼之外多加一層保護。

此控制項會在下列情況下產生PASSED問題清單：

- 根使用者憑證存在於帳戶中，並為根使用者啟用 MFA。
- 根使用者憑證不存在於帳戶中。

如果根使用者憑證存在於帳戶中，且未為根使用者啟用 MFA，控制項會產生FAILED調查結果。

修補

如需為 的根使用者啟用 MFA 的詳細資訊 AWS 帳戶，請參閱AWS Identity and Access Management 《使用者指南》中的 [的多重要素驗證 AWS 帳戶根使用者](#)。

【IAM.10】 IAM 使用者的密碼政策應具有強大的組態

相關要求：NIST.800-171.r2 3.5.2、NIST.800-171.r2 3.5.7、NIST.800-171.r2 3.5.8、PCI DSS v3.2.1/8.1.4、PCI DSS v3.2.1/8.2.3、PCI DSS v3.2.1/8.2.4、PCI DSS v3.2.1/8.2.5

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：[iam-password-policy](#)

排程類型：定期

參數：無

此控制項會檢查 IAM 使用者的帳戶密碼政策是否使用以下最低 PCI DSS 組態。

- RequireUppercaseCharacters – 密碼中至少需要一個大寫字元。(預設 = true)
- RequireLowercaseCharacters – 密碼中至少需要一個小寫字元。(預設 = true)
- RequireNumbers – 密碼中至少需要一個數字。(預設 = true)
- MinimumPasswordLength – 密碼長度下限。(預設值 = 7 或更久)
- PasswordReusePrevention – 允許重複使用之前的密碼數目。(預設 = 4)
- MaxPasswordAge – 密碼過期前的天數。(預設 = 90)

 Note

2025 年 5 月 30 日，Security Hub CSPM 將此控制項從 PCI DSS v4.0.1 標準中移除。PCI DSS v4.0.1 現在需要密碼至少 8 個字元。此控制會持續套用至具有不同密碼要求的 PCI DSS v3.2.1 標準。

若要根據 PCI DSS v4.0.1 要求評估帳戶密碼政策，您可以使用 [IAM.7 控制項](#)。此控制項需要密碼至少 8 個字元。它也支援密碼長度和其他參數的自訂值。IAM.7 控制項是 Security Hub CSPM 中 PCI DSS v4.0.1 標準的一部分。

修補

若要更新密碼政策以使用建議的組態，請參閱 [《IAM 使用者指南》](#) 中的 [為 IAM 使用者設定帳戶密碼政策](#)。

【IAM.11】 確保 IAM 密碼政策至少需要一個大寫字母

相關要求：CIS AWS Foundations Benchmark v1.2.0/1.5、NIST.800-171.r2 3.5.7、PCI DSS v4.0.1/8.3.6、PCI DSS v4.0.1/8.6.3

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：[iam-password-policy](#)

排程類型：定期

參數：無

密碼政策是強制執行密碼複雜性要求的一部分。使用 IAM 密碼政策來確保密碼使用不同的字元集。

CIS 建議密碼政策至少需要一個大寫字母。設定密碼複雜性政策以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱 [《IAM 使用者指南》](#) 中的 [為 IAM 使用者設定帳戶密碼政策](#)。針對密碼強度，從拉丁字母 (A–Z) 選取至少需要一個大寫字母。

【IAM.12】 確保 IAM 密碼政策至少需要一個小寫字母

相關要求：CIS AWS Foundations Benchmark v1.2.0/1.6、NIST.800-171.r2 3.5.7、PCI DSS v4.0.1/8.3.6、PCI DSS v4.0.1/8.6.3

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：[iam-password-policy](#)

排程類型：定期

參數：無

密碼政策是強制執行密碼複雜性要求的一部分。使用 IAM 密碼政策來確保密碼使用不同的字元集。CIS 建議密碼政策至少需要一個小寫字母。設定密碼複雜性政策以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱《[IAM 使用者指南](#)》中的為 IAM 使用者設定帳戶密碼政策。對於密碼強度，請從拉丁字母 (A–Z) 選取至少需要一個小寫字母。

【IAM.13】 確保 IAM 密碼政策至少需要一個符號

相關要求：CIS AWS Foundations Benchmark v1.2.0/1.7、NIST.800-171.r2 3.5.7

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：[iam-password-policy](#)

排程類型：定期

參數：無

密碼政策是強制執行密碼複雜性要求的一部分。使用 IAM 密碼政策來確保密碼使用不同的字元集。

CIS 建議密碼政策至少需要一個符號。設定密碼複雜性政策以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱《[IAM 使用者指南](#)》中的為 IAM 使用者設定帳戶密碼政策。針對密碼強度，選取至少需要一個非英數字元。

【IAM.14】 確保 IAM 密碼政策至少需要一個數字

相關要求：CIS AWS Foundations Benchmark v1.2.0/1.8、NIST.800-171.r2 3.5.7、PCI DSS v4.0.1/8.3.6、PCI DSS v4.0.1/8.6.3

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS:::Account

AWS Config 規則：[iam-password-policy](#)

排程類型：定期

參數：無

密碼政策是強制執行密碼複雜性要求的一部分。使用 IAM 密碼政策來確保密碼使用不同的字元集。

CIS 建議密碼政策至少需要一個數字。設定密碼複雜性政策以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱《[IAM 使用者指南](#)》中的為 IAM 使用者設定帳戶密碼政策。針對密碼強度，選取至少需要一個數字。

【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.7、CIS AWS Foundations Benchmark v3.0.0/1.8、CIS AWS Foundations Benchmark v1.4.0/1.8、CIS AWS Foundations Benchmark v1.2.0/1.9、NIST.800-171.r2 3.5.7

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：[iam-password-policy](#)

排程類型：定期

參數：無

密碼政策是強制執行密碼複雜性要求的一部分。使用 IAM 密碼政策來確保密碼至少為指定長度。

CIS 建議密碼政策至少需要 14 個字元的密碼長度。設定密碼複雜性政策以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱《[IAM 使用者指南](#)》中的[為 IAM 使用者設定帳戶密碼政策](#)。針對密碼長度下限，輸入 **14**或較大的數字。

【IAM.16】 確保 IAM 密碼政策防止密碼重複使用

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.8、CIS AWS Foundations Benchmark v3.0.0/1.9、CIS AWS Foundations Benchmark v1.4.0/1.9、CIS AWS Foundations Benchmark v1.2.0/1.10、NIST.800-171.r2 3.5.8、PCI DSS v4.0.1/8.3.7

類別：保護 > 安全存取管理

嚴重性：低

資源類型：AWS::::Account

AWS Config 規則：[iam-password-policy](#)

排程類型：定期

參數：無

此控制項會檢查要記住的密碼數目是否設定為 24。如果值不是 24，則控制項會失敗。

IAM 密碼政策可防止相同使用者重複使用指定的密碼。

CIS 建議密碼政策防止密碼重複使用。防止重複使用密碼以提高帳戶彈性，因應暴力登入嘗試。

修補

若要變更密碼政策，請參閱《[IAM 使用者指南](#)》中的為 IAM 使用者設定帳戶密碼政策。針對防止密碼重複使用，輸入 **24**。

【IAM.17】 確保 IAM 密碼政策在 90 天內過期密碼

相關要求：CIS AWS Foundations Benchmark v1.2.0/1.11、PCI DSS v4.0.1/8.3.9、PCI DSS v4.0.1/8.3.10.1

類別：保護 > 安全存取管理

嚴重性：低

資源類型：AWS::::Account

AWS Config 規則：[iam-password-policy](#)

排程類型：定期

參數：無

IAM 密碼政策可以要求密碼在特定天數後輪換或過期。

CIS 建議密碼政策在 90 天後過期密碼。縮短密碼生命週期以提高帳戶彈性，因應暴力登入嘗試。要求定期密碼變更，也有助於下列案例：

- 在您不知情時，密碼遭竊或被盜用。這會透過系統入侵、軟體漏洞或內部威脅而發生。
- 某些企業和政府的 web 篩選條件或代理伺服器可以攔截並記錄流量，即使流量加密。
- 許多人在很多系統 (如工作、電子郵件和個人) 都使用相同的密碼。
- 遭入侵的最終使用者工作站可能有按鍵記錄器。

修補

若要變更密碼政策，請參閱《[IAM 使用者指南](#)》中的為 IAM 使用者設定帳戶密碼政策。針對開啟密碼過期，輸入 **90**或較小的數字。

【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.16、CIS AWS Foundations Benchmark v3.0.0/1.17、CIS AWS Foundations Benchmark v1.4.0/1.17、CIS AWS Foundations Benchmark v1.2.0/1.20、NIST.800-171.r2 3.1.2、PCI DSS v4.0.1/12.10.3

類別：保護 > 安全存取管理

嚴重性：低

資源類型：AWS:::Account

AWS Config 規則：[iam-policy-in-use](#)

排程類型：定期

參數：

- policyARN : arn:*partition*:iam::aws:policy/AWSSupportAccess (不可自訂)
- policyUsageType : ANY (不可自訂)

AWS 提供可用於事件通知和回應的支援中心，以及技術支援和客戶服務。

建立 IAM 角色，以允許授權使用者透過 AWS Support 管理事件。透過實作存取控制的最低權限，IAM 角色將需要適當的 IAM 政策，以允許支援中心存取，以便使用 管理事件 支援。

Note

AWS Config 應在您使用 Security Hub CSPM 的所有區域中啟用。不過，可在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要修復此問題，請建立 角色，以允許授權使用者管理 支援 事件。

建立用於 支援 存取的角色

1. 前往 <https://console.aws.amazon.com/iam/> 開啟 IAM 主控台。
2. 在 IAM 導覽窗格中，選擇角色，然後選擇建立角色。
3. 針對角色類型，選擇另一個 AWS 帳戶。
4. 針對帳戶 ID，輸入您要授予資源存取權之 AWS 帳戶 的 AWS 帳戶 ID。

如果將擔任此角色的使用者或群組位在相同帳戶，則請輸入本機帳戶號碼。

Note

指定帳戶的管理員可以授予許可給該帳戶中的任何使用者來擔任此角色。若要執行此操作，管理員要將政策連接到授予 `sts:AssumeRole` 動作之許可的使用者或群組。在該政策中，資源必須是角色 ARN。

5. 選擇下一步：許可。
6. 搜尋受管政策 `AWSSupportAccess`。
7. 選取 `AWSSupportAccess` 受管政策的核取方塊。
8. 選擇下一步：標籤。
9. (選用) 若要將中繼資料新增至角色，請將標籤附加為索引鍵/值對。

如需在 IAM 中使用標籤的詳細資訊，請參閱 [《IAM 使用者指南》中的標記 IAM 使用者和角色](#)。

10. 選擇下一步：檢閱。
11. 針對 Role name (角色名稱)，輸入您的角色名稱。

角色名稱在您的 中必須是唯一的 AWS 帳戶。不區分大小寫。

12. (選用) 在 Role description (角色說明) 中，輸入新角色的說明。
13. 檢閱角色，然後選擇 Create role (建立角色)。

【IAM.19】應為所有 IAM 使用者啟用 MFA

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 IA-2(1)、NIST.800-53.r5 IA-2(2)、NIST.800-53.r5 IA-2(6)、NIST.800-53.r5 IA-2(8)、NIST.800-171.r2 3.8、NIST.800-171.r2 3.5.3、NIST.800-171.r2 3.5.4、NIST.800-17.5

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::IAM::User

AWS Config 規則：[iam-user-mfa-enabled](#)

排程類型：定期

參數：無

此控制項會檢查 IAM 使用者是否已啟用多重要素驗證 (MFA)。

 Note

AWS Config 應在您使用 Security Hub CSPM 的所有區域中啟用。不過，可在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要為 IAM 使用者新增 MFA，請參閱《IAM 使用者指南》中的[在中為使用者啟用 MFA 裝置 AWS](#)。

【IAM.20】 避免使用根使用者

 Important

Security Hub CSPM 已於 2024 年 4 月淘汰此控制項。如需詳細資訊，請參閱[Security Hub CSPM 控制項的變更日誌](#)。

相關要求：CIS AWS Foundations Benchmark v1.2.0/1.1

類別：保護 > 安全存取管理

嚴重性：低

資源類型：AWS::IAM::User

AWS Config rule：use-of-root-account-test (自訂 Security Hub CSPM 規則)

排程類型：定期

參數：無

此控制項會檢查 AWS 帳戶 對根使用者的用量是否有限制。控制項會評估下列資源：

- Amazon Simple Notification Service (Amazon SNS) 主題
- AWS CloudTrail 線索
- 與 CloudTrail 追蹤相關聯的指標篩選條件

- 根據篩選條件的 Amazon CloudWatch 警示

如果下列一或多個陳述式為 true，則此檢查會產生 FAILED 問題清單：

- 帳戶中不存在 CloudTrail 追蹤。
- CloudTrail 追蹤已啟用，但未設定至少一個包含讀取和寫入管理事件的多區域追蹤。
- CloudTrail 追蹤已啟用，但未與 CloudWatch Logs 日誌群組建立關聯。
- 不會使用 Center for Internet Security (CIS) 指定的確切指標篩選條件。指定的指標篩選條件為 `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}'`。
- 帳戶中不存在以指標篩選條件為基礎的 CloudWatch 警示。
- 設定為傳送通知至相關聯 SNS 主題的 CloudWatch 警示不會根據警示條件觸發。
- SNS 主題不符合[傳送訊息至 SNS 主題的限制](#)。
- SNS 主題至少沒有一個訂閱者。

NO_DATA 如果下列一或多個陳述式為 true，則此檢查會導致控制狀態為：

- 多區域追蹤是以不同的區域為基礎。Security Hub CSPM 只能在追蹤所在的區域中產生問題清單。
- 多區域追蹤屬於不同的帳戶。Security Hub CSPM 只能為擁有追蹤的帳戶產生問題清單。

WARNING 如果下列一或多個陳述式為 true，則此檢查會導致控制狀態為：

- 目前帳戶不擁有 CloudWatch 警示中參考的 SNS 主題。
- 目前帳戶在叫用 SNS API 時無法存取 ListSubscriptionsByTopic SNS 主題。

Note

我們建議您使用組織追蹤記錄組織中許多帳戶的事件。根據預設，組織線索是多區域線索，只能由 AWS Organizations 管理帳戶或 CloudTrail 委派管理員帳戶管理。對於組織成員帳戶中評估的控制項，使用組織線索會導致 NO_DATA 的控制狀態。在成員帳戶中，Security Hub CSPM 只會為成員擁有的資源產生調查結果。與組織追蹤相關的調查結果會在資源擁有者的帳戶中產生。您可以使用跨區域彙總，在 Security Hub CSPM 委派管理員帳戶中查看這些問題清單。

最佳實務是，只有在需要執行帳戶和服務管理任務時，才使用您的根使用者憑證。將 IAM 政策直接套用至群組和角色，而非使用者。如需設定管理員以供每日使用的指示，請參閱《[IAM 使用者指南](#)》中的[建立您的第一個 IAM 管理員使用者和群組](#)。

修補

修復此問題的步驟包括設定 Amazon SNS 主題、CloudTrail 追蹤、指標篩選條件，以及指標篩選條件的警示。

建立 Amazon SNS 主題

1. 在 <https://console.aws.amazon.com/sns/v3/home> 開啟 Amazon SNS 主控台。
2. 建立接收所有 CIS 警示的 Amazon SNS 主題。

至少建立一個主題訂閱者。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 [Amazon SNS 入門](#)。

接著，設定套用至所有區域的作用中 CloudTrail。若要執行此作業，請遵循 [the section called “【CloudTrail.1】CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤”](#) 中的修補步驟。

記下您與 CloudTrail 追蹤建立關聯的 CloudWatch Logs 日誌群組名稱。CloudTrail 您可以為該日誌群組建立指標篩選條件。

最後，建立指標篩選條件和警示。

建立指標篩選條件和警示

1. 透過 <https://console.aws.amazon.com/cloudwatch/> 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇 Log groups (日誌群組)。
3. 選取與您建立的 CloudTrail 追蹤相關聯的 CloudWatch Logs 日誌群組的核取方塊。CloudTrail
4. 在動作中，選擇建立指標篩選條件。
5. 在定義模式下，執行下列動作：
 - a. 複製以下模式，然後將它貼入 Filter Pattern (篩選條件模式) 欄位。

```
{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}
```

- b. 選擇下一步。

6. 在指派指標下，執行下列動作：
 - a. 在篩選條件名稱中，輸入指標篩選條件的名稱。
 - b. 針對指標命名空間，輸入 **LogMetrics**。

如果您對所有 CIS 日誌指標篩選條件使用相同的命名空間，則所有 CIS 基準指標都會分組在一起。
 - c. 針對指標名稱，輸入指標的名稱。記住指標的名稱。建立警示時，您將需要選取指標。
 - d. 針對 Metric value (指標值)，輸入 **1**。
 - e. 選擇下一步。
7. 在檢閱和建立下，驗證您為新指標篩選條件提供的資訊。然後，選擇建立指標篩選條件。
8. 在導覽窗格中，選擇日誌群組，然後選擇您在指標篩選條件下建立的篩選條件。
9. 選取篩選條件的核取方塊。選擇 Create alarm (建立警示)。
10. 在指定指標和條件下，執行下列動作：
 - a. 在條件下，針對閾值選擇靜態。
 - b. 針對定義警示條件，選擇大於/等於。
 - c. 針對定義閾值，輸入 **1**。
 - d. 選擇下一步。
11. 在設定動作下，執行下列動作：
 - a. 在警示狀態觸發下，選擇警示中。
 - b. 在 Select an SNS topic (選取 SNS 主題) 下，選擇 Select an existing SNS topic (選取現有的 SNS 主題)。
 - c. 針對傳送通知至，輸入您在先前程序中建立的 SNS 主題名稱。
 - d. 選擇下一步。
12. 在新增名稱和描述下，輸入警示的名稱和描述，例如 **CIS-1.1-RootAccountUsage**。然後選擇下一步。
13. 在預覽和建立下，檢閱警示組態。然後選擇 Create Alarm (建立警示)。

【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作

相關需求：NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2)、NIST.800-53.r5 AC-6(3)、NIST.800-171.1.13。

類別：偵測 > 安全存取管理

嚴重性：低

資源類型：AWS::IAM::Policy

AWS Config 規則：[iam-policy-no-statements-with-full-access](#)

排程類型：已觸發變更

參數：

- `excludePermissionBoundaryPolicy` : `True` (不可自訂)

此控制項會檢查您建立的 IAM 身分型政策是否具有使用 * 萬用字元授予任何服務上所有動作許可的允許陳述式。如果任何政策陳述式包含 "Effect": "Allow" 與 "Action": "Service:*"。

例如，政策中的下列陳述式會導致問題清單失敗。

```
"Statement": [  
  {  
    "Sid": "EC2-Wildcard",  
    "Effect": "Allow",  
    "Action": "ec2:*",  
    "Resource": "*"  
  }  
]
```

如果您 "Effect": "Allow" 搭配使用 "NotAction": "*service*:"，控制項也會失敗。在這種情況下，NotAction 元素會提供中所有動作的存取權 AWS 服務，但中指定的動作除外 NotAction。

此控制僅適用於客戶受管 IAM 政策。它不適用於由管理的 IAM 政策 AWS。

當您將許可指派給時 AWS 服務，請務必在 IAM 政策中限制允許的 IAM 動作。您應該將 IAM 動作限制為僅需要的動作。這可協助您佈建最低權限許可。如果政策連接到可能不需要許可的 IAM 主體，過度寬鬆的政策可能會導致權限提升。

在某些情況下，您可能想要允許具有類似字首的 IAM 動作，例如 DescribeFlowLogs 和 DescribeAvailabilityZones。在這些授權情況下，您可以將尾碼的萬用字元新增至通用字首。例如 `ec2:Describe*`。

如果您使用字首 IAM 動作搭配尾碼萬用字元，則此控制項會通過。例如，政策中的下列陳述式會導致問題清單通過。

```
"Statement": [  
  {  
    "Sid": "EC2-Wildcard",  
    "Effect": "Allow",  
    "Action": "ec2:Describe*",  
    "Resource": "*"   
  }  
]
```

當您以這種方式將相關的 IAM 動作分組時，您也可以避免超過 IAM 政策大小限制。

Note

AWS Config 應在您使用 Security Hub CSPM 的所有區域中啟用。不過，可在單一區域中啟用全域資源記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

若要修復此問題，請更新您的 IAM 政策，使其不允許完整的「*」管理權限。如需如何編輯 IAM 政策的詳細資訊，請參閱 [《IAM 使用者指南》中的編輯 IAM 政策](#)。

【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.11、CIS AWS Foundations Benchmark v3.0.0/1.12、CIS AWS Foundations Benchmark v1.4.0/1.12、NIST.800-171.r2 3.1.2

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::IAM::User

AWS Config 規則：[iam-user-unused-credentials-check](#)

排程類型：定期

參數：無

此控制項會檢查您的 IAM 使用者是否有密碼或作用中的存取金鑰，而這些金鑰已在 45 天或更長時間內未使用。若要這樣做，它會檢查 AWS Config 規則的 `maxCredentialUsageAge` 參數是否等於 45 個或更多。

使用者可以使用不同類型的登入資料來存取 AWS 資源，例如密碼或存取金鑰。

CIS 建議您移除或停用所有已使用 45 天或更長時間的登入資料。停用或移除不必要的登入資料，可以減少使用與被盜用或放棄帳戶相關聯登入資料的機會。

此控制項的 AWS Config 規則使用 [GetCredentialReport](#) 和 [GenerateCredentialReport](#) API 操作，只會每四小時更新一次。IAM 使用者變更最多可能需要四小時才能顯示此控制項。

Note

AWS Config 應在您使用 Security Hub CSPM 的所有區域中啟用。不過，您可以在單一區域中啟用全域資源的記錄。如果您只記錄單一區域中的全域資源，則可以在所有區域中停用此控制項，但記錄全域資源的區域以外。

修補

當您在 IAM 主控台中檢視使用者資訊時，有存取金鑰存留期、密碼存留期和上次活動的資料欄。如果任何資料欄中的值大於 45 天，請將這些使用者的登入資料設為非作用中。

您也可以使用[登入資料報告](#)來監控使用者，並識別 45 天或更長時間內沒有活動的使用者。您可以從 IAM 主控台下載 `.csv` 格式的登入資料報告。

識別非作用中帳戶或未使用的登入資料後，請停用它們。如需說明，請參閱 [《IAM 使用者指南》中的建立、變更或刪除 IAM 使用者密碼（主控台）](#)。

【IAM.23】 IAM Access Analyzer 分析器應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::AccessAnalyzer::Analyzer

AWS Config rule：tagged-accessanalyzer-analyzer（自訂 Security Hub CSPM 規則）

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查由 AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) 管理的分析器是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果分析器沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果分析器未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至分析器，請參閱《AWS IAM Access Analyzer API 參考 [TagResource](#)》中的。

【IAM.24】IAM 角色應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IAM::Role

AWS Config rule：tagged-iam-role (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1-6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS Identity and Access Management (IAM) 角色是否具有具有參數中定義之特定金鑰的標籤requiredTagKeys。如果角色沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果角色未標記任何索引鍵，則會失敗。系統會aws:忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#)一般參考。

修補

若要將標籤新增至 IAM 角色，請參閱《[IAM 使用者指南](#)》中的標記 IAM 資源。

【IAM.25】 IAM 使用者應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IAM::User

AWS Config rule：tagged-iam-user (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS Identity and Access Management (IAM) 使用者是否具有含參數 中定義之特定金鑰的標籤requiredTagKeys。如果使用者沒有任何標籤索引鍵，或如果它沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果使用者未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 IAM 使用者，請參閱 [《IAM 使用者指南》中的標記 IAM 資源](#)。

【IAM.26】應移除在 IAM 中管理的過期 SSL/TLS 憑證

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.18、CIS AWS Foundations Benchmark v3.0.0/1.19

類別：識別 > 合規

嚴重性：中

資源類型：AWS::IAM::ServerCertificate

AWS Config 規則：[iam-server-certificate-expiration-check](#)

排程類型：定期

參數：無

此控制項會檢查在 IAM 中管理的作用中 SSL/TLS 伺服器憑證是否已過期。如果未移除過期的 SSL/TLS 伺服器憑證，則控制項會失敗。

若要在中啟用網站或應用程式的 HTTPS 連線 AWS，您需要 SSL/TLS 伺服器憑證。您可以使用 IAM 或 AWS Certificate Manager (ACM) 來存放和部署伺服器憑證。只有當您必須在 ACM 不支援的中支援 HTTPS 連線時 AWS 區域，才能使用 IAM 做為憑證管理員。IAM 會安全地加密您的私有金鑰並將加密的版本儲存在 IAM SSL 憑證存放區中。IAM 支援在所有區域中部署伺服器憑證，但您必須從外部供應商取得憑證以搭配使用 AWS。您無法將 ACM 憑證上傳至 IAM。此外，您無法從 IAM 主控台管理憑證。移除過期的 SSL/TLS 憑證可避免將無效憑證意外部署到資源的風險，這可能會損害基礎應用程式或網站的可信度。

修補

若要從 IAM 移除伺服器憑證，請參閱 [《IAM 使用者指南》中的在 IAM 中管理伺服器憑證](#)。

【IAM.27】IAM 身分不應連接 AWSCloudShellFullAccess 政策

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.21、CIS AWS Foundations Benchmark v3.0.0/1.22

類別：保護 > 安全存取管理 > 安全 IAM 政策

嚴重性：中

資源類型：AWS::IAM::Role、AWS::IAM::User、AWS::IAM::Group

AWS Config 規則：[iam-policy-blacklisted-check](#)

排程類型：已觸發變更

參數：

- "policyArns": "arn : aws : iam : : aws : policy/AWSCloudShellFullAccess , arn : aws-cn : iam : : aws : policy/AWSCloudShellFullAccess , arn : aws-us-gov : iam : : aws : policy/AWSCloudShellFullAccess"

此控制項會檢查 IAM 身分（使用者、角色或群組）是否已AWSCloudShellFullAccess連接 AWS 受管政策。如果 IAM 身分已連接AWSCloudShellFullAccess政策，則控制項會失敗。

AWS CloudShell 提供執行 CLI 命令的便利方式 AWS 服務。AWS 受管政策AWSCloudShellFullAccess提供 CloudShell 的完整存取權，允許使用者本機系統和 CloudShell 環境之間的檔案上傳和下載功能。在 CloudShell 環境中，使用者具有 sudo 許可，並且可以存取網際網路。因此，將此受管政策轉換為 IAM 身分，讓他們能夠安裝檔案傳輸軟體，並將資料從 CloudShell 移至外部網際網路伺服器。我們建議您遵循最低權限原則，並將較窄的許可連接至您的 IAM 身分。

修補

若要從 IAM 身分分離AWSCloudShellFullAccess政策，請參閱 [《IAM 使用者指南》中的新增和移除 IAM 身分許可](#)。

【IAM.28】應啟用 IAM Access Analyzer 外部存取分析器

相關要求：CIS AWS Foundations Benchmark v5.0.0/1.19、CIS AWS Foundations Benchmark v3.0.0/1.20

類別：偵測 > 偵測服務 > 特殊權限用量監控

嚴重性：高

資源類型：AWS::AccessAnalyzer::Analyzer

AWS Config 規則：[iam-external-access-analyzer-enabled](#)

排程類型：定期

參數：無

此控制項會檢查 AWS 帳戶 是否已啟用 IAM Access Analyzer 外部存取分析器。如果目前選取的帳戶未啟用外部存取分析器，則控制項會失敗 AWS 區域。

IAM Access Analyzer 外部存取分析器可協助識別與外部實體共用的資源，例如 Amazon Simple Storage Service (Amazon S3) 儲存貯體或 IAM 角色。這可協助您避免意外存取資源和資料。IAM Access Analyzer 是區域性的，必須在每個區域中啟用。為了識別與外部主體共用的資源，存取分析器會使用邏輯推理來分析您 AWS 環境中以資源為基礎的政策。當您建立外部存取分析器時，您可以為整個組織或個別帳戶建立並啟用它。

 Note

如果帳戶是 中組織的一部分 AWS Organizations，則此控制項不會考慮將組織指定為信任區域的外部存取分析器，並在目前區域中為組織啟用。如果您的組織使用此類型的組態，請考慮停用組織中個別成員帳戶的此控制項。

修補

如需有關在特定區域中啟用外部存取分析器的資訊，請參閱 [《IAM 使用者指南》中的 IAM Access Analyzer 入門](#)。您必須在要監控資源存取權的每個區域中啟用分析器。

Amazon Inspector 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Inspector 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Inspector.1】 應啟用 Amazon Inspector EC2 掃描

相關要求：PCI DSS v4.0.1/11.3.1

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::::Account

AWS Config 規則：[inspector-ec2-scan-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否已啟用 Amazon Inspector EC2 掃描。對於獨立帳戶，如果在帳戶中停用 Amazon Inspector EC2 掃描，則控制項會失敗。在多帳戶環境中，如果委派的 Amazon Inspector 管理員帳戶和所有成員帳戶未啟用 EC2 掃描，則控制項會失敗。

在多帳戶環境中，控制項只會在委派的 Amazon Inspector 管理員帳戶中產生問題清單。只有委派管理員才能啟用或停用組織中成員帳戶的 EC2 掃描功能。Amazon Inspector 成員帳戶無法從其帳戶修改此組態。如果委派管理員的暫停成員帳戶未啟用 Amazon Inspector EC2 掃描，則此控制項會產生 FAILED 調查結果。若要接收 PASSED 問題清單，委派管理員必須在 Amazon Inspector 中取消這些暫停帳戶的關聯。

Amazon Inspector EC2 掃描會從 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體擷取中繼資料，然後將此中繼資料與從安全建議收集的規則進行比較，以產生問題清單。Amazon Inspector 會掃描執行個體是否有套件漏洞和網路連線能力問題。如需有關支援的作業系統的資訊，包括哪些作業系統可以在不使用 SSM 代理程式的情況下掃描，請參閱 [支援的作業系統：Amazon EC2 掃描](#)。

修補

若要啟用 Amazon Inspector EC2 掃描，請參閱《Amazon Inspector 使用者指南》中的 [啟用掃描](#)。

【Inspector.2】應啟用 Amazon Inspector ECR 掃描

相關要求：PCI DSS v4.0.1/11.3.1

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::::Account

AWS Config 規則：[inspector-ecr-scan-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否已啟用 Amazon Inspector ECR 掃描。對於獨立帳戶，如果在帳戶中停用 Amazon Inspector ECR 掃描，則控制項會失敗。在多帳戶環境中，如果委派的 Amazon Inspector 管理員帳戶和所有成員帳戶未啟用 ECR 掃描，則控制項會失敗。

在多帳戶環境中，控制項只會在委派的 Amazon Inspector 管理員帳戶中產生問題清單。只有委派管理員才能啟用或停用組織中成員帳戶的 ECR 掃描功能。Amazon Inspector 成員帳戶無法從其帳戶修改此組態。如果委派管理員的暫停成員帳戶未啟用 Amazon Inspector ECR 掃描，則此控制項會產生 FAILED 調查結果。若要接收 PASSED 問題清單，委派管理員必須在 Amazon Inspector 中取消這些暫停帳戶的關聯。

Amazon Inspector 會掃描存放在 Amazon Elastic Container Registry (Amazon ECR) 中的容器映像是否有軟體漏洞，以產生套件漏洞問題清單。當您啟用 Amazon ECR 的 Amazon Inspector 掃描時，您可以將 Amazon Inspector 設定為私有登錄檔的偏好掃描服務。這會取代 Amazon ECR 免費提供的基本掃描，以及透過 Amazon Inspector 提供和計費的增強型掃描。增強型掃描可讓您在登錄檔層級掃描作業系統和程式設計語言套件的漏洞。您可以在 Amazon ECR 主控台上檢閱影像層級使用增強型掃描對影像每一層發現的問題清單。此外，您可以在其他不適用於基本掃描問題清單的服務中檢閱和使用這些問題清單，包括 AWS Security Hub CSPM 和 Amazon EventBridge。

修補

若要啟用 Amazon Inspector ECR 掃描，請參閱《Amazon Inspector 使用者指南》中的[啟用掃描](#)。

【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描

相關要求：PCI DSS v4.0.1/6.2.4、PCI DSS v4.0.1/6.3.1

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::::Account

AWS Config 規則：[inspector-lambda-code-scan-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否已啟用 Amazon Inspector Lambda 程式碼掃描。對於獨立帳戶，如果在帳戶中停用 Amazon Inspector Lambda 程式碼掃描，則控制項會失敗。在多帳戶環境中，如果委派的 Amazon Inspector 管理員帳戶和所有成員帳戶未啟用 Lambda 程式碼掃描，則控制項會失敗。

在多帳戶環境中，控制項只會在委派的 Amazon Inspector 管理員帳戶中產生問題清單。只有委派管理員才能啟用或停用組織中成員帳戶的 Lambda 程式碼掃描功能。Amazon Inspector 成員帳戶無法從其帳戶修改此組態。如果委派管理員的暫停成員帳戶未啟用 Amazon Inspector Lambda 程式碼掃描，則

此控制項會產生FAILED調查結果。若要接收PASSED問題清單，委派管理員必須在 Amazon Inspector 中取消這些暫停帳戶的關聯。

Amazon Inspector Lambda 程式碼掃描會根據 AWS 安全最佳實務，掃描 AWS Lambda 函數中的自訂應用程式程式碼是否有程式碼漏洞。Lambda 程式碼掃描可以偵測程式碼中的注入缺陷、資料洩漏、弱式密碼編譯或缺少加密。此功能[AWS 區域 僅適用於特定](#)。您可以啟用 Lambda 程式碼掃描與 Lambda 標準掃描（請參閱 [【Inspector.4】應啟用 Amazon Inspector Lambda 標準掃描](#)）。

修補

若要啟用 Amazon Inspector Lambda 程式碼掃描，請參閱《Amazon Inspector 使用者指南》中的[啟用掃描](#)。

【Inspector.4】應啟用 Amazon Inspector Lambda 標準掃描

相關要求：PCI DSS v4.0.1/6.2.4、PCI DSS v4.0.1/6.3.1

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS:::Account

AWS Config 規則：[inspector-lambda-standard-scan-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否已啟用 Amazon Inspector Lambda 標準掃描。對於獨立帳戶，如果在帳戶中停用 Amazon Inspector Lambda 標準掃描，則控制項會失敗。在多帳戶環境中，如果委派的 Amazon Inspector 管理員帳戶和所有成員帳戶未啟用 Lambda 標準掃描，則控制項會失敗。

在多帳戶環境中，控制項只會在委派的 Amazon Inspector 管理員帳戶中產生問題清單。只有委派管理員才能啟用或停用組織中成員帳戶的 Lambda 標準掃描功能。Amazon Inspector 成員帳戶無法從其帳戶修改此組態。如果委派管理員的暫停成員帳戶未啟用 Amazon Inspector Lambda 標準掃描，則此控制項會產生FAILED調查結果。若要接收PASSED問題清單，委派管理員必須在 Amazon Inspector 中取消這些暫停帳戶的關聯。

Amazon Inspector Lambda 標準掃描可識別您新增至 AWS Lambda 函數程式碼和層的應用程式套件相依性中的軟體漏洞。如果 Amazon Inspector 在您的 Lambda 函數應用程式套件相依性中偵測到漏洞，Amazon Inspector 會產生詳細的Package Vulnerability類型調查結果。您可以啟用 Lambda

程式碼掃描與 Lambda 標準掃描 (請參閱 [【Inspector.3】應啟用 Amazon Inspector Lambda 程式碼掃描](#))。

修補

若要啟用 Amazon Inspector Lambda 標準掃描，請參閱《Amazon Inspector 使用者指南》中的[啟用掃描](#)。

的 Security Hub CSPM 控制項 AWS IoT

這些 AWS Security Hub CSPM 控制項會評估 AWS IoT 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【IoT.1】AWS IoT Device Defender 安全設定檔應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoT::SecurityProfile

AWS Config rule：tagged-iot-securityprofile (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS IoT Device Defender 安全性描述檔是否具有具有參數中定義之特定金鑰的標籤requiredTagKeys。如果安全性描述檔沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果沒有使用任何索引鍵標記安全性設定檔，則會失敗。系統會aws:忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 AWS IoT Device Defender 安全性描述檔，請參閱《AWS IoT 開發人員指南》中的[標記您的 AWS IoT 資源](#)。

【IoT.2】AWS IoT Core 應標記緩解動作

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoT::MitigationAction

AWS Config rule：tagged-iot-mitigationaction (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS IoT Core 緩解動作是否具有具有參數 中定義之特定金鑰的標籤 `requiredTagKeys`。如果緩解動作沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果緩解動作未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 AWS IoT Core 緩解動作，請參閱《AWS IoT 開發人員指南》中的 [標記您的 AWS IoT 資源](#)。

【IoT.3】AWS IoT Core 維度應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoT::Dimension

AWS Config rule：tagged-iot-dimension（自訂 Security Hub CSPM 規則）

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	No default value

此控制項會檢查維度是否具有具有參數中定義之特定索引鍵的標籤 `requiredTagKeys`。如果維度沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果維度未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 AWS IoT Core 維度，請參閱《AWS IoT 開發人員指南》中的 [標記您的 AWS IoT 資源](#)。

【IoT.4】AWS IoT Core 授權方應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoT::Authorizer

AWS Config rule : tagged-iot-authorizer (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS IoT Core 授權方是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果授權方沒有任何標籤索引鍵，或如果它沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果授權方未標記任何索引鍵，則控制項會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 AWS IoT Core 授權方，請參閱《AWS IoT 開發人員指南》中的 [標記您的 AWS IoT 資源](#)。

【IoT.5】AWS IoT Core 角色別名應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoT::RoleAlias

AWS Config rule：tagged-iot-rolealias (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS IoT Core 角色別名是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果角色別名沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果角色別名未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#)AWS 一般參考。

修補

若要將標籤新增至 AWS IoT Core 角色別名，請參閱《AWS IoT 開發人員指南》中的[標記您的 AWS IoT 資源](#)。

【IoT.6】AWS IoT Core 政策應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoT::Policy

AWS Config rule：tagged-iot-policy (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS IoT Core 政策是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果政策沒有任何標籤索引鍵，或如果它沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果政策未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 AWS IoT Core 政策，請參閱《AWS IoT 開發人員指南》中的[標記您的 AWS IoT 資源](#)。

AWS IoT 事件的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 AWS IoT Events 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【IoTEvents.1】AWS IoT Events 輸入應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTEvents::Input

AWS Config 規則：iotevents-input-tagged

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT Events 輸入是否具有具有參數 中定義之特定金鑰的標籤requiredKeyTags。如果輸入沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項

會失敗 `requiredKeyTags`。如果 `requiredKeyTags` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果輸入未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT Events 輸入，請參閱《AWS IoT Events 開發人員指南》中的[標記您的 AWS IoT Events 資源](#)。

【IoTEvents.2】AWS IoT Events 偵測器模型應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTEvents::DetectorModel

AWS Config 規則：iotevents-detector-model-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT Events 偵測器模型是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果偵測器模型沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果偵測器模型未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT Events 偵測器模型，請參閱《AWS IoT Events 開發人員指南》中的 [標記您的 AWS IoT Events 資源](#)。

【IoTEvents.3】AWS IoT Events 警示模型應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTEvents::AlarmModel

AWS Config 規則：iotevents-alarm-model-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT Events 警示模型是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果警示模型沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果警示模型未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT 事件警示模型，請參閱《AWS IoT Events 開發人員指南》中的 [標記您的 AWS IoT Events 資源](#)。

適用於 AWS IoT SiteWise 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 AWS IoT SiteWise 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【IoTSiteWise.1】AWS IoT SiteWise 資產模型應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTSiteWise::AssetModel

AWS Config 規則：iotsitewise-asset-model-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT SiteWise 資產模型是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果資產模型沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果資產模型未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT SiteWise 資產模型，請參閱AWS IoT SiteWise 《使用者指南》中的[標記您的 AWS IoT SiteWise 資源](#)。

【IoTSiteWise.2】AWS IoT SiteWise 儀表板應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTSiteWise::Dashboard

AWS Config 規則：iotsitewise-dashboard-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT SiteWise 儀表板是否具有具有參數中定義之特定金鑰的標籤requiredKeyTags。如果儀表板沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗requiredKeyTags。如果requiredKeyTags未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果儀表板未標記任何索引鍵，則會失敗。系統會aws:忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT SiteWise 儀表板，請參閱AWS IoT SiteWise 《使用者指南》中的[標記您的 AWS IoT SiteWise 資源](#)。

【IoTSiteWise.3】AWS IoT SiteWise 閘道應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTSiteWise::Gateway

AWS Config 規則：iotsitewise-gateway-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT SiteWise 閘道是否具有具有參數 中定義之特定金鑰的標籤 `requiredKeyTags`。如果閘道沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredKeyTags`。如果 `requiredKeyTags` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果閘道未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT SiteWise 閘道，請參閱 AWS IoT SiteWise 《使用者指南》中的[標記您的 AWS IoT SiteWise 資源](#)。

【IoTSiteWise.4】AWS IoT SiteWise 入口網站應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTSiteWise::Portal

AWS Config 規則：iotsitewise-portal-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT SiteWise 入口網站是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果入口網站沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果入口網站未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT SiteWise 入口網站，請參閱 AWS IoT SiteWise 《使用者指南》中的 [標記您的 AWS IoT SiteWise 資源](#)。

【IoTSiteWise.5】AWS IoT SiteWise 專案應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTSiteWise::Project

AWS Config 規則：iotsitewise-project-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT SiteWise 專案是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果專案沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果專案未標記任何索引鍵，則控制會失敗。系統會忽略以 aws: 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 AWS 服務都可以存取標籤，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT SiteWise 專案，請參閱 AWS IoT SiteWise 《使用者指南》中的 [標記您的 AWS IoT SiteWise 資源](#)。

適用於 AWS IoT TwinMaker 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 AWS IoT TwinMaker 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【IoT TwinMaker.1】AWS 應標記 IoT TwinMaker 同步任務

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoT TwinMaker::SyncJob

AWS Config 規則：iottwinmaker-sync-job-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT TwinMaker 同步任務是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果同步任務沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果同步任務未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT TwinMaker 同步任務，請參閱AWS IoT TwinMaker 《使用者指南[TagResource](#)》中的 。

【IoTtwinmaker.2】AWS IoT TwinMaker 工作區應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTtwinmaker::Workspace

AWS Config 規則：iottwinmaker-workspace-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT TwinMaker 工作區是否具有具有參數 中定義之特定金鑰的標籤requiredKeyTags。如果工作區沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredKeyTags。如果requiredKeyTags未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果工作區未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT TwinMaker 工作區，請參閱 AWS IoT TwinMaker 《使用者指南 [TagResource](#)》中的。

【IoT TwinMaker.3】AWS IoT TwinMaker 場景應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoT::TwinMaker::Scene

AWS Config 規則：iottwinmaker-scene-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT TwinMaker 場景是否具有具有參數 中定義之特定金鑰的標籤 `requiredKeyTags`。如果場景沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredKeyTags`。如果 `requiredKeyTags` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果場景未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT TwinMaker 場景，請參閱 AWS IoT TwinMaker 《使用者指南 [TagResource](#)》中的 。

【IoT TwinMaker.4】AWS IoT TwinMaker 實體應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoT::TwinMaker::Entity

AWS Config 規則：iottwinmaker-entity-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS IoT TwinMaker 實體是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果實體沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果實體未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 AWS IoT TwinMaker 實體，請參閱 AWS IoT TwinMaker 《使用者指南 [TagResource](#)》中的。

適用於 AWS IoT Wireless 的 Security Hub CSPM 控制

這些 AWS Security Hub CSPM 控制項會評估 AWS IoT Wireless 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【IoTWireless.1】AWS IoT Wireless 多點傳送群組應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTWireless::MulticastGroup

AWS Config 規則：iotwireless-multicast-group-tagged

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 an AWS IoT Wireless 多點傳送群組是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果多點傳送群組沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果多點傳送群組未標記任何索引鍵，則會失敗。系統會 aws: 忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 an AWS IoT Wireless 多點傳送群組，請參閱《AWS IoT Wireless 開發人員指南》中的[標記您的 AWS IoT Wireless 資源](#)。

【IoTWireless.2】AWS IoT Wireless 服務設定檔應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTWireless::ServiceProfile

AWS Config 規則：iotwireless-service-profile-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 an AWS IoT Wireless 服務描述檔是否具有具有參數中定義之特定金鑰的標籤requiredKeyTags。如果服務描述檔沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗requiredKeyTags。如果requiredKeyTags未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果服務設定檔未標記任何索引鍵，則會失敗。系統會aws:忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 an AWS IoT Wireless 服務設定檔，請參閱《AWS IoT Wireless 開發人員指南》中的[標記您的 AWS IoT Wireless 資源](#)。

【IoTWireless.3】AWS IoT FUOTA 任務應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IoTWireless::FuotaTask

AWS Config 規則：iotwireless-fuota-task-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 an AWS IoT Wireless 韌體over-the-air(FUOTA) 任務是否具有具有參數 中定義之特定金鑰的標籤requiredKeyTags。如果 FUOTA 任務沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredKeyTags。如果requiredKeyTags未提供 參數，則控制項只會檢查標籤金鑰是否存在，如果 FUOTA 任務未標記任何金鑰，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 an AWS IoT Wireless FUOTA 任務，請參閱《AWS IoT Wireless 開發人員指南》中的[標記您的 AWS IoT Wireless 資源](#)。

Amazon IVS 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Interactive Video Service (IVS) 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【IVS.1】 IVS 播放金鑰對應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IVS::PlaybackKeyPair

AWS Config 規則：ivs-playback-key-pair-tagged

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon IVS 播放金鑰對是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果播放金鑰對沒有任何標籤金鑰，或沒有參數中指定的所有金鑰，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤金鑰是否存在，如果播放金鑰對未標記任何金鑰，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 IVS 播放金鑰對，請參閱《Amazon IVS 即時串流 API 參考 [TagResource](#)》中的。

【IVS.2】 IVS 記錄組態應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IVS::RecordingConfiguration

AWS Config 規則：ivs-recording configuration-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon IVS 錄製組態是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果錄製組態沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果記錄組態未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 IVS 錄製組態，請參閱《Amazon IVS 即時串流 API 參考 [TagResource](#)》中的。

【IVS.3】 IVS 頻道應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::IVS::Channel

AWS Config 規則：ivs-channel-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon IVS 頻道是否具有具有參數中定義之特定金鑰的標籤 requiredKeyTags。如果頻道沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredKeyTags。如果 requiredKeyTags 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果頻道未標記任何索引鍵，則會失敗。系統會 aws: 忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的 [最佳實務和策略](#)。

修補

若要將標籤新增至 IVS 頻道，請參閱《Amazon IVS 即時串流 API 參考[TagResource](#)》中的。

Amazon Keyspaces 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Keyspaces 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Cassandra::Keyspace

AWS Config 規則：cassandra-keyspace-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon Keyspaces 金鑰空間是否具有具有參數中定義之特定金鑰的標籤requiredKeyTags。如果鍵空間沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗requiredKeyTags。如果requiredKeyTags未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果索引鍵空間未標記任何索引鍵，則會失敗。系統會aws:忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義

許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 Amazon Keyspaces 金鑰空間，請參閱《Amazon Keyspaces 開發人員指南》中的[將標籤新增至金鑰空間](#)。

Kinesis 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Kinesis 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Kinesis.1】 Kinesis 串流應靜態加密

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::Kinesis::Stream

AWS Config 規則：[kinesis-stream-encrypted](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Kinesis Data Streams 是否使用伺服器端加密進行靜態加密。如果 Kinesis 串流未使用伺服器端加密進行靜態加密，則此控制會失敗。

伺服器端加密是 Amazon Kinesis Data Streams 的一項功能，可在資料處於靜態狀態之前使用 自動加密資料 AWS KMS key。資料會在寫入 Kinesis 串流儲存層之前加密，並在從儲存體擷取資料後解密。因此，您的資料會在 Amazon Kinesis Data Streams 服務內進行靜態加密。

修補

如需有關為 Kinesis 串流啟用伺服器端加密的資訊，請參閱《Amazon Kinesis 開發人員指南》中的[如何開始使用伺服器端加密？](#)。

【Kinesis.2】 Kinesis 串流應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Kinesis::Stream

AWS Config rule：tagged-kinesis-stream (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon Kinesis 資料串流是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果資料串流沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果資料串流未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義

許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 AWS 服務，包括 AWS Billing，都可以存取標籤。如需更多標記最佳實務，請參閱《[標記您的 AWS 資源](#)》中的 [標記您的 AWS 資源](#) 一般參考。

修補

若要將標籤新增至 Kinesis 資料串流，請參閱《[Amazon Kinesis 開發人員指南](#)》中的在 [Amazon Kinesis Data Streams 中標記串流](#)。Amazon Kinesis

【Kinesis.3】 Kinesis 串流應具有足夠的資料保留期

嚴重性：中

資源類型：AWS::Kinesis::Stream

AWS Config規則：[kinesis-stream-backup-retention-check](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
minimumBackupRetentionPeriod	應保留資料的最小時數。	String	24 至 8760	168

此控制項會檢查 Amazon Kinesis 資料串流的資料保留期間是否大於或等於指定的時間範圍。如果資料保留期間小於指定的時間範圍，則控制項會失敗。除非您提供資料保留期間的自訂參數值，否則 Security Hub CSPM 會使用預設值 168 小時。

在 Kinesis Data Streams 中，資料串流是一系列排序的資料記錄，旨在即時寫入和讀取。資料記錄會暫時存放在串流中的碎片中。從新增記錄的時間期間，到記錄不再可供存取的時間稱為保留期間。Kinesis Data Streams 幾乎會在減少保留期間後，立即讓超過新保留期的記錄無法存取。例如，將保留期間從 24 小時變更為 48 小時，表示在 23 小時 55 分鐘之前新增到串流的記錄仍會在 24 小時後提供。

修補

若要變更 Kinesis Data Streams 的備份保留期，請參閱《Amazon Kinesis Data Streams 開發人員指南》中的[變更資料保留期](#)。

的 Security Hub CSPM 控制項 AWS KMS

這些 AWS Security Hub CSPM 控制項會評估 AWS Key Management Service (AWS KMS) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作

相關需求：NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::IAM::Policy

AWS Config 規則：[iam-customer-policy-blocked-kms-actions](#)

排程類型：已觸發變更

參數：

- blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt (不可自訂)
- excludePermissionBoundaryPolicy: True (不可自訂)

檢查 IAM 客戶受管政策的預設版本是否允許主體在所有資源上使用 AWS KMS 解密動作。如果政策開啟程度足以允許對所有 KMS 金鑰執行 kms:Decrypt 或 kms:ReEncryptFrom 動作，則控制項會失敗。

控制項只會檢查資源元素中的 KMS 金鑰，不會考慮政策條件元素中的任何條件。此外，控制項會評估已連接和未連接的客戶受管政策。它不會檢查內嵌政策或 AWS 受管政策。

透過 AWS KMS，您可以控制誰可以使用您的 KMS 金鑰，並存取您的加密資料。IAM 政策定義身分（使用者、群組或角色）可以對哪些資源執行哪些動作。遵循安全最佳實務，AWS 建議您允許最低權限。換句話說，您應該僅將 `kms:Decrypt` 或 `kms:ReEncryptFrom` 許可授予身分，並僅授予執行任務所需的金鑰。否則，使用者可能會使用不適合您資料的金鑰。

決定使用者存取加密資料所需的最低金鑰集，而不是授予所有金鑰的許可。然後設計僅允許使用者使用這些金鑰的政策。例如，不允許所有 KMS 金鑰的 `kms:Decrypt` 許可。反之，`kms:Decrypt` 只允許帳戶特定區域中的金鑰。透過採用最低權限原則，您可以降低意外揭露資料的風險。

修補

若要修改 IAM 客戶受管政策，請參閱《IAM 使用者指南》中的[編輯客戶受管政策](#)。編輯政策時，請針對 Resource 欄位提供您要允許解密動作之特定金鑰的 Amazon Resource Name (ARN)。

【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策

相關需求：NIST.800-53.r5 AC-2、NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(3)

類別：保護 > 安全存取管理

嚴重性：中

資源類型：

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

AWS Config 規則：[iam-inline-policy-blocked-kms-actions](#)

排程類型：已觸發變更

參數：

- `blockedActionsPatterns`: `kms:ReEncryptFrom`, `kms:Decrypt` (不可自訂)

此控制項會檢查內嵌在 IAM 身分（角色、使用者或群組）中的內嵌政策是否允許對所有 KMS 金鑰進行 AWS KMS 解密和重新加密動作。如果政策開啟程度足以允許對所有 KMS 金鑰執行 `kms:Decrypt` 或 `kms:ReEncryptFrom` 動作，則控制項會失敗。

控制項只會檢查資源元素中的 KMS 金鑰，不會考慮政策條件元素中的任何條件。

透過 AWS KMS，您可以控制誰可以使用您的 KMS 金鑰，並存取您的加密資料。IAM 政策定義身分（使用者、群組或角色）可以對哪些資源執行哪些動作。遵循安全最佳實務，AWS 建議您允許最低權限。換言之，您應該僅授予身分所需的許可，並僅授予執行任務所需的金鑰。否則，使用者可能會使用不適合您資料的金鑰。

決定使用者存取加密資料所需的金鑰集下限，而不是授予所有金鑰的許可。然後設計僅允許使用者使用這些金鑰的政策。例如，不允許所有 KMS 金鑰的 `kms:Decrypt` 許可。反之，請只對帳戶特定區域中的特定金鑰允許許可。透過採用最低權限原則，您可以降低意外揭露資料的風險。

修補

若要修改 IAM 內嵌政策，請參閱《IAM 使用者指南》中的[編輯內嵌政策](#)。編輯政策時，請針對 Resource 欄位提供您要允許解密動作之特定金鑰的 Amazon Resource Name (ARN)。

【KMS.3】AWS KMS keys 不應意外刪除

相關要求：NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-12(2)

類別：保護 > 資料保護 > 資料刪除保護

嚴重性：嚴重

資源類型：AWS::KMS::Key

AWS Config rule：kms-cmk-not-scheduled-for-deletion-2 (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已排定刪除 KMS 金鑰。如果排定刪除 KMS 金鑰，則控制項會失敗。

刪除後，無法復原 KMS 金鑰。如果刪除 KMS 金鑰，在 KMS 金鑰下加密的資料也會永久無法復原。如果有意義的資料已在排程刪除的 KMS 金鑰下加密，請考慮解密資料或在新的 KMS 金鑰下重新加密資料，除非您刻意執行密碼編譯清除。

當 KMS 金鑰排定刪除時，如果排程錯誤，則會強制執行強制等待期間，以允許時間反轉刪除。預設等待期間為 30 天，但在排定刪除 KMS 金鑰時，可以縮短為 7 天。在等待期間，排程刪除可以取消，而且不會刪除 KMS 金鑰。

如需有關刪除 KMS 金鑰的其他資訊，請參閱《AWS Key Management Service 開發人員指南》中的[刪除 KMS 金鑰](#)。

修補

若要取消排定的 KMS 金鑰刪除，請參閱《AWS Key Management Service 開發人員指南》中的在[排程和取消金鑰刪除（主控台）](#)下取消金鑰刪除。

【KMS.4】應啟用 AWS KMS 金鑰輪換

相關要求：CIS AWS Foundations Benchmark v5.0.0/3.6、CIS AWS Foundations Benchmark v3.0.0/3.6、CIS AWS Foundations Benchmark v1.4.0/3.8、CIS AWS Foundations Benchmark v1.2.0/2.8、NIST.800-53.r5 SC-12、NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 SC-28(3)、PCI DSS v3.2.1/3.6.4、PCI DSS v4.0.1/3.7.4

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::KMS::Key

AWS Config 規則：[cmk-backing-key-rotation-enabled](#)

排程類型：定期

參數：無

AWS KMS 可讓客戶輪換後端金鑰，這是存放在中的金鑰材料 AWS KMS，並與 KMS 金鑰的金鑰 ID 繫結。它是用來執行加密操作的備份金鑰，例如加密和解密。自動化輪換金鑰目前會保留之前所有的備份金鑰，以便透明解密加密的資料。

CIS 建議您啟用 KMS 金鑰輪換。輪換加密金鑰有助於降低被盜用金鑰造成的可能影響，因為可能公開的舊金鑰無法存取使用新金鑰加密的資料。

修補

若要啟用 KMS 金鑰輪換，請參閱《AWS Key Management Service 開發人員指南》中的[如何啟用和停用自動金鑰輪換](#)。

【KMS.5】不應公開存取 KMS 金鑰

類別：保護 > 安全網路組態 > 資源不可公開存取

嚴重性：嚴重

資源類型：AWS::KMS::Key

AWS Config 規則：[kms-key-policy-no-public-access](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 是否 AWS KMS key 可公開存取。如果 KMS 金鑰可公開存取，則控制項會失敗。

實作最低權限存取對於降低安全風險以及錯誤或惡意意圖的影響至關重要。如果的金鑰政策 AWS KMS key 允許從外部帳戶存取，第三方可能可以使用金鑰來加密和解密資料。這可能會導致來自使用金鑰 AWS 服務 之 的內部或外部威脅滲透資料。

Note

AWS KMS key 如果您的組態 AWS Config 無法在 KMS 金鑰的組態項目 (CI) 中記錄金鑰政策，則此控制項也會傳回 的問題 FAILED 清單。若要 AWS Config 讓 在 KMS 金鑰的 CI 中填入金鑰政策，[AWS Config 角色](#) 必須具有使用 [GetKeyPolicy](#) API 呼叫讀取金鑰政策的存取權。若要解決此類 FAILED 問題清單，請檢查可阻止 AWS Config 角色對 KMS 金鑰的金鑰政策具有讀取存取權的政策。例如，請檢查下列項目：

- KMS 金鑰的金鑰政策。
- 適用於您帳戶的 中的 [服務控制政策 \(SCPs\)](#) 和 [資源控制政策 RCPs](#)。AWS Organizations
- 如果您未使用 [AWS Config 服務連結](#) AWS Config 角色，則為角色的許可。

此外，此控制項不會評估使用萬用字元或變數的政策條件。若要產生 PASSED 調查結果，金鑰政策中的條件只能使用固定值，這些值不包含萬用字元或政策變數。如需政策變數的相關資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的 [變數和標籤](#)。

修補

如需更新 金鑰政策的相關資訊 AWS KMS key，請參閱《AWS Key Management Service 開發人員指南》中的 [金鑰政策 AWS KMS](#)。

的 Security Hub CSPM 控制項 AWS Lambda

這些 AWS Security Hub CSPM 控制項會評估 AWS Lambda 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Lambda.1】 Lambda 函數政策應禁止公開存取

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：AWS::Lambda::Function

AWS Config 規則：[lambda-function-public-access-prohibited](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Lambda 函數資源型政策是否禁止您帳戶外部的公開存取。如果允許公開存取，則控制項會失敗。如果從 Amazon S3 叫用 Lambda 函數，且政策不包含限制公開存取的條件，則控制項也會失敗，例如 AWS:SourceAccount。我們建議您在儲存貯體政策AWS:SourceAccount中使用其他 S3 條件以及，以獲得更精確的存取。

Note

此控制項不會評估使用萬用字元或變數的政策條件。若要產生PASSED調查結果，Lambda 函數政策中的條件只能使用固定值，這些值不包含萬用字元或政策變數。如需政策變數的相關資訊，請參閱AWS Identity and Access Management 《使用者指南》中的[變數和標籤](#)。

Lambda 函數不應公開存取，因為這可能會允許意外存取您的函數程式碼。

修補

若要修復此問題，您必須更新函數的資源型政策，以移除許可或新增AWS:SourceAccount條件。您只能從 Lambda API 或 更新資源型政策 AWS CLI。

若要開始，[請檢閱 Lambda 主控台上的資源型政策](#)。識別具有讓政策公開之Principal欄位值的政策陳述式，例如 "*"或 { "AWS": "*" }。

您無法從 主控台編輯政策。若要從 函數移除許可，請從 執行 [remove-permission](#)命令 AWS CLI。

```
$ aws lambda remove-permission --function-name <function-name> --statement-id <statement-id>
```

<function-name> 將 取代為 Lambda 函數的名稱，並將 <statement-id> 取代為您要移除之陳述式的陳述式 ID (Sid)。

【Lambda.2】 Lambda 函數應使用支援的執行時間

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/12.3.4

類別：保護 > 安全開發

嚴重性：中

資源類型：AWS::Lambda::Function

AWS Config 規則：[lambda-function-settings-check](#)

排程類型：變更已觸發

參數：

- runtime: dotnet10, dotnet8, java25, java21, java17, java11, java8.al2, nodejs24.x, nodejs22.x, python3.14, python3.13, python3.12, python3.11, python3.10, ruby4.0, ruby3.4, ruby3.3 (不可自訂)

此控制項會檢查 AWS Lambda 函數執行時間設定是否符合每種語言中支援執行時間設定的預期值。如果 Lambda 函數不使用支援的執行時間，則控制項會失敗，如參數一節所述。Security Hub CSPM 會忽略套件類型為 的函數Image。

Lambda 執行時間是以作業系統、程式設計語言和軟體程式庫的組合為基礎，這些程式庫會受到維護和安全性更新的影響。當安全性更新不再支援執行期元件時，Lambda 會棄用執行期。即使您無法建立使用已棄用執行時間的函數，該函數仍然可用於處理調用事件。我們建議確保您的 Lambda 函數是最新的，並且不使用已棄用的執行時間環境。如需支援的執行時間清單，請參閱《AWS Lambda 開發人員指南》中的 [Lambda 執行時間](#)。

修補

如需支援的執行期和棄用排程的詳細資訊，請參閱《AWS Lambda 開發人員指南》中的[執行期棄用政策](#)。當將執行時間遷移至最新版本時，請遵循語言發佈者提供的語法和指導。我們也建議套用[執行時間更新](#)，以協助降低在執行時間版本不相容的罕見情況下，對工作負載造成影響的風險。

【Lambda.3】 Lambda 函數應該位於 VPC 中

相關要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7

類別：保護 > 安全網路組態

嚴重性：低

資源類型：AWS::Lambda::Function

AWS Config 規則：[lambda-inside-vpc](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Lambda 函數是否部署在虛擬私有雲端 (VPC) 中。如果未在 VPC 中部署 Lambda 函數，則控制項會失敗。Security Hub CSPM 不會評估 VPC 子網路路由組態來判斷公有連線能力。您可能會看到 Lambda@Edge 資源的失敗問題清單。

在 VPC 中部署資源可增強安全性並控制網路組態。這類部署也提供跨多個可用區域的可擴展性和高容錯能力。您可以自訂 VPC 部署以滿足各種應用程式需求。

修補

若要將現有函數設定為連接到 VPC 中的私有子網路，請參閱《AWS Lambda 開發人員指南》中的[設定 VPC 存取](#)。我們建議您為高可用性選擇至少兩個私有子網路，以及至少有一個符合函數連線需求的安全群組。

【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::Lambda::Function

AWS Config 規則：[lambda-vpc-multi-az-check](#)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
availabilityZones	可用區域數目下限	列舉	2, 3, 4, 5, 6	2

此控制項會檢查連線至虛擬私有雲端 (VPC) 的 AWS Lambda 函數是否至少在指定數量的可用區域 (AZs) 中運作。如果函數未在至少指定數量 AZs 中操作，則控制項會失敗。除非您提供最低 AZs 數量的自訂參數值，否則 Security Hub CSPM 會使用兩個 AZs 的預設值。

在多個 AZs 部署資源是 AWS 最佳實務，可確保架構內的高可用性。可用性是機密性、完整性和可用性三要素安全模型的核心支柱。連接到 VPC 的所有 Lambda 函數都應有多可用區域部署，以確保單一故障區域不會造成操作的完全中斷。

修補

如果您將函數設定為連接到帳戶中的 VPC，請在多個 AZs 指定子網路，以確保高可用性。如需說明，請參閱《AWS Lambda 開發人員指南》中的[設定 VPC 存取](#)。

Lambda 會自動在多個 AZs 執行其他函數，以確保在單一區域中發生服務中斷時，它可用於處理事件。

【Lambda.6】應標記 Lambda 函數

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Lambda::Function

AWS Config rule：tagged-lambda-function (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS Lambda 函數是否具有具有參數中定義之特定索引鍵的標籤 `requiredTagKeys`。如果函數沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果函數未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Lambda 函數，請參閱《AWS Lambda 開發人員指南》中的 [在 Lambda 函數上使用標籤](#)。

【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤

相關需求：NIST.800-53.r5 CA-7

類別：識別 > 記錄日誌

嚴重性：低

資源類型：AWS::Lambda::Function

AWS Config 規則：[lambda-function-xray-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS X-Ray 函數是否已啟用使用的 AWS Lambda 主動追蹤。如果停用 Lambda 函數的 X-Ray 主動追蹤，則控制項會失敗。

AWS X-Ray 可以為 AWS Lambda 函數提供追蹤和監控功能，可節省時間和精力偵錯和操作 Lambda 函數。它可以透過分解 Lambda 函數的延遲，協助您診斷錯誤並識別效能瓶頸、速度變慢和逾時。它也可以協助處理資料隱私權和合規要求。如果您啟用 Lambda 函數的主動追蹤，X-Ray 會提供 Lambda 函數內資料流程和處理的整體檢視，這可協助您識別潛在的安全漏洞或不合規的資料處理實務。此可見性可協助您維護資料完整性、機密性和符合相關法規。

Note

AWS X-Ray 使用 Amazon Managed Streaming for Apache Kafka (Amazon MSK)、自我管理 Apache Kafka、使用 ActiveMQ 和 RabbitMQ 的 Amazon MQ 或 Amazon DocumentDB 事件來源映射的 Lambda 函數目前不支援追蹤。

修補

如需為 AWS Lambda 函數啟用主動追蹤的詳細資訊，請參閱《AWS Lambda 開發人員指南》中的[使用視覺化 Lambda 函數叫用 AWS X-Ray](#)。

Macie 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Macie 服務。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Macie.1】應啟用 Amazon Macie

相關需求：NIST.800-53.r5 CA-7、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 RA-5、NIST.800-53.r5 SA-8(19)、NIST.800-53.r5 SI-4

類別：偵測 > 偵測服務

嚴重性：中

資源類型：AWS:::Account

AWS Config 規則：[macie-status-check](#)

排程類型：定期

此控制項會檢查帳戶是否已啟用 Amazon Macie。如果未為帳戶啟用 Macie，則控制項會失敗。

Amazon Macie 使用機器學習和模式比對來探索敏感資料，提供資料安全風險的可見性，並實現對這些風險的自動化保護。Macie 會自動並持續評估 Amazon Simple Storage Service (Amazon S3) 儲存貯體的安全性和存取控制，並產生調查結果，以通知您 Amazon S3 資料的安全性或隱私權潛在問題。Macie 也會自動化敏感資料的探索和報告，例如個人身分識別資訊 (PII)，讓您更深入了解存放在 Amazon S3 中的資料。若要進一步了解，請參閱 [Amazon Macie 使用者指南](#)。

修補

若要啟用 Macie，請參閱《Amazon [Macie 使用者指南](#)》中的[啟用 Macie](#)。Amazon Macie

【Macie.2】應啟用 Macie 自動化敏感資料探索

相關需求：NIST.800-53.r5 CA-7、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 RA-5、NIST.800-53.r5 SA-8(19)、NIST.800-53.r5 SI-4

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS:::Account

AWS Config 規則：[macie-auto-sensitive-data-discovery-check](#)

排程類型：定期

此控制項會檢查 Amazon Macie 管理員帳戶是否已啟用自動敏感資料探索。如果 Macie 管理員帳戶未啟用自動敏感資料探索，則控制項會失敗。此控制項僅適用於管理員帳戶。

Macie 會自動探索和報告 Amazon Simple Storage Service (Amazon S3) 儲存貯體中的敏感資料，例如個人身分識別資訊 (PII)。透過自動化敏感資料探索，Macie 會持續評估您的儲存貯體庫存，並使用抽樣技術來識別和選取儲存貯體中的代表性 S3 物件。Macie 接著會分析選取的物件，並檢查它們是否有敏感資料。隨著分析的進行，Macie 會更新統計資料、庫存資料，以及它提供的 S3 資料其他資訊。Macie 也會產生調查結果，以報告找到的敏感資料。

修補

若要建立和設定自動敏感資料探索任務以分析 S3 儲存貯體中的物件，請參閱《Amazon Macie 使用者指南》中的[為您的帳戶設定自動敏感資料探索](#)。

Amazon MSK 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Managed Streaming for Apache Kafka (Amazon MSK) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密

相關要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、PCI DSS v4.0.1/4.2.1

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::MSK::Cluster

AWS Config 規則：[msk-in-cluster-node-require-tls](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon MSK 叢集是否在叢集的代理程式節點之間使用 HTTPS (TLS) 傳輸中加密。如果啟用叢集代理程式節點連線的純文字通訊，則控制項會失敗。

HTTPS 提供額外的安全層，因為它使用 TLS 來移動資料，可用於防止潛在攻擊者使用 person-in-the-middle 或類似攻擊來竊聽或操作網路流量。根據預設，Amazon MSK 會使用 TLS 加密傳輸中的資料。不過，您可以在建立叢集時覆寫此預設值。我們建議透過 HTTPS (TLS) 為代理程式節點連線使用加密連線。

修補

如需有關更新 Amazon MSK 叢集加密設定的資訊，請參閱《Amazon Managed Streaming for Apache Kafka 開發人員指南》中的[更新叢集的安全性設定](#)。

【MSK.2】 MSK 叢集應已設定增強型監控

相關要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

類別：偵測 > 偵測服務

嚴重性：低

資源類型：AWS::MSK::Cluster

AWS Config 規則：[msk-enhanced-monitoring-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon MSK 叢集是否已設定增強型監控，由至少 的監控層級指定 PER_TOPIC_PER_BROKER。如果叢集的監控層級設定為 DEFAULT 或 ，則控制項會失敗 PER_BROKER。

PER_TOPIC_PER_BROKER 監控層級提供更精細的 MSK 叢集效能洞察，也提供與資源使用率相關的指標，例如 CPU 和記憶體使用量。這可協助您識別個別主題和代理程式的效能瓶頸和資源使用率模式。此可見性可最佳化 Kafka 代理程式的效能。

修補

若要設定 MSK 叢集的增強型監控，請完成下列步驟：

1. 開啟 Amazon MSK 主控台，網址為 <https://console.aws.amazon.com/msk/home?region=us-east-1#/home/>。
2. 在導覽窗格中，選擇叢集。然後，選擇叢集。
3. 針對動作，選取編輯監控。
4. 選取增強型主題層級監控的選項。
5. 選擇儲存變更。

如需監控層級的詳細資訊，請參閱 [《Amazon Managed Streaming for Apache Kafka 開發人員指南》](#) 中的使用 CloudWatch 監控標準代理程式的 Amazon MSK 指標。

【MSK.3】 MSK Connect 連接器應在傳輸中加密

相關要求：PCI DSS v4.0.1/4.2.1

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::KafkaConnect::Connector

AWS Config rule：msk-connect-connector-encrypted (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon MSK Connect 連接器是否在傳輸中加密。如果連接器未在傳輸中加密，則此控制項會失敗。

傳輸中的資料是指從一個位置移動到另一個位置的資料，例如叢集中的節點之間，或叢集與您的應用程式之間。資料可能會在網際網路或私有網路中移動。加密傳輸中的資料可降低未經授權的使用者可以竊聽網路流量的風險。

修補

您可以在建立 MSK Connect 連接器時啟用傳輸中加密。您無法在建立連接器後變更加密設定。如需詳細資訊，請參閱《Amazon Managed Streaming for Apache Kafka 開發人員指南》中的[建立連接器](#)。

【MSK.4】MSK 叢集應停用公有存取

類別：保護 > 安全存取管理 > 資源不可公開存取

嚴重性：嚴重

資源類型：AWS::MSK::Cluster

AWS Config 規則：[msk-cluster-public-access-disabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon MSK 叢集的公有存取是否已停用。如果 MSK 叢集已啟用公有存取，則控制項會失敗。

根據預設，用戶端只有在與叢集位於相同的 VPC 中時，才能存取 Amazon MSK 叢集。根據預設，Kafka 用戶端和 MSK 叢集之間的所有通訊都是私有的，串流資料不會周遊網際網路。不過，如果

MSK 叢集設定為允許公開存取，則網際網路上的任何人都可以與叢集內執行的 Apache Kafka 代理程式建立連線。這可能會導致未經授權的存取、資料外洩或漏洞利用等問題。如果您要求身分驗證和授權措施來限制對叢集的存取，您可以協助保護敏感資訊和維護資源的完整性。

修補

如需管理 Amazon MSK 叢集公有存取權的資訊，請參閱《Amazon Managed Streaming for Apache Kafka 開發人員指南》中的[開啟 MSK 佈建叢集的公有存取權](#)。

【MSK.5】 MSK 連接器應該已啟用記錄

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::KafkaConnect::Connector

AWS Config 規則：[msk-connect-connector-logging-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已為 Amazon MSK 連接器啟用記錄。如果停用 MSK 連接器的記錄，則控制項會失敗。

Amazon MSK 連接器透過持續將串流資料從資料來源複製到 Apache Kafka 叢集，或持續將資料從叢集複製到資料接收器，來整合外部系統和 Amazon 服務與 Apache Kafka。MSK Connect 可以撰寫日誌事件，以協助偵錯連接器。當您建立連接器時，您可以指定下列零個或多個日誌目的地：Amazon CloudWatch Logs、Amazon S3 和 Amazon Data Firehose。

Note

如果外掛程式未將這些值定義為秘密，則敏感組態值可能會顯示在連接器日誌中。Kafka Connect 會將未定義的組態值視為與任何其他純文字值相同。

修補

若要啟用現有 Amazon MSK 連接器的記錄，您必須使用適當的記錄組態重新建立連接器。如需組態選項的詳細資訊，請參閱《Amazon Managed Streaming for Apache Kafka 開發人員指南》中的[MSK Connect 記錄](#)。

【MSK.6】 MSK 叢集應停用未驗證的存取

類別：保護 > 安全存取管理 > 無密碼身分驗證

嚴重性：中

資源類型：AWS::MSK::Cluster

AWS Config 規則：[msk-unrestricted-access-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已啟用 Amazon MSK 叢集的未驗證存取。如果 MSK 叢集已啟用未經驗證的存取，則控制項會失敗。

Amazon MSK 支援用戶端身分驗證和授權機制，以控制對叢集的存取。這些機制會驗證連線至叢集之用戶端的身分，並判斷用戶端可執行的動作。MSK 叢集可以設定為允許未經驗證的存取，這允許具有網路連線的任何用戶端發佈和訂閱 Kafka 主題，而無需提供登入資料。在不要求身分驗證的情況下執行 MSK 叢集會違反最低權限原則，而且可能會讓叢集暴露在未經授權的存取中。它可以允許任何用戶端存取、修改或刪除 Kafka 主題中的資料，這可能會導致資料外洩、未經授權的資料修改或服務中斷。我們建議啟用身分驗證機制，例如 IAM 身分驗證、SASL/SCRAM 或交互 TLS，以確保適當的存取控制和維護安全合規。

修補

如需有關變更 Amazon MSK 叢集身分驗證設定的資訊，請參閱《Amazon Managed Streaming for Apache Kafka 開發人員指南》中的下列章節：[更新 Amazon MSK 叢集的安全性設定](#)，以及[Apache Kafka APIs 的身分驗證和授權](#)。

Amazon MQ 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon MQ 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch

相關要求：NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-12、NIST.800-53.r5 SI-4、PCI DSS v4.0.1/10.3.3

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::AmazonMQ::Broker

AWS Config 規則：[mq-cloudwatch-audit-log-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon MQ ActiveMQ 代理程式是否將稽核日誌串流至 Amazon CloudWatch Logs。如果代理程式未將稽核日誌串流至 CloudWatch Logs，則控制項會失敗。

透過將 ActiveMQ 代理程式日誌發佈至 CloudWatch Logs，您可以建立 CloudWatch 警示和指標，以提高安全相關資訊的可見性。

修補

若要將 ActiveMQ 代理程式日誌串流至 CloudWatch Logs，請參閱《[Amazon MQ 開發人員指南](#)》中的[設定 Amazon MQ for ActiveMQ 日誌](#)。Amazon MQ

【MQ.3】 Amazon MQ 代理程式應該啟用自動次要版本升級

 Important

Security Hub CSPM 已於 2026 年 1 月淘汰此控制項。如需詳細資訊，請參閱[Security Hub CSPM 控制項的變更日誌](#)。

相關要求：NIST.800-53.r5 CM-3、NIST.800-53.r5 SI-2、PCI DSS v4.0.1/6.3.3

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：AWS::AmazonMQ::Broker

AWS Config 規則：[mq-auto-minor-version-upgrade-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon MQ 代理程式是否已啟用自動次要版本升級。如果代理程式未啟用自動次要版本升級，則控制項會失敗。

隨著 Amazon MQ 發行並支援新的代理程式引擎版本，變更會與現有的應用程式回溯相容，而不會取代現有的功能。自動代理程式引擎版本更新可保護您免於安全風險、協助修正錯誤並改善功能。

Note

當與自動次要版本升級相關聯的代理程式在其最新的修補程式上且變得不受支援時，您必須採取手動動作進行升級。

修補

若要啟用 MQ 代理程式的自動次要版本升級，請參閱《Amazon MQ 開發人員指南》中的[自動升級次要引擎版本](#)。

【MQ.4】 Amazon MQ 代理程式應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::AmazonMQ::Broker

AWS Config rule：tagged-amazonmq-broker (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon MQ 代理程式是否具有具有參數 中定義之特定金鑰的標籤 `requiredTagKeys`。如果代理程式沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果代理程式未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Amazon MQ 代理程式，請參閱《Amazon MQ 開發人員指南》中的 [標記資源](#)。

【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：低

資源類型：AWS::AmazonMQ::Broker

AWS Config 規則：[mq-active-deployment-mode](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon MQ ActiveMQ 代理程式的部署模式是否設定為作用中/待命。如果單一執行個體代理程式（預設為啟用）設定為部署模式，則控制項會失敗。

作用中/待命部署可為 中的 Amazon MQ ActiveMQ 代理程式提供高可用性 AWS 區域。作用中/待命部署模式包括在兩個不同可用區域中的兩個代理程式執行個體，以備援對設定。這些代理程式會與您的應用程式同步通訊，以減少發生故障時的停機時間和資料遺失。

修補

若要使用作用中/待命部署模式建立新的 ActiveMQ 代理程式，請參閱《Amazon MQ 開發人員指南》中的[建立和設定 ActiveMQ 代理程式](#)。Amazon MQ 針對部署模式，選擇作用中/待命代理程式。您無法變更現有代理程式的部署模式。相反地，您必須建立新的代理程式，並從舊代理程式複製設定。

【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：低

資源類型：AWS::AmazonMQ::Broker

AWS Config 規則：[mq-rabbit-deployment-mode](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon MQ RabbitMQ 代理程式的部署模式是否設定為叢集部署。如果單一執行個體代理程式（預設為啟用）設定為部署模式，則控制項會失敗。

叢集部署可為 中的 Amazon MQ RabbitMQ 代理程式提供高可用性 AWS 區域。叢集部署是三個 RabbitMQ 代理程式節點的邏輯分組，每個節點都有自己的 Amazon Elastic Block Store (Amazon EBS) 磁碟區和共用狀態。叢集部署可確保資料複製到叢集中的所有節點，這可減少發生故障時的停機時間和資料遺失。

修補

若要使用叢集部署模式建立新的 RabbitMQ 代理程式，請參閱《Amazon MQ 開發人員指南》中的[建立並連線至 RabbitMQ 代理程式](#)。Amazon MQ 針對部署模式，選擇叢集部署。您無法變更現有代理程式的部署模式。相反地，您必須建立新的代理程式，並從舊代理程式複製設定。

Neptune 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Neptune 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Neptune.1】 Neptune 資料庫叢集應靜態加密

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[neptune-cluster-encrypted](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune 資料庫叢集是否靜態加密。如果 Neptune 資料庫叢集未靜態加密，則控制項會失敗。

靜態資料是指在任何期間內存放在持久性、非揮發性儲存體中的任何資料。加密可協助您保護此類資料的機密性，降低未經授權的使用者可存取資料的風險。加密 Neptune 資料庫叢集可保護您的資料和中繼資料免於未經授權的存取。它還滿足生產檔案系統data-at-rest加密的合規要求。

修補

您可以在建立 Neptune 資料庫叢集時啟用靜態加密。您無法在建立叢集後變更加密設定。如需詳細資訊，請參閱《[Neptune 使用者指南](#)》中的[加密靜態 Neptune 資源](#)。

【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs

相關要求：NIST.800-53.r5 AC-2(4)，NIST.800-53.r5 AC-4(26)，NIST.800-53.r5 AC-6(9)，NIST.800-53.r5 AU-10，NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(1)，NIST.800-53.r5 AU-6(3)，NIST.800-53.r5 AU-6(4)，NIST.800-53.r5

AU-6(5) , NIST.800-53.r5 AU-7(1) , NIST.800-53.r5 AU-9(7) , NIST.800-53.r5 CA-7、
NIST.800-53.r5 SC-7(9) , NIST.800-53.r5 SI-20、 NIST.800-53.r5 SI-3(8) , NIST.800-53.r5
SI-4(20) , NIST.800-53.r5 SI-4(5) , NIST.800-53.r5 SI-7(8) , PCI DSS 4.0.1/10.3.3 版

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[neptune-cluster-cloudwatch-log-export-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune 資料庫叢集是否將稽核日誌發佈至 Amazon CloudWatch Logs。
如果 Neptune 資料庫叢集未將稽核日誌發佈至 CloudWatch Logs，則控制項會失敗。
EnableCloudWatchLogsExport 應該設定為 Audit。

Amazon Neptune 與 Amazon CloudWatch 整合，以便您可以收集並分析效能指標。Neptune 會自動將指標傳送至 CloudWatch，也支援 CloudWatch 警示。稽核日誌可高度自訂。當您稽核資料庫時，可以監控資料上的每個操作並將其記錄到稽核追蹤，包括有關存取哪些資料庫叢集以及如何存取的資訊。建議您將這些日誌傳送至 CloudWatch，以協助您監控 Neptune 資料庫叢集。

修補

若要將 Neptune 稽核日誌發佈至 CloudWatch Logs，請參閱 [《Neptune 使用者指南》中的將 Neptune 日誌發佈至 Amazon CloudWatch Logs](#)。在日誌匯出區段中，選擇稽核。

【Neptune.3】 Neptune 資料庫叢集快照不應公開

相關需求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-75
NIST.800-53.r5 SC-7)

類別：保護 > 安全網路組態 > 不可公開存取的資源

嚴重性：嚴重

資源類型：AWS::RDS::DBClusterSnapshot

AWS Config 規則：[neptune-cluster-snapshot-public-prohibited](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune 手動資料庫叢集快照是否為公有。如果 Neptune 手動資料庫叢集快照為公有，則控制項會失敗。

除非預期，否則 Neptune 資料庫叢集手動快照不應公開。如果您將未加密的手動快照共用為公有，則快照可供所有使用 AWS 帳戶。公有快照可能會導致意外的資料暴露。

修補

若要移除 Neptune 手動資料庫叢集快照的公有存取權，請參閱 [Neptune 使用者指南中的共用資料庫叢集快照](#)。

【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

類別：保護 > 資料保護 > 資料刪除保護

嚴重性：低

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[neptune-cluster-deletion-protection-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune 資料庫叢集是否已啟用刪除保護。如果 Neptune 資料庫叢集未啟用刪除保護，則控制項會失敗。

啟用叢集刪除保護可提供額外的保護層，防止未經授權的使用者意外刪除或刪除資料庫。啟用刪除保護時，無法刪除 Neptune 資料庫叢集。您必須先停用刪除保護，刪除請求才能成功。

修補

若要啟用現有 Neptune 資料庫叢集的刪除保護，請參閱《Amazon Aurora 使用者指南》中的[使用主控台、CLI 和 API 修改資料庫叢集](#)。

【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份

相關要求：NIST.800-53.r5 SI-12

類別：復原 > 恢復 > 備份已啟用

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[neptune-cluster-backup-retention-check](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
minimumBackupRetentionPeriod	最短備份保留期間，以天為單位	Integer	7 至 35	7

此控制項會檢查 Neptune 資料庫叢集是否已啟用自動備份，以及大於或等於指定時間範圍的備份保留期間。如果未為 Neptune 資料庫叢集啟用備份，或保留期間小於指定的時間範圍，則控制項會失敗。除非您提供備份保留期間的自訂參數值，否則 Security Hub CSPM 會使用預設值 7 天。

備份可協助您更快速地從安全事件中復原，並強化系統的彈性。透過自動化 Neptune 資料庫叢集的備份，您可以將系統還原到某個時間點，並將停機時間和資料遺失降至最低。

修補

若要啟用自動備份並設定 Neptune 資料庫叢集的備份保留期，請參閱《Amazon RDS 使用者指南》中的[啟用自動備份](#)。針對備份保留期間，選擇大於或等於 7 的值。

【Neptune.6】 Neptune 資料庫叢集快照應靜態加密

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(18)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::RDS::DBClusterSnapshot

AWS Config 規則：[neptune-cluster-snapshot-encrypted](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune 資料庫叢集快照是否靜態加密。如果 Neptune 資料庫叢集未靜態加密，則控制項會失敗。

靜態資料是指在任何期間內存放在持久性、非揮發性儲存體中的任何資料。加密可協助您保護此類資料的機密性，降低未經授權的使用者存取資料的風險。Neptune 資料庫叢集快照中的資料應靜態加密，以增加一層安全性。

修補

您無法加密現有的 Neptune 資料庫叢集快照。反之，您必須將快照還原至新的資料庫叢集，並在叢集上啟用加密。您可以從加密叢集建立加密快照。如需說明，請參閱《Neptune 使用者指南》中的[從資料庫叢集快照還原](#)和在 Neptune 中建立資料庫叢集快照。<https://docs.aws.amazon.com/neptune/latest/userguide/backup-restore-create-snapshot.html>

【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

類別：保護 > 安全存取管理 > 無密碼身分驗證

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[neptune-cluster-iam-database-authentication](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Neptune 資料庫叢集是否已啟用 IAM 資料庫身分驗證。如果未針對 Neptune 資料庫叢集啟用 IAM 資料庫身分驗證，則控制項會失敗。

Amazon Neptune 資料庫叢集的 IAM 資料庫身分驗證不需要將使用者登入資料存放在資料庫組態中，因為身分驗證是使用 IAM 進行外部管理。啟用 IAM 資料庫身分驗證時，每個請求都需要使用 AWS Signature 第 4 版進行簽署。

修補

根據預設，IAM 資料庫身分驗證會在您建立 Neptune 資料庫叢集時停用。若要啟用它，請參閱 [《Neptune 使用者指南》中的在 Neptune 中啟用 IAM 資料庫身分驗證](#)。

【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[neptune-cluster-copy-tags-to-snapshot-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Neptune 資料庫叢集是否設定為在建立快照時將所有標籤複製到快照。如果 Neptune 資料庫叢集未設定為將標籤複製到快照，則控制項會失敗。

識別和清查您的 IT 資產是控管和安全性的重要層面。您應該以與其父 Amazon RDS 資料庫叢集相同的方式標記快照。複製標籤可確保資料庫快照的中繼資料符合父資料庫叢集的中繼資料，而且資料庫快照的存取政策也符合父資料庫執行個體的中繼資料。

修補

若要將標籤複製到 Neptune 資料庫叢集的快照，請參閱 [《Neptune 使用者指南》中的在 Neptune 中複製標籤](#)。

【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[neptune-cluster-multi-az-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon Neptune 資料庫叢集在多個可用區域 (AZs) 中是否有僅供讀取複本執行個體。如果叢集僅部署在一個 AZ 中，則控制項會失敗。

如果 AZ 無法使用，且在定期維護事件期間，僅供讀取複本會做為主要執行個體的容錯移轉目標。亦即，如果主要執行個體失敗，則 Neptune 會提升僅供讀取複本以成為主要執行個體。相反地，如果您的資料庫叢集不包含任何僅供讀取複本執行個體，則當主要執行個體失敗時，資料庫叢集仍無法使用，直到重新建立為止。重新建立主要執行個體所花費的時間比提升僅供讀取複本要長得多。為了確保高可用性，我們建議您建立一或多個僅供讀取複本執行個體，其資料庫執行個體類別與主要執行個體相同，且位於與主要執行個體不同的 AZs 中。

修補

若要在多個 AZs 中部署 Neptune 資料庫叢集，請參閱《Neptune 使用者指南》[中的 Neptune 資料庫叢集中的僅供讀取複本資料庫執行個體](#)。

的 Security Hub CSPM 控制項 AWS Network Firewall

這些 AWS Security Hub CSPM 控制項會評估 AWS Network Firewall 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【NetworkFirewall.1】 網路防火牆防火牆應部署在多個可用區域

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::NetworkFirewall::Firewall

AWS Config 規則：[netfw-multi-az-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會評估透過 AWS Network Firewall 管理的防火牆是否跨多個可用區域 (AZs) 部署。如果防火牆僅部署在一個可用區域中，則控制項會失敗。

AWS 全球基礎設施包含多個 AWS 區域。AZs 區域是每個區域內以低延遲、高輸送量和高備援聯網連接的實際隔離位置。透過在多個可用 AZs 部署 Network Firewall 防火牆，您可以在 AZs 之間平衡和轉移流量，這可協助您設計高可用性的解決方案。

修補

在多個 AZs 部署 Network Firewall 防火牆

1. 在 <https://console.aws.amazon.com/vpc/> 開啟 Amazon VPC 主控台。
2. 在導覽窗格的網路防火牆下，選擇防火牆。
3. 在防火牆頁面上，選取要編輯的防火牆。
4. 在防火牆詳細資訊頁面上，選擇防火牆詳細資訊索引標籤。
5. 在關聯的政策和 VPC 區段中，選擇編輯
6. 若要新增可用區域，請選擇新增子網路。選取您要使用的 AZ 和子網路。請確定您至少選取兩個 AZs。
7. 選擇儲存。

【NetworkFirewall.2】應啟用網路防火牆記錄

相關要求：NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.8000-5.r5)、AU-6NIST.5 AU-9 CA-7 NIST.800-53.r5 SC-7 SI-3 SI-4 SI-7 3.1.20

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::NetworkFirewall::LoggingConfiguration

AWS Config 規則：[netfw-logging-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否已為 AWS Network Firewall 防火牆啟用記錄。如果未針對至少一個日誌類型啟用記錄，或記錄目的地不存在，則控制項會失敗。

記錄可協助您維護防火牆的可靠性、可用性和效能。在 Network Firewall 中，記錄可提供網路流量的詳細資訊，包括具狀態引擎收到封包流程的時間、封包流程的詳細資訊，以及針對封包流程採取的任何具狀態規則動作。

修補

若要啟用防火牆的記錄，請參閱《AWS Network Firewall 開發人員指南》中的[更新防火牆的記錄組態](#)。

【NetworkFirewall.3】網路防火牆政策應至少有一個相關聯的規則群組

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-171.r2 3.1.3、NIST.800-171.r2 3.13.1

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::NetworkFirewall::FirewallPolicy

AWS Config 規則：[netfw-policy-rule-group-associated](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Network Firewall 政策是否有任何相關聯的具狀態或無狀態規則群組。如果未指派無狀態或有狀態規則群組，則控制項會失敗。

防火牆政策會定義防火牆如何監控和處理 Amazon Virtual Private Cloud (Amazon VPC) 中的流量。無狀態和有狀態規則群組的組態有助於篩選封包和流量流程，並定義預設流量處理。

修補

若要將規則群組新增至網路防火牆政策，請參閱《AWS Network Firewall 開發人員指南》中的[更新防火牆政策](#)。如需建立和管理規則群組的資訊，請參閱 [中的規則群組 AWS Network Firewall](#)。

【NetworkFirewall.4】Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::NetworkFirewall::FirewallPolicy

AWS Config 規則：[netfw-policy-default-action-full-packets](#)

排程類型：已觸發變更

參數：

- statelessDefaultActions: aws:drop,aws:forward_to_sfe (不可自訂)

此控制項會檢查網路防火牆政策完整封包的預設無狀態動作是捨棄還是轉送。如果選取 Drop 或 Forward，則控制項會通過，如果選取 Pass，則會失敗。

防火牆政策會定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包和流量。預設為 Pass 可允許意外流量。

修補

若要變更防火牆政策，請參閱《AWS Network Firewall 開發人員指南》中的[更新防火牆政策](#)。針對無狀態預設動作，選擇編輯。然後，選擇捨棄或轉送至具狀態規則群組作為動作。

【NetworkFirewall.5】網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-171.r2 3.1.3、NIST.800-171.r2 3.1.14、NIST.800-171.r2 3.13.1、NIST.800-171.r2 3.13.6

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::NetworkFirewall::FirewallPolicy

AWS Config 規則：[netfw-policy-default-action-fragment-packets](#)

排程類型：已觸發變更

參數：

- statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe (不可自訂)

此控制項會檢查網路防火牆政策片段封包的預設無狀態動作是捨棄還是轉送。如果選取 Drop 或 Forward，則控制項會通過，如果選取 Pass，則會失敗。

防火牆政策會定義防火牆如何監控和處理 Amazon VPC 中的流量。您可以設定無狀態和有狀態規則群組來篩選封包和流量。預設為 Pass 可允許意外流量。

修補

若要變更防火牆政策，請參閱《AWS Network Firewall 開發人員指南》中的[更新防火牆政策](#)。針對無狀態預設動作，選擇編輯。然後，選擇捨棄或轉送至具狀態規則群組作為動作。

【NetworkFirewall.6】無狀態網路防火牆規則群組不應為空

相關需求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(5)、NIST.800-171.r2 3.1.3、NIST.800-171.r2 3.1.14、NIST.800-171.r2 3.13.1

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::NetworkFirewall::RuleGroup

AWS Config 規則：[netfw-stateless-rule-group-not-empty](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 中的無狀態規則群組是否 AWS Network Firewall 包含規則。如果規則群組中沒有規則，則控制項會失敗。

規則群組包含定義防火牆如何處理 VPC 中流量的規則。當防火牆政策中有空的無狀態規則群組時，可能會給人留下規則群組將處理流量的印象。不過，當無狀態規則群組為空時，不會處理流量。

修補

若要將規則新增至 Network Firewall 規則群組，請參閱《AWS Network Firewall 開發人員指南》中的[更新具狀態規則群組](#)。在防火牆詳細資訊頁面上，針對無狀態規則群組，選擇編輯以新增規則。

【NetworkFirewall.7】應標記網路防火牆

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::NetworkFirewall::Firewall

AWS Config rule：tagged-networkfirewall-firewall (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1-6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS Network Firewall 防火牆是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果防火牆沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤金鑰是否存在，如果防火牆未標記任何金鑰，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義

許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 AWS 服務，包括 AWS Billing，都可以存取標籤。如需更多標記最佳實務，請參閱《[標記您的 AWS 資源](#)》中的 AWS 一般參考。

修補

若要將標籤新增至 Network Firewall 防火牆，請參閱《AWS Network Firewall 開發人員指南》中的[標記 AWS Network Firewall 資源](#)。

【NetworkFirewall.8】應標記網路防火牆防火牆政策

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::NetworkFirewall::FirewallPolicy

AWS Config rule：tagged-networkfirewall-firewallpolicy（自訂 Security Hub CSPM 規則）

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS Network Firewall 防火牆政策是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果防火牆政策沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則

控制項會失敗 `requiredTagKeys`。如果 `requiredTagKeys` 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果防火牆政策未標記任何索引鍵，則 會失敗。系統會 `aws:` 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Network Firewall 政策，請參閱《AWS Network Firewall 開發人員指南》中的[標記 AWS Network Firewall 資源](#)。

【NetworkFirewall.9】網路防火牆防火牆應啟用刪除保護

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

類別：保護 > 網路安全

嚴重性：中

資源類型：AWS::NetworkFirewall::Firewall

AWS Config 規則：[netfw-deletion-protection-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 AWS Network Firewall 防火牆是否已啟用刪除保護。如果防火牆未啟用刪除保護，則控制項會失敗。

AWS Network Firewall 是一種具狀態的受管網路防火牆和入侵偵測服務，可讓您檢查和篩選進出虛擬私有雲端 (VPCs) 的流量。刪除保護設定可防止意外刪除防火牆。

修補

若要在現有的 Network Firewall 防火牆上啟用刪除保護，請參閱《AWS Network Firewall 開發人員指南》中的[更新防火牆](#)。針對變更保護，選取啟用。您也可以叫用 [UpdateFirewallDeleteProtection](#) API 並將 DeleteProtection 欄位設定為 `true`，以啟用刪除保護。

【NetworkFirewall.10】網路防火牆防火牆應啟用子網路變更保護

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

類別：保護 > 網路安全

嚴重性：中

資源類型：AWS::NetworkFirewall::Firewall

AWS Config 規則：[netfw-subnet-change-protection-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已啟用防火牆的 AWS Network Firewall 子網路變更保護。如果防火牆未啟用子網路變更保護，則控制項會失敗。

AWS Network Firewall 是一項具狀態的受管網路防火牆和入侵偵測服務，可用來檢查和篩選進出虛擬私有雲端 (VPCs) 的流量。如果您啟用 Network Firewall 防火牆的子網路變更保護，您可以保護防火牆免於意外變更防火牆的子網路關聯。

修補

如需有關啟用現有 Network Firewall 防火牆子網路變更保護的資訊，請參閱《AWS Network Firewall 開發人員指南》中的[更新防火牆](#)。

Amazon OpenSearch Service 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon OpenSearch Service (OpenSearch Service) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Opensearch.1】 OpenSearch 網域應該啟用靜態加密

相關要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.80-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：[opensearch-encrypted-at-rest](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 OpenSearch 網域是否已啟用encryption-at-rest組態。如果未啟用靜態加密，則檢查會失敗。

為了為敏感資料增加一層安全性，您應該將 OpenSearch Service 網域設定為靜態加密。當您設定靜態資料的加密時，會 AWS KMS 儲存並管理您的加密金鑰。若要執行加密，AWS KMS 會使用進階加密標準演算法搭配 256 位元金鑰 (AES-256)。

若要進一步了解 OpenSearch Service 靜態加密，請參閱《[Amazon OpenSearch Service 開發人員指南](#)》中的 [Amazon OpenSearch Service 靜態資料加密](#)。 OpenSearch

修補

若要為新的和現有的 OpenSearch 網域啟用靜態加密，請參閱《Amazon OpenSearch Service 開發人員指南》中的[啟用靜態資料加密](#)。

【Opensearch.2】 不應公開存取 OpenSearch 網域

相關要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-40-53.r50 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7

類別：保護 > 安全網路組態 > VPC 內的資源

嚴重性：嚴重

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：[opensearch-in-vpc-only](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 OpenSearch 網域是否位於 VPC 中。它不會評估 VPC 子網路路由組態來判斷公有存取。

您應該確保 OpenSearch 網域未連接到公有子網路。請參閱《Amazon OpenSearch Service 開發人員指南》中的[資源型政策](#)。您也應該確保您的 VPC 已根據建議的最佳實務進行設定。請參閱《Amazon VPC 使用者指南》中的[VPC 的安全最佳實務](#)。

在 VPC 內部署的 OpenSearch 網域可以透過私有 AWS 網路與 VPC 資源通訊，而不需要周遊公有網際網路。此組態透過限制對傳輸中資料的存取來增加安全狀態。VPCs 提供多種網路控制，以安全存取 OpenSearch 網域，包括網路 ACL 和安全群組。Security Hub 建議您將公有 OpenSearch 網域遷移至 VPCs，以利用這些控制項。

修補

如果您建立了具備公有端點的網域，您稍後便無法將其置放於 VPC 內。反之，您必須建立新網域並遷移您的資料。反之亦然。如果您在 VPC 中建立了網域，該網域便無法擁有公有端點。您必須改為[建立另一個網域](#)或停用此控制項。

如需說明，請參閱《[Amazon OpenSearch Service 開發人員指南](#)》中的在 VPC 中啟動 Amazon OpenSearch Service 網域。 OpenSearch

【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料

相關要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)

類別：保護 > 資料保護 > data-in-transit

嚴重性：中

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：[opensearch-node-to-node-encryption-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 OpenSearch 網域是否已啟用node-to-node加密。如果在網域上停用node-to-node加密，此控制項會失敗。

HTTPS (TLS) 可用來協助防止潛在攻擊者竊聽或使用person-in-the-middle或類似攻擊操縱網路流量。只能允許透過 HTTPS (TLS) 進行加密連線。啟用 OpenSearch 網域的node-to-node加密，可確保叢集內通訊在傳輸中加密。

與此組態相關聯的效能可能會受到懲罰。在啟用此選項之前，您應該注意並測試效能權衡。

修補

若要在 OpenSearch 網域上啟用node-to-node加密，請參閱《Amazon OpenSearch Service 開發人員指南》中的[啟用node-to-node加密](#)。

【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄

相關需求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.8000-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-7

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：[opensearch-logs-to-cloudwatch](#)

排程類型：已觸發變更

參數：

- logtype = 'error' (不可自訂)

此控制項會檢查 OpenSearch 網域是否設定為將錯誤日誌傳送至 CloudWatch Logs。如果未針對網域啟用 CloudWatch 的錯誤記錄，則此控制項會失敗。

您應該啟用 OpenSearch 網域的錯誤日誌，並將這些日誌傳送至 CloudWatch Logs 以進行保留和回應。網域錯誤日誌可協助進行安全和存取稽核，也可協助診斷可用性問題。

修補

若要啟用日誌發佈，請參閱《Amazon OpenSearch Service 開發人員指南》中的[啟用日誌發佈（主控台）](#)。

【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.2.1

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：[opensearch-audit-logging-enabled](#)

排程類型：已觸發變更

參數：

- `cloudWatchLogsLogGroupArnList`（不可自訂）– Security Hub CSPM 不會填入此參數。應為稽核日誌設定的 CloudWatch Logs 日誌群組逗號分隔清單。

此控制項會檢查 OpenSearch 網域是否已啟用稽核記錄。如果 OpenSearch 網域未啟用稽核記錄，則此控制項會失敗。

稽核日誌可高度自訂。它們可讓您追蹤 OpenSearch 叢集上的使用者活動，包括身分驗證成功和失敗、對 OpenSearch 的請求、索引變更，以及傳入的搜尋查詢。

修補

如需啟用稽核日誌的指示，請參閱《Amazon OpenSearch Service 開發人員指南》中的[啟用稽核日誌](#)。

【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：[opensearch-data-node-fault-tolerance](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 OpenSearch 網域是否已設定至少三個資料節點，且zoneAwarenessEnabled為true。如果小於3或instanceCount zoneAwarenessEnabled為，則 OpenSearch 網域的此控制項會失敗false。

為了實現叢集層級的高可用性和容錯能力，OpenSearch 網域應至少具有三個資料節點。部署具有至少三個資料節點的 OpenSearch 網域可確保在節點失敗時執行叢集操作。

修補

修改 OpenSearch 網域中的資料節點數量

1. 登入 AWS 主控台，並在 <https://console.aws.amazon.com/aos/>：// 開啟 Amazon OpenSearch Service 主控台。
2. 在我的網域下，選擇要編輯的網域名稱，然後選擇編輯。
3. 在資料節點下，將節點數量設定為大於的數字3。如果您要部署到三個可用區域，請將數字設定為三個的倍數，以確保可用區域之間的分佈相等。
4. 選擇提交。

【Opensearch.7】 OpenSearch 網域應啟用精細存取控制

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-5、NIST.800-53.r5 AC-6

類別：保護 > 安全存取管理 > 敏感 API 動作受限

嚴重性：高

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：[opensearch-access-control-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 OpenSearch 網域是否已啟用精細存取控制。如果未啟用精細存取控制，則控制項會失敗。精細存取控制需要在 OpenSearch 參數advanced-security-options中update-domain-config啟用。

精細存取控制可提供額外的方式，以控制在 Amazon OpenSearch Service 上對資料的存取。

修補

若要啟用精細存取控制，請參閱《[Amazon OpenSearch Service 開發人員指南](#)》中的 [Amazon OpenSearch Service 精細存取控制](#)。 OpenSearch

【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線

相關要求：NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5 SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-85.r5 SI-7

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：[opensearch-https-required](#)

排程類型：已觸發變更

參數：

- tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10 (不可自訂)

此控制項會檢查 Amazon OpenSearch Service 網域端點是否設定為使用最新的 TLS 安全政策。如果 OpenSearch 網域端點未設定為使用最新支援的政策，或未啟用 HTTPS，則控制項會失敗。

HTTPS (TLS) 可用來防止潛在攻擊者使用中間人攻擊或類似的攻擊手法來竊聽或操控網路流量。只能允許透過 HTTPS (TLS) 進行加密連線。加密傳輸中的資料可能會影響效能。您應該使用此功能測試應用程式，以了解效能描述檔和 TLS 的影響。TLS 1.2 提供相較於舊版 TLS 的數個安全性增強功能。

修補

若要啟用 TLS 加密，請使用 [UpdateDomainConfig](#) API 操作。設定 [DomainEndpointOptions](#) 欄位以指定的值 TLSSecurityPolicy。如需詳細資訊，請參閱《Amazon OpenSearch Service 開發人員指南》中的 [Node-to-node 加密](#)。

【Opensearch.9】應標記 OpenSearch 網域

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::OpenSearch::Domain

AWS Config rule：tagged-opensearch-domain (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon OpenSearch Service 網域是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果網域沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果網域未標記任何索引鍵，則失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知

的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 OpenSearch Service 網域，請參閱《Amazon OpenSearch Service 開發人員指南》中的[使用標籤](#)。

【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新

相關要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：[opensearch-update-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon OpenSearch Service 網域是否已安裝最新的軟體更新。如果有可用的軟體更新，但未為網域安裝軟體更新，則控制項會失敗。

OpenSearch Service 軟體更新提供適用於環境的最新平台修正、更新和功能。使用修補程式安裝 up-to-date 有助於維持網域安全性和可用性。如果未對所需的更新採取任何動作，服務軟體會自動更新（通常在 2 週後）。我們建議在低流量到網域期間排程更新，以將服務中斷降至最低。

修補

若要安裝 OpenSearch 網域的軟體更新，請參閱《Amazon OpenSearch Service 開發人員指南》中的[啟動更新](#)。

【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-2、NIST.800-53.r5 SC-5、NIST.800-53.r5 SC-36、NIST.800-53.r5 SI-13

類別：復原 > 彈性 > 高可用性

嚴重性：低

資源類型：AWS::OpenSearch::Domain

AWS Config 規則：[opensearch-primary-node-fault-tolerance](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon OpenSearch Service 網域是否已設定至少三個專用主節點。如果網域的專用主節點少於三個，則控制項會失敗。

OpenSearch Service 使用專用主節點來提高叢集穩定性。專用主節點會執行叢集管理任務，但不會保留資料或回應資料上傳請求。我們建議您將多可用區與待命搭配使用，這會為每個生產 OpenSearch 網域新增三個專用主節點。

修補

若要變更 OpenSearch 網域的主要節點數量，請參閱《[Amazon OpenSearch Service 開發人員指南](#)》中的[建立和管理](#) Amazon OpenSearch Service 網域。

的 Security Hub CSPM 控制項 AWS 私有 CA

這些 AWS Security Hub CSPM 控制項會評估 AWS 私有憑證授權單位 (AWS 私有 CA) 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【PCA.1】應停用 AWS 私有 CA 根憑證授權單位

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

類別：保護 > 安全網路組態

嚴重性：低

資源類型：AWS::ACMPCA::CertificateAuthority

AWS Config 規則：[acm-pca-root-ca-disabled](#)

排程類型：定期

參數：無

此控制項會檢查 AWS 私有 CA 是否有已停用的根憑證授權機構 (CA)。如果啟用根 CA，則控制項會失敗。

您可以使用 AWS 私有 CA 建立包含根 CA 和次級 CA CAs 階層。您應該盡量減少將根 CA 用於日常任務，尤其是在生產環境中。根 CA 應僅用於為中繼 CAs 發行憑證。這可以讓您透過不會造成損害的方式存放根 CA，並讓中繼 CA 執行發行終端實體憑證的日常任務。

修補

若要停用根 CA，請參閱 AWS 私有憑證授權單位 《使用者指南》中的[更新 CA 狀態](#)。

【PCA.2】應標記 AWS 私有 CA 憑證授權單位

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::ACMPCA::CertificateAuthority

AWS Config 規則：acmpca-certificate-authority-tagged

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS 私有 CA 憑證授權機構是否具有具有參數 中定義之特定金鑰的標籤 `requiredKeyTags`。如果憑證授權機構沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 `requiredKeyTags`。如果 `requiredKeyTags` 未提供 參數，則控制項只會檢查標籤金鑰是否存在，如果憑證授權單位未標記任何金鑰，則 會失敗。系統會 `aws:忽略自動套用並以 開頭的系統標籤`。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[最佳實務和策略](#)。

修補

若要將標籤新增至 AWS 私有 CA 授權機構，請參閱 AWS 私有憑證授權單位 《使用者指南》中的[為您的私有 CA 新增標籤](#)。

Amazon RDS 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Relational Database Service (Amazon RDS) 和 Amazon RDS 資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【RDS.1】 RDS 快照應為私有

相關要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4-4(21)、NIST.800-53.r5 AC-60 NIST.800-53.r5 SC-7

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：AWS::RDS::DBClusterSnapshot、AWS::RDS::DBSnapshot

AWS Config 規則：[rds-snapshots-public-prohibited](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon RDS 快照是否為公有。如果 RDS 快照為公有，則控制項會失敗。此控制項會評估 RDS 執行個體、Aurora 資料庫執行個體、Neptune 資料庫執行個體和 Amazon DocumentDB 叢集。

RDS 快照會用來備份特定時間點您 RDS 執行個體上的資料。快照可以用來還原 RDS 執行個體先前的狀態。

除非預期，否則 RDS 快照不應處於公有狀態。如果您將未加密的手動快照共用為公有，這會使快照可供所有人使用 AWS 帳戶。這可能會導致意外公開您 RDS 執行個體的資料。

請注意，如果組態變更為允許公開存取，則 AWS Config 規則可能無法偵測變更長達 12 小時。在 AWS Config 規則偵測到變更之前，即使組態違反規則，檢查仍會通過。

若要進一步了解共用資料庫快照，請參閱《Amazon RDS 使用者指南》中的[共用資料庫快照](#)。

修補

若要從 RDS 快照移除公有存取權，請參閱[《Amazon RDS 使用者指南》中的共用快照](#)。對於資料庫快照可見性，我們選擇私有。

【RDS.2】 RDS 資料庫執行個體應禁止公開存取，由 PubliclyAccessible 組態決定

相關要求：CIS AWS Foundations Benchmark v5.0.0/2.2.3、CIS AWS Foundations Benchmark v3.0.0/2.3.3、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-75。

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-instance-public-access-check](#)

排程類型：變更已觸發

參數：無

此控制項會評估執行個體組態項目中的 PubliclyAccessible 欄位，以檢查 Amazon RDS 執行個體是否可公開存取。

Neptune 資料庫執行個體和 Amazon DocumentDB 叢集沒有 PubliclyAccessible 旗標，且無法評估。不過，此控制項仍然可以產生這些資源的問題清單。您可以隱藏這些調查結果。

RDS 執行個體組態中的 PubliclyAccessible 值會指出資料庫執行個體是否可以公開存取。將資料庫執行個體設為 PubliclyAccessible 時，其為具有可公開解析 DNS 名稱的面向網際網路執行個體，且此名稱可解析為公有 IP 地址。當無法公開存取資料庫執行個體時，其為具備解析為私有 IP 地址 DNS 名稱的內部執行個體。

除非您打算公開存取 RDS 執行個體，否則不應使用 PubliclyAccessible 值設定 RDS 執行個體。這樣做可能會允許不必要的流量流向資料庫執行個體。

修補

若要從 RDS 資料庫執行個體移除公有存取權，請參閱 [《Amazon RDS 使用者指南》中的修改 Amazon RDS 資料庫執行個體](#)。針對公開存取，選擇否。

[RDS.3] RDS 資料庫執行個體應啟用靜態加密

相關要求：CIS AWS Foundations Benchmark v5.0.0/2.2.1、CIS AWS Foundations Benchmark v3.0.0/2.3.1、CIS AWS Foundations Benchmark v1.4.0/2.3.1、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7

類別：保護 > 資料保護 > data-at-rest 加密

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-storage-encrypted](#)

排程類型：變更已觸發

參數：無

此控制項會檢查您的 Amazon RDS 資料庫執行個體是否已啟用儲存加密。

此控制項適用於 RDS 資料庫執行個體。不過，它也可以產生 Aurora 資料庫執行個體、Neptune 資料庫執行個體和 Amazon DocumentDB 叢集的問題清單。如果這些問題清單沒有用，您可以加以隱藏。

如需為您在 RDS 資料庫執行個體中的敏感資料新增多一層安全，建議您設定 RDS 資料庫執行個體進行靜態加密。如要加密您的 RDS 資料庫執行個體和靜態快照，請為您的 RDS 資料庫執行個體啟用加密選項。靜態加密的資料包括資料庫執行個體的基礎儲存體、其自動化備份、僅供讀取複本，以及快照。

RDS 加密資料庫執行個體會使用開放標準 AES-256 加密演算法，來加密託管 RDS 資料庫執行個體伺服器上的資料。加密資料後，Amazon RDS 會以透明的方式處理資料的存取和解密身分驗證，且對效能的影響最小。您不需要修改資料庫用戶端應用程式即可使用加密。

Amazon RDS 加密目前適用於所有資料庫引擎和儲存類型。大多數資料庫執行個體類別可以使用 Amazon RDS 加密。若要了解不支援 Amazon RDS 加密的資料庫執行個體類別，請參閱 [《Amazon RDS 使用者指南》中的加密 Amazon RDS 資源](#)。

修補

如需有關在 Amazon RDS 中加密資料庫執行個體的資訊，請參閱 [《Amazon RDS 使用者指南》中的加密 Amazon RDS 資源](#)。

【RDS.4】 RDS 叢集快照和資料庫快照應靜態加密

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::RDS::DBClusterSnapshot、 AWS::RDS::DBSnapshot

AWS Config 規則：[rds-snapshot-encrypted](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 RDS 資料庫快照是否已加密。如果未加密 RDS 資料庫快照，則控制項會失敗。

此控制項適用於 RDS 資料庫執行個體。不過，它也可以產生 Aurora 資料庫執行個體、Neptune 資料庫執行個體和 Amazon DocumentDB 叢集快照的問題清單。如果這些問題清單沒有用，您可以加以隱藏。

加密靜態資料可降低未經驗證的使用者存取儲存在磁碟上的資料的風險。RDS 快照中的資料應靜態加密，以增加一層安全性。

修補

若要加密 RDS 快照，請參閱《[Amazon RDS 使用者指南](#)》中的[加密 Amazon RDS 資源](#)。當您加密 RDS 資料庫執行個體時，加密的資料會包含執行個體的基礎儲存體、其自動備份、僅供讀取複本和快照。

您只能在建立 RDS 資料庫執行個體時加密它，而不是在建立資料庫執行個體之後。不過，因為您可以加密未加密快照的副本，所以可以有效地將加密新增至未加密的資料庫執行個體。亦即，您可以建立資料庫執行個體的快照，然後建立該快照的加密副本。接著，從加密快照中還原資料庫執行個體，因此您有原始資料庫執行個體的加密副本。

【RDS.5】 RDS 資料庫執行個體應該設定多個可用區域

相關要求：CIS AWS Foundations Benchmark v5.0.0/2.2.4、NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-multi-az-support](#)

排程類型：變更已觸發

參數：無

此控制項會檢查您的 RDS 資料庫執行個體是否已啟用高可用性。如果 RDS 資料庫執行個體未設定多個可用區域 (AZs)，則控制項會失敗。此控制項不適用於屬於多可用區域資料庫叢集部署的 RDS 資料庫執行個體。

使用 AZs 設定 Amazon RDS 資料庫執行個體有助於確保儲存資料的可用性。如果 AZ 可用性和定期 RDS 維護期間發生問題，多可用區域部署允許自動容錯移轉。

修補

若要在多個 AZs 中部署資料庫執行個體，請在 Amazon RDS 使用者指南中[將資料庫執行個體修改為多可用區域資料庫執行個體部署](#)。

【RDS.6】 應為 RDS 資料庫執行個體設定增強型監控

相關需求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

類別：偵測 > 偵測服務

嚴重性：低

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-enhanced-monitoring-enabled](#)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
monitoringInterval	監控指標收集間隔之間的秒數	列舉	1, 5, 10, 15, 30, 60	無預設值

此控制項會檢查是否已為 Amazon Relational Database Service (Amazon RDS) 資料庫執行個體啟用增強型監控。如果未為執行個體啟用增強型監控，則控制項會失敗。如果您為 monitoringInterval 參數提供自訂值，則只有在指定間隔為執行個體收集增強型監控指標時，控制項才會通過。

在 Amazon RDS 中，增強型監控可更快速回應基礎基礎設施的效能變更。這些效能變更可能會導致資料無法使用。增強型監控可為您的 RDS 資料庫執行個體執行所在的作業系統提供即時指標。代理程式安裝在執行個體上。代理程式可以比 Hypervisor layer 更準確地取得指標。

如果您想查看資料庫執行個體上不同的程序或執行緒如何使用 CPU，增強型監控指標可以派上用場。如需詳細資訊，請參閱 Amazon RDS User Guide (《Amazon RDS 使用者指南》) 中的 [Enhanced Monitoring](#) (增強型監控)。

修補

如需為資料庫執行個體啟用增強型監控的詳細說明，請參閱《Amazon RDS 使用者指南》中的[設定和啟用增強型監控](#)。

【RDS.7】 RDS 叢集應該啟用刪除保護

相關要求：NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

類別：保護 > 資料保護 > 資料刪除保護

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[rds-cluster-deletion-protection-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 RDS 資料庫叢集是否已啟用刪除保護。如果 RDS 資料庫叢集未啟用刪除保護，則控制項會失敗。

此控制項適用於 RDS 資料庫執行個體。不過，它也可以產生 Aurora 資料庫執行個體、Neptune 資料庫執行個體和 Amazon DocumentDB 叢集的問題清單。如果這些問題清單沒有用，您可以加以隱藏。

啟用叢集刪除保護是防止未經授權的實體意外刪除或刪除資料庫的額外保護層。

啟用刪除保護時，無法刪除 RDS 叢集。刪除請求成功之前，必須先停用刪除保護。

修補

若要啟用 RDS 資料庫叢集的刪除保護，請參閱《Amazon RDS 使用者指南》中的[使用主控台、CLI 和 API 修改資料庫叢集](#)。針對刪除保護，選擇啟用刪除保護。

【RDS.8】 RDS 資料庫執行個體應啟用刪除保護

相關需求：NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：保護 > 資料保護 > 資料刪除保護

嚴重性：低

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-instance-deletion-protection-enabled](#)

排程類型：已觸發變更

參數：

- databaseEngines : mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web (不可自訂)

此控制項會檢查使用其中一個所列資料庫引擎的 RDS 資料庫執行個體是否已啟用刪除保護。如果 RDS 資料庫執行個體未啟用刪除保護，則控制項會失敗。

啟用執行個體刪除保護是防止未經授權的實體意外刪除或刪除資料庫的額外保護層。

啟用刪除保護時，無法刪除 RDS 資料庫執行個體。刪除請求成功之前，必須先停用刪除保護。

修補

若要啟用 RDS 資料庫執行個體的刪除保護，請參閱《[Amazon RDS 使用者指南](#)》中的[修改 Amazon RDS 資料庫執行個體](#)。針對刪除保護，選擇啟用刪除保護。

【RDS.9】 RDS 資料庫執行個體應將日誌發佈至 CloudWatch Logs

相關需求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.2.1

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-logging-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon RDS 資料庫執行個體是否已設定為將下列日誌發佈至 Amazon CloudWatch Logs。如果執行個體未設定為將下列日誌發佈至 CloudWatch Logs，則控制項會失敗：

- Oracle：警示、稽核、追蹤、接聽程式
- PostgreSQL：Postgresql、升級
- MySQL：稽核、錯誤、一般、SlowQuery
- MariaDB：稽核、錯誤、一般、SlowQuery
- SQL Server：錯誤、代理程式
- Aurora-MySQL：稽核、錯誤、一般、SlowQuery
- Aurora-PostgreSQL：Postgresql

RDS 資料庫應該啟用相關日誌。資料庫記錄提供對 RDS 提出之請求的詳細記錄。資料庫日誌可協助安全和存取稽核，並有助於診斷可用性問題。

修補

如需有關將 RDS 資料庫日誌發佈至 CloudWatch Logs 的資訊，請參閱《Amazon RDS 使用者指南》中的[指定要發佈至 CloudWatch Logs](#) 的日誌。

【RDS.10】 應為 RDS 執行個體設定 IAM 身分驗證

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

類別：保護 > 安全存取管理 > 無密碼身分驗證

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-instance-iam-authentication-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 資料庫執行個體是否已啟用 IAM 資料庫身分驗證。如果未針對 RDS 資料庫執行個體設定 IAM 身分驗證，則控制項會失敗。此控制項只會評估具有下列引擎類型的 RDS aurora 執行個體：mysql、postgres、aurora-mysql、aurora-postgresql 和 mariadb。RDS 執行個體也必須處於下列其中一種狀態，才能產生問題清單：available、storage-optimization、backing-up 或 storage-full。

IAM 資料庫身分驗證允許使用身分驗證字符而非密碼對資料庫執行個體進行身分驗證。進出資料庫的網路流量會使用 SSL 加密。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的 [IAM 資料庫身分驗證](#)。

修補

若要在 RDS 資料庫執行個體上啟用 IAM 資料庫身分驗證，請參閱《Amazon RDS 使用者指南》中的 [啟用和停用 IAM 資料庫身分驗證](#)。

【RDS.11】 RDS 執行個體應該啟用自動備份

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

類別：復原 > 恢復 > 備份已啟用

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[db-instance-backup-enabled](#)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值	
backupRetentionMinimum	最短備份保留期間，以天為單位	Integer	7 至 35	7	

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值	
checkRead Replicas	檢查 RDS 資料庫執行個體是否已啟用僅供讀取複本的備份	Boolean	無法自訂	false	

此控制項會檢查 Amazon Relational Database Service 執行個體是否已啟用自動備份，以及大於或等於指定時間範圍的備份保留期間。僅供讀取複本會從評估中排除。如果未為執行個體啟用備份，或保留期間小於指定的時間範圍，則控制項會失敗。除非您提供備份保留期間的自訂參數值，否則 Security Hub CSPM 會使用預設值 7 天。

備份可協助您更快速地從安全事件中復原，並強化系統的彈性。Amazon RDS 可讓您設定每日完整執行個體磁碟區快照。如需 Amazon RDS 自動化備份的詳細資訊，請參閱《Amazon RDS 使用者指南》中的[使用備份](#)。

修補

若要在 RDS 資料庫執行個體上啟用自動備份，請參閱《Amazon RDS 使用者指南》中的[啟用自動備份](#)。

【RDS.12】 應為 RDS 叢集設定 IAM 身分驗證

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

類別：保護 > 安全存取管理 > 無密碼身分驗證

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[rds-cluster-iam-authentication-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon RDS 資料庫叢集是否已啟用 IAM 資料庫身分驗證。

IAM 資料庫身分驗證允許對資料庫執行個體進行無密碼身分驗證。身分驗證使用身分驗證字符。進出資料庫的網路流量會使用 SSL 加密。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的 [IAM 資料庫身分驗證](#)。

修補

若要啟用資料庫叢集的 IAM 身分驗證，請參閱《Amazon Aurora 使用者指南》中的 [啟用和停用 IAM 資料庫身分驗證](#)。

【RDS.13】應啟用 RDS 自動次要版本升級

相關要求：CIS AWS Foundations Benchmark v5.0.0/2.2.2、CIS AWS Foundations Benchmark v3.0.0/2.3.2、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：高

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-automatic-minor-version-upgrade-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已為 RDS 資料庫執行個體啟用自動次要版本升級。

自動次要版本升級會定期將資料庫更新為最新的資料庫引擎版本。不過，升級不一定包含最新的資料庫引擎版本。如果您需要在特定時間將資料庫維持在特定版本上，建議您根據所需的排程手動升級至所需的資料庫版本。如果發生重大安全問題或版本達到end-of-support日期時，Amazon RDS 可能會套用次要版本升級，即使您尚未啟用自動次要版本升級選項。如需詳細資訊，請參閱特定資料庫引擎的 Amazon RDS 升級文件：

- [RDS for MariaDB 的自動次要版本升級](#)
- [RDS for MySQL 的自動次要版本升級](#)
- [RDS for PostgreSQL 的自動次要版本升級](#)
- [Amazon RDS 版本的 Db2](#)
- [Oracle 次要版本升級](#)

- [Microsoft SQL Server 資料庫引擎的升級](#)

修補

若要啟用現有資料庫執行個體的自動次要版本升級，請參閱《[Amazon RDS 使用者指南](#)》中的[修改 Amazon RDS 資料庫執行個體](#)。對於自動次要版本升級，選取是。

【RDS.14】 Amazon Aurora 叢集應該已啟用恢復

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SI-13(5)

類別：復原 > 恢復 > 備份已啟用

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[aurora-mysql-backtracking-enabled](#)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值	
BacktrackWindowInHours	恢復 Aurora MySQL 叢集的時數	Double	0.1 至 72	無預設值	

此控制項會檢查 Amazon Aurora 叢集是否已啟用恢復。如果叢集未啟用恢復，則控制項會失敗。如果您為 BacktrackWindowInHours 參數提供自訂值，則只有在叢集恢復指定的時間長度時，控制項才會通過。

備份可協助您更快地從安全事件中復原。它們也會增強您系統的彈性。Aurora 恢復可將資料庫復原至某個時間點的時間縮短。它不需要資料庫還原即可執行此操作。

修補

若要啟用 Aurora 恢復，請參閱《Amazon Aurora 使用者指南》中的[設定恢復](#)。

請注意，您無法在現有叢集上啟用恢復。反之，您可以建立已啟用恢復的複製。如需 Aurora 恢復限制的詳細資訊，請參閱[恢復概觀](#)中的限制清單。

【RDS.15】 應為多個可用區域設定 RDS 資料庫叢集

相關要求：CIS AWS Foundations Benchmark v5.0.0/2.2.4、NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 SC-36、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[rds-cluster-multi-az-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查您的 RDS 資料庫叢集是否已啟用高可用性。如果 RDS 資料庫叢集未部署在多個可用區域 (AZs) 中，則控制項會失敗。

應為多個 AZs 設定 RDS 資料庫叢集，以確保儲存資料的可用性。部署到多個 AZs 允許在發生可用區域可用性問題時以及在一般 RDS 維護事件期間自動容錯移轉。

修補

若要在多個 AZs 部署資料庫叢集，請在 Amazon RDS 使用者指南中[將資料庫執行個體修改為多可用區域資料庫執行個體部署](#)。

Aurora 全域資料庫的修復步驟不同。若要設定 Aurora 全域資料庫的多個可用區域，請選取您的資料庫叢集。然後，選擇動作和新增讀取器，並指定多個 AZs。如需詳細資訊，請參閱《Amazon [Aurora 使用者指南](#)》中的[將 Aurora 複本新增至資料庫叢集](#)。

【RDS.16】 Aurora 資料庫叢集應設定為將標籤複製到資料庫快照

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

類別：識別 > 清查

嚴重性：低

資源類型：AWS::RDS::DBCluster

AWS Config rule：rds-cluster-copy-tags-to-snapshots-enabled (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Aurora 資料庫叢集是否設定為在建立快照時自動將標籤複製到資料庫叢集的快照。如果 Aurora 資料庫叢集未設定為在建立快照時自動將標籤複製到叢集的快照，則控制項會失敗。

識別和清查您的 IT 資產是控管和安全性的重要層面。您需要擁有所有 Amazon Aurora 資料庫叢集的可見性，才能評估其安全狀態，並對潛在弱點區域採取行動。Aurora 資料庫快照應具有與其父資料庫叢集相同的標籤。在 Amazon Aurora 中，您可以設定資料庫叢集，以自動將叢集的所有標籤複製到叢集的快照。啟用此設定可確保資料庫快照繼承與其父資料庫叢集相同的標籤。

修補

如需有關設定 Amazon Aurora 資料庫叢集以自動將標籤複製到資料庫快照的資訊，請參閱 [《Amazon Aurora 使用者指南》](#) 中的 [修改 Amazon Aurora 資料庫叢集](#)。

【RDS.17】 RDS 資料庫執行個體應設定為將標籤複製到快照

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)

類別：識別 > 清查

嚴重性：低

資源類型：AWS::RDS::DBInstance

AWS Config rule：rds-instance-copy-tags-to-snapshots-enabled (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 資料庫執行個體是否設定為在建立快照時將所有標籤複製到快照。

識別和清查您的 IT 資產是控管和安全性的重要層面。您需要擁有所有 RDS 資料庫執行個體的可見性，才能評估其安全性狀態，並對潛在弱點區域採取動作。快照的標記方式應該與其父 RDS 資料庫執行個體相同。啟用此設定可確保快照繼承其父資料庫執行個體的標籤。

修補

若要自動將標籤複製到 RDS 資料庫執行個體的快照，請參閱 [《Amazon RDS 使用者指南》中的修改 Amazon RDS 資料庫執行個體](#)。選取將標籤複製到快照。

【RDS.18】 RDS 執行個體應部署在 VPC 中

類別：保護 > 安全網路組態 > VPC 內的資源

嚴重性：高

資源類型：AWS::RDS::DBInstance

AWS Config rule：rds-deployed-in-vpc (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon RDS 執行個體是否部署在 EC2-VPC 上。

VPCs 提供多種網路控制，以安全存取 RDS 資源。這些控制項包括 VPC 端點、網路 ACLs 和安全群組。若要利用這些控制項，建議您在 EC2-VPC 上建立 RDS 執行個體。

修補

如需將 RDS 執行個體移至 VPC 的指示，請參閱 [《Amazon RDS 使用者指南》中的更新資料庫執行個體的 VPC](#)。

【RDS.19】 應為關鍵叢集事件設定現有的 RDS 事件通知訂閱

相關需求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2

類別：偵測 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：AWS::RDS::EventSubscription

AWS Config rule：rds-cluster-event-notifications-configured (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查資料庫叢集的現有 Amazon RDS 事件訂閱是否已啟用下列來源類型和事件類別索引鍵/值對的通知：

```
DBCluster: ["maintenance","failure"]
```

如果您的帳戶中沒有現有的事件訂閱，則控制項會通過。

RDS 事件通知使用 Amazon SNS，讓您了解 RDS 資源可用性或組態的變更。這些通知允許快速回應。如需 RDS 事件通知的其他資訊，請參閱 [《Amazon RDS 使用者指南》中的使用 Amazon RDS 事件通知](#)。

修補

若要訂閱 RDS 叢集事件通知，請參閱 [《Amazon RDS 使用者指南》中的訂閱 Amazon RDS 事件通知](#)。使用下列的值：

欄位	Value
Source type (來源類型)	叢集
要包含的叢集	所有叢集
要包含的事件類別	選取特定事件類別或所有事件類別

【RDS.20】 應為關鍵資料庫執行個體事件設定現有的 RDS 事件通知訂閱

相關要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2、PCI DSS v4.0.1/11.5.2

類別：偵測 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：AWS::RDS::EventSubscription

AWS Config rule：rds-instance-event-notifications-configured (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查資料庫執行個體的現有 Amazon RDS 事件訂閱是否已啟用下列來源類型和事件類別索引鍵/值對的通知：

```
DBInstance: ["maintenance","configuration change","failure"]
```

如果您的帳戶中沒有現有的事件訂閱，則控制項會通過。

RDS 事件通知使用 Amazon SNS，讓您了解 RDS 資源可用性或組態的變更。這些通知允許快速回應。如需 RDS 事件通知的其他資訊，請參閱 [《Amazon RDS 使用者指南》中的使用 Amazon RDS 事件通知](#)。

修補

若要訂閱 RDS 執行個體事件通知，請參閱 [《Amazon RDS 使用者指南》中的訂閱 Amazon RDS 事件通知](#)。使用下列的值：

欄位	Value
Source type (來源類型)	執行個體
要包含的執行個體	所有執行個體
要包含的事件類別	選取特定事件類別或所有事件類別

【RDS.21】 應為關鍵資料庫參數群組事件設定 RDS 事件通知訂閱

相關要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2、PCI DSS v4.0.1/11.5.2

類別：偵測 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：AWS::RDS::EventSubscription

AWS Config rule：rds-pg-event-notifications-configured (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon RDS 事件訂閱是否存在，並針對下列來源類型事件類別索引鍵/值對啟用通知。如果您的帳戶中沒有現有的事件訂閱，則控制項會通過。

```
DBParameterGroup: ["configuration change"]
```

RDS 事件通知使用 Amazon SNS，讓您了解 RDS 資源可用性或組態的變更。這些通知允許快速回應。如需 RDS 事件通知的其他資訊，請參閱 [《Amazon RDS 使用者指南》](#) 中的 [使用 Amazon RDS 事件通知](#)。

修補

若要訂閱 RDS 資料庫參數群組事件通知，請參閱 [《Amazon RDS 使用者指南》](#) 中的 [訂閱 Amazon RDS 事件通知](#)。使用下列的值：

欄位	Value
Source type (來源類型)	參數群組
要包含的參數群組	所有參數群組
要包含的事件類別	選取特定事件類別或所有事件類別

【RDS.22】 應為關鍵資料庫安全群組事件設定 RDS 事件通知訂閱

相關要求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-2、PCI DSS v4.0.1/11.5.2

類別：偵測 > 偵測服務 > 應用程式監控

嚴重性：低

資源類型：AWS::RDS::EventSubscription

AWS Config rule : rds-sg-event-notifications-configured (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon RDS 事件訂閱是否存在，並針對下列來源類型事件類別索引鍵/值對啟用通知。如果您的帳戶中沒有現有的事件訂閱，則控制項會通過。

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS 事件通知使用 Amazon SNS，讓您了解 RDS 資源可用性或組態的變更。這些通知允許快速回應。如需 RDS 事件通知的其他資訊，請參閱 [《Amazon RDS 使用者指南》中的使用 Amazon RDS 事件通知](#)。

修補

若要訂閱 RDS 執行個體事件通知，請參閱 [《Amazon RDS 使用者指南》中的訂閱 Amazon RDS 事件通知](#)。使用下列的值：

欄位	Value
Source type (來源類型)	Security groups (安全群組)
要包含的安全群組	所有安全群組
要包含的事件類別	選取特定事件類別或所有事件類別

【RDS.23】 RDS 執行個體不應使用資料庫引擎預設連接埠

相關要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(5)

類別：保護 > 安全網路組態

嚴重性：低

資源類型：AWS::RDS::DBInstance

AWS Config rule : rds-no-default-ports (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 叢集或執行個體是否使用資料庫引擎預設連接埠以外的連接埠。如果 RDS 叢集或執行個體使用預設連接埠，則控制項會失敗。此控制項不適用於屬於叢集的 RDS 執行個體。

如果您使用已知連接埠來部署 RDS 叢集或執行個體，攻擊者可以猜測叢集或執行個體的相關資訊。攻擊者可以將此資訊與其他資訊搭配使用，以連線至 RDS 叢集或執行個體，或取得您應用程式的其他資訊。

當您變更連接埠時，也必須更新用來連線至舊連接埠的現有連線字串。您也應該檢查資料庫執行個體的安全群組，以確保它包含允許在新連接埠上連線的輸入規則。

修補

若要修改現有 RDS 資料庫執行個體的預設連接埠，請參閱《[Amazon RDS 使用者指南](#)》中的[修改 Amazon RDS 資料庫執行個體](#)。若要修改現有 RDS 資料庫叢集的預設連接埠，請參閱《[Amazon Aurora 使用者指南](#)》中的[使用主控台、CLI 和 API 修改資料庫叢集](#)。對於資料庫連接埠，將連接埠值變更為非預設值。

【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/2.2.2

類別：識別 > 資源組態

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[rds-cluster-default-admin-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon RDS 資料庫叢集是否已變更其預設值的管理員使用者名稱。控制項不適用於 neptune (Neptune 資料庫) 或 docdb (DocumentDB) 類型的引擎。如果管理員使用者名稱設定為預設值，則此規則將會失敗。

建立 Amazon RDS 資料庫時，您應該將預設管理員使用者名稱變更為唯一值。預設使用者名稱是公有知識，應該在 RDS 資料庫建立期間變更。變更預設使用者名稱可降低意外存取的風險。

修補

若要變更與 Amazon RDS 資料庫叢集相關聯的管理員使用者名稱，[請建立新的 RDS 資料庫叢集](#)，並在建立資料庫時變更預設的管理員使用者名稱。

【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、PCI DSS v4.0.1/2.2.2

類別：識別 > 資源組態

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-instance-default-admin-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查您是否已從預設值變更 Amazon Relational Database Service (Amazon RDS) 資料庫執行個體的管理使用者名稱。如果管理使用者名稱設定為預設值，則控制項會失敗。控制項不適用於 neptune (Neptune 資料庫) 或 docdb (DocumentDB) 類型的引擎，以及屬於叢集的 RDS 執行個體。

Amazon RDS 資料庫上的預設管理使用者名稱為公有知識。建立 Amazon RDS 資料庫時，您應該將預設管理使用者名稱變更為唯一值，以降低意外存取的風險。

修補

若要變更與 RDS 資料庫執行個體相關聯的管理使用者名稱，請先[建立新的 RDS 資料庫執行個體](#)。在建立資料庫時變更預設管理使用者名稱。

【RDS.26】 RDS 資料庫執行個體應受備份計劃保護

類別：復原 > 恢復 > 備份已啟用

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-resources-protected-by-backup-plan](#)

排程類型：定期

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
backupVaultLockCheck	如果參數設為 true 且資源使用 AWS Backup 保存庫鎖定，則控制項會產生 PASSED 問題清單。	Boolean	true 或 false *	無預設值

此控制項會評估備份計畫是否涵蓋 Amazon RDS 資料庫執行個體。如果備份計畫未涵蓋 RDS 資料庫執行個體，則此控制項會失敗。如果您將 backupVaultLockCheck 參數設定為等於 true，則只有在執行個體備份在 AWS Backup 鎖定的保存庫中時，控制項才會通過。

Note

此控制項不會評估 Neptune 和 DocumentDB 執行個體。它也不會評估屬於叢集成員的 RDS 資料庫執行個體。

AWS Backup 是一種全受管備份服務，可集中和自動化跨的資料備份 AWS 服務。使用 AWS Backup，您可以建立稱為備份計畫的備份政策。您可以使用這些計畫來定義備份需求，例如備份資料的頻率，以及這些備份的保留時間。在備份計畫中包含 RDS 資料庫執行個體，可協助您保護資料免於意外遺失或遭到刪除。

修補

若要將 RDS 資料庫執行個體新增至 AWS Backup 備份計畫，請參閱《AWS Backup 開發人員指南》中的[將資源指派給備份計畫](#)。

【RDS.27】 RDS 資料庫叢集應靜態加密

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[rds-cluster-encrypted-at-rest](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 RDS 資料庫叢集是否靜態加密。如果 RDS 資料庫叢集未靜態加密，則控制項會失敗。

靜態資料是指在任何期間內存放在持久性、非揮發性儲存體中的任何資料。加密可協助您保護此類資料的機密性，降低未經授權的使用者可存取資料的風險。加密 RDS 資料庫叢集可保護您的資料和中繼資料免於未經授權的存取。它還滿足生產檔案系統data-at-rest加密的合規要求。

修補

您可以在建立 RDS 資料庫叢集時啟用靜態加密。您無法在建立叢集後變更加密設定。如需詳細資訊，請參閱 [《Amazon Aurora 使用者指南》中的加密 Amazon Aurora 資料庫叢集](#)。

【RDS.28】 RDS 資料庫叢集應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::RDS::DBCluster

AWS Config rule：tagged-rds-dbcluster (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon RDS 資料庫叢集是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果資料庫叢集沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果資料庫叢集未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 RDS 資料庫叢集，請參閱 [《Amazon RDS 使用者指南》](#) 中的 [標記 Amazon RDS 資源](#)。

【RDS.29】應標記 RDS 資料庫叢集快照

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::RDS::DBClusterSnapshot

AWS Config rule：tagged-rds-dbclustersnapshot (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon RDS 資料庫叢集快照是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果資料庫叢集快照沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果資料庫叢集快照未標記任何索引鍵，則會失敗。系統會忽略以 aws: 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 RDS 資料庫叢集快照，請參閱 [《Amazon RDS 使用者指南》](#) 中的標記 [Amazon RDS 資源](#)。

【RDS.30】 RDS 資料庫執行個體應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::RDS::DBInstance

AWS Config rule：tagged-rds-dbinstance (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon RDS 資料庫執行個體是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果資料庫執行個體沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果資料庫執行個體未標記任何索引鍵，則 會失敗。系統會 aws: 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 RDS 資料庫執行個體，請參閱 [《Amazon RDS 使用者指南》](#) 中的標記 [Amazon RDS 資源](#)。

【RDS.31】 RDS 資料庫安全群組應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::RDS::DBSecurityGroup

AWS Config rule：tagged-rds-dbsecuritygroup (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon RDS 資料庫安全群組是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果資料庫安全群組沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果資料庫安全群組未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的負責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 RDS 資料庫安全群組，請參閱《[Amazon RDS 使用者指南](#)》中的標記 [Amazon RDS 資源](#)。

【RDS.32】 RDS 資料庫快照應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::RDS::DBSnapshot

AWS Config rule：tagged-rds-dbsnapshot (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon RDS 資料庫快照是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果資料庫快照沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果資料庫快照未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱[什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 RDS 資料庫快照，請參閱《[Amazon RDS 使用者指南](#)》中的標記 [Amazon RDS 資源](#)。

【RDS.33】 RDS 資料庫子網路群組應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::RDS::DBSubnetGroup

AWS Config rule：tagged-rds-dbsubnetgroups (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon RDS 資料庫子網路群組是否具有具有參數 `中定義之特定金鑰的標籤requiredTagKeys`。如果資料庫子網路群組沒有任何標籤索引鍵，或沒有參數 `中指定的所有索引鍵`，則控制項會失敗`requiredTagKeys`。如果`requiredTagKeys`未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果資料庫子網路群組未標記任何索引鍵，則會失敗。系統會`aws:忽略自動套用並以開頭的系統標籤`。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱[什麼是 ABAC AWS？](#) IAM 使用者指南中的。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 RDS 資料庫子網路群組，請參閱 [《Amazon RDS 使用者指南》中的標記 Amazon RDS 資源](#)。

【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.8000-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.2.1

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[rds-aurora-mysql-audit-logging-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon Aurora MySQL 資料庫叢集是否已設定為將稽核日誌發佈至 Amazon CloudWatch Logs。如果叢集未設定為將稽核日誌發佈至 CloudWatch Logs，則控制項會失敗。控制項不會產生 Aurora Serverless v1 資料庫叢集的問題清單。

稽核日誌會擷取資料庫活動的記錄，包括登入嘗試、資料修改、結構描述變更，以及其他可基於安全與合規目的而稽核的事件。當您設定 Aurora MySQL 資料庫叢集將稽核日誌發佈至 Amazon CloudWatch Logs 中的日誌群組時，您可以執行日誌資料的即時分析。CloudWatch Logs 會將日誌保留在高耐用性的儲存中。您也可以 CloudWatch 中建立警示和檢視指標。

 Note

將稽核日誌發佈至 CloudWatch Logs 的另一種方法是啟用進階稽核，並將叢集層級資料庫參數 `server_audit_logs_upload` 設為 1。的預設值 `server_audit_logs_upload parameter` 為 0。不過，我們建議您改用下列修補指示來傳遞此控制項。

修補

若要將 Aurora MySQL 資料庫叢集稽核日誌發佈至 CloudWatch Logs，請參閱 [《Amazon Aurora 使用者指南》](#) 中的 [將 Amazon Aurora MySQL 日誌發佈至 Amazon CloudWatch Logs](#)。

【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級

相關要求：NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、PCI DSS v4.0.1/6.3.3

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[rds-cluster-auto-minor-version-upgrade-enable](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon RDS Multi-AZ 資料庫叢集是否已啟用自動次要版本升級。如果未為多可用區域資料庫叢集啟用自動次要版本升級，則控制項會失敗。

RDS 提供自動次要版本升級，讓您可以將多可用區域資料庫叢集保持在最新狀態。次要版本可以引進新的軟體功能、錯誤修正、安全性修補程式和效能改善。透過在 RDS 資料庫叢集上啟用自動次要版本升級，當有新版本可用時，叢集以及叢集中的執行個體都會收到次要版本的自動更新。更新會在維護時段期間自動套用。

修補

若要在多可用區域資料庫叢集上啟用自動次要版本升級，請參閱《Amazon RDS 使用者指南》中的[修改多可用區域資料庫叢集](#)。

【RDS.36】 RDS for PostgreSQL 資料庫執行個體應將日誌發佈至 CloudWatch Logs

相關要求：PCI DSS v4.0.1/10.4.2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-postgresql-logs-to-cloudwatch](#)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
logTypes	要發佈至 CloudWatch Logs 的日誌類型逗號分隔清單	StringList	無法自訂	postgresq l

此控制項會檢查 Amazon RDS for PostgreSQL 資料庫執行個體是否已設定為將日誌發佈至 Amazon CloudWatch Logs。如果 PostgreSQL 資料庫執行個體未設定為將 logTypes 參數中提到的日誌類型發佈至 CloudWatch Logs，則控制項會失敗。

資料庫記錄提供對 RDS 執行個體提出之請求的詳細記錄。PostgreSQL 會產生事件日誌，其中包含管理員的實用資訊。將這些日誌發佈到 CloudWatch Logs 可集中管理日誌，並協助您執行日誌資料的即

時分析。CloudWatch Logs 會將日誌保留在高耐用性的儲存中。您也可以在 CloudWatch 中建立警示和檢視指標。

修補

若要將 PostgreSQL 資料庫執行個體日誌發佈至 CloudWatch Logs，請參閱《[Amazon RDS 使用者指南](#)》中的將 [PostgreSQL 日誌發佈至 Amazon CloudWatch Logs](#)。

【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs

相關要求：PCI DSS v4.0.1/10.4.2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[rds-aurora-postgresql-logs-to-cloudwatch](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon Aurora PostgreSQL 資料庫叢集是否設定為將日誌發佈至 Amazon CloudWatch Logs。如果 Aurora PostgreSQL 資料庫叢集未設定為將 PostgreSQL 日誌發佈至 CloudWatch Logs，則控制項會失敗。

資料庫記錄提供對 RDS 叢集提出之請求的詳細記錄。Aurora PostgreSQL 會產生事件日誌，其中包含管理員的實用資訊。將這些日誌發佈至 CloudWatch Logs 可集中管理日誌，並協助您執行日誌資料的即時分析。CloudWatch Logs 會將日誌保留在高耐用性的儲存中。您也可以在 CloudWatch 中建立警示和檢視指標。

修補

若要將 Aurora PostgreSQL 資料庫叢集日誌發佈至 CloudWatch Logs，請參閱《[Amazon RDS 使用者指南](#)》中的將 [Aurora PostgreSQL 日誌發佈至 Amazon CloudWatch Logs](#)。

【RDS.38】 RDS for PostgreSQL 資料庫執行個體應在傳輸中加密

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-postgres-instance-encrypted-in-transit](#)

排程類型：定期

參數：無

此控制項會檢查與 Amazon RDS for PostgreSQL 資料庫 (DB) 執行個體的連線是否在傳輸中加密。如果與執行個體相關聯之參數群組的 `rds.force_ssl` 參數設定為 0 (關閉)，則控制項會失敗。此控制項不會評估屬於資料庫叢集的 RDS 資料庫執行個體。

傳輸中的資料是指從一個位置移動到另一個位置的資料，例如叢集中的節點之間，或叢集與您的應用程式之間。資料可能會在網際網路或私有網路中移動。加密傳輸中的資料可降低未經授權的使用者可以竊聽網路流量的風險。

修補

若要要求 RDS for PostgreSQL 資料庫執行個體的所有連線使用 SSL，請參閱《Amazon RDS 使用者指南》中的[搭配使用 SSL 與 PostgreSQL 資料庫執行個體](#)。

【RDS.39】 RDS for MySQL 資料庫執行個體應在傳輸中加密

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-mysql-instance-encrypted-in-transit](#)

排程類型：定期

參數：無

此控制項會檢查與 Amazon RDS for MySQL 資料庫 (DB) 執行個體的連線是否在傳輸中加密。如果與執行個體相關聯之參數群組的 `rds.require_secure_transport` 參數設定為 0 (關閉)，則控制項會失敗。此控制項不會評估屬於資料庫叢集的 RDS 資料庫執行個體。

傳輸中的資料是指從一個位置移動到另一個位置的資料，例如叢集中的節點之間，或叢集與您的應用程式之間。資料可能會在網際網路或私有網路中移動。加密傳輸中的資料可降低未經授權的使用者可以竊聽網路流量的風險。

修補

若要要求 RDS for MySQL 資料庫執行個體的所有連線都使用 SSL，請參閱 [《Amazon RDS 使用者指南》中的 Amazon RDS 上 MySQL 資料庫執行個體的 SSL/TLS 支援](#)。

【RDS.40】 RDS for SQL Server 資料庫執行個體應將日誌發佈至 CloudWatch Logs

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-7

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-sql-server-logs-to-cloudwatch](#)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
logTypes	RDS for SQL Server 資料庫執行個體應設定為發佈至 CloudWatch Logs 的日誌類型清單。如果資料庫執行個體未設定為發佈清單中指定的日誌類型，則此控制項會失敗。	EnumList (最多 2 個項目)	agent, error	agent, error

此控制項會檢查 Amazon RDS for Microsoft SQL Server 資料庫執行個體是否已設定為將日誌發佈至 Amazon CloudWatch Logs。如果 RDS for SQL Server 資料庫執行個體未設定為將日誌發佈至 CloudWatch Logs，則控制項會失敗。您可以選擇性地指定資料庫執行個體應設定為發佈的日誌類型。

資料庫記錄提供對 Amazon RDS 資料庫執行個體提出之請求的詳細記錄。將日誌發佈至 CloudWatch Logs 可集中管理日誌，並協助您執行日誌資料的即時分析。CloudWatch Logs 會將日誌保留在高耐用

性的儲存中。此外，您可以使用它來為可能發生的特定錯誤建立警示，例如在錯誤日誌中記錄的頻繁重新啟動。同樣地，您可以針對 SQL Server 代理程式任務相關日誌中記錄的錯誤或警告建立警示。

修補

如需有關將日誌發佈至 RDS for SQL Server 資料庫執行個體的 CloudWatch Logs 的資訊，請參閱 [《Amazon Relational Database Service 使用者指南》](#) 中的 [Amazon RDS for Microsoft SQL Server 資料庫日誌檔案](#)。Amazon Relational Database Service

【RDS.41】 RDS for SQL Server 資料庫執行個體應在傳輸中加密

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-sqlserver-encrypted-in-transit](#)

排程類型：定期

參數：無

此控制項會檢查與 Amazon RDS for Microsoft SQL Server 資料庫執行個體的連線是否在傳輸中加密。如果與資料庫執行個體相關聯的參數群組的 `rds.force_ssl` 參數設定為 `off`，則控制項會失敗 (off)。

傳輸中的資料是指從一個位置移動到另一個位置的資料，例如資料庫叢集中的節點之間，或資料庫叢集與用戶端應用程式之間。資料可以跨網際網路或在私有網路中移動。加密傳輸中的資料可降低未經授權的使用者竊聽網路流量的風險。

修補

如需有關為執行 Microsoft SQL Server 的 Amazon RDS 資料庫執行個體啟用 SSL/TLS 的詳細資訊，請參閱 [《Amazon Relational Database Service 使用者指南》](#) 中的 [搭配使用 SSL 與 Microsoft SQL Server 資料庫執行個體](#)。

【RDS.42】 RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5

AU-6(4)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-75 NIST.800-53.r5 SC-7 SI-3 SI-4 SI-7

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[mariadb-publish-logs-to-cloudwatch-logs](#)

排程類型：定期

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
logTypes	MariaDB 資料庫執行個體應設定為發佈至 CloudWatch Logs 的日誌類型清單。如果資料庫執行個體未設定為發佈清單中指定的日誌類型，控制項會產生 FAILED 問題清單。	EnumList (最多 4 個項目)	audit, error, general, slowquery	audit, error

此控制項會檢查 Amazon RDS for MariaDB 資料庫執行個體是否設定為將特定類型的日誌發佈至 Amazon CloudWatch Logs。如果 MariaDB 資料庫執行個體未設定為將日誌發佈至 CloudWatch Logs，則控制項會失敗。您可以選擇性地指定應設定 MariaDB 資料庫執行個體發佈的日誌類型。

資料庫記錄提供對 Amazon RDS for MariaDB 資料庫執行個體提出之請求的詳細記錄。將日誌發佈至 Amazon CloudWatch Logs 可集中管理日誌，並協助您執行日誌資料的即時分析。此外，CloudWatch Logs 會將日誌保留在耐用的儲存體中，以支援安全性、存取和可用性審查和稽核。使用 CloudWatch Logs，您也可以建立警示並檢閱指標。

修補

如需有關設定 Amazon RDS for MariaDB 資料庫執行個體將日誌發佈至 Amazon CloudWatch Logs 的資訊，請參閱《Amazon Relational Database Service 使用者指南》中的[將 MariaDB 日誌發佈至 Amazon CloudWatch Logs](#)。Amazon Relational Database Service

【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密

類別：保護 > 資料保護 > data-in-transit

嚴重性：中

資源類型：AWS::RDS::DBProxy

AWS Config 規則：[rds-proxy-tls-encryption](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon RDS 資料庫代理是否需要代理與基礎 RDS 資料庫執行個體之間所有連線的 TLS。如果代理不需要代理與 RDS 資料庫執行個體之間所有連線的 TLS，則控制項會失敗。

Amazon RDS Proxy 可以充當用戶端應用程式與基礎 RDS 資料庫執行個體之間的額外安全層。例如，您可以使用 TLS 1.3 連線到 RDS 代理，即使基礎資料庫執行個體支援舊版 TLS。透過使用 RDS Proxy，您可以對資料庫應用程式強制執行強大的身分驗證要求。

修補

如需有關將 Amazon RDS 代理的設定變更為需要 TLS 的資訊，請參閱《Amazon Relational Database Service 使用者指南》中的[修改 RDS 代理](#)。

【RDS.44】 RDS for MariaDB 資料庫執行個體應在傳輸中加密

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-mariadb-instance-encrypted-in-transit](#)

排程類型：定期

參數：無

此控制項會檢查與 Amazon RDS for MariaDB 資料庫執行個體的連線是否在傳輸中加密。如果與資料庫執行個體相關聯的資料庫參數群組未同步，或參數群組的 `require_secure_transport` 參數未設定為 `ON`，則控制項會失敗。

Note

此控制項不會評估使用早於 10.5 版的 MariaDB 版本的 Amazon RDS 資料庫執行個體。`require_secure_transport` 參數僅支援 MariaDB 10.5 版和更新版本。

傳輸中的資料是指從一個位置移動到另一個位置的資料，例如資料庫叢集中的節點之間，或資料庫叢集與用戶端應用程式之間。資料可以跨網際網路或在私有網路中移動。加密傳輸中的資料可降低未經授權的使用者竊聽網路流量的風險。

修補

如需為 Amazon RDS for MariaDB 資料庫執行個體的連線啟用 SSL/TLS 的詳細資訊，請參閱《Amazon Relational Database Service 使用者指南》中的需要[所有 MariaDB 資料庫執行個體連線的 SSL/TLS](#)。

【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-75 SI-3 SI-4 SI-7

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[aurora-mysql-cluster-audit-logging](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon Aurora MySQL 資料庫叢集是否已啟用稽核記錄。如果與資料庫叢集相關聯的資料庫參數群組未同步、`server_audit_logging`參數未設定為 1，或`server_audit_events`參數設定為空值，則控制項會失敗。

資料庫日誌可協助安全和存取稽核，並協助診斷可用性問題。稽核日誌會擷取資料庫活動的記錄，包括登入嘗試、資料修改、結構描述變更，以及其他可基於安全與合規目的而稽核的事件。

修補

如需有關啟用 Amazon Aurora MySQL 資料庫叢集記錄的資訊，請參閱 [《Amazon Aurora 使用者指南》](#) 中的將 Amazon Aurora MySQL 日誌發佈至 Amazon CloudWatch Logs。

【RDS.46】 RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中

類別：保護 > 安全網路組態 > 資源不可公開存取

嚴重性：高

資源類型：AWS::RDS::DBInstance

AWS Config 規則：[rds-instance-subnet-igw-check](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon RDS 資料庫執行個體是否部署在具有網際網路閘道路由的公有子網路中。如果 RDS 資料庫執行個體部署在具有網際網路閘道路由的子網路中，且目的地設定為 0.0.0.0/0 或，則控制項會失敗。:/0。

透過在私有子網路中佈建 Amazon RDS 資源，您可以防止 RDS 資源從公有網際網路接收傳入流量，進而防止意外存取 RDS 資料庫執行個體。如果 RDS 資源佈建在開放給網際網路的公有子網路中，它們可能會面臨資料外洩等風險。

修補

如需有關為 Amazon RDS 資料庫執行個體佈建私有子網路的資訊，請參閱《Amazon Relational Database Service 使用者指南》中的[在 VPC 中使用資料庫執行個體](#)。

【RDS.47】 RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[rds-pgsql-cluster-copy-tags-to-snapshot-check](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon RDS for PostgreSQL 資料庫叢集是否設定為在建立快照時自動將標籤複製到資料庫叢集的快照。如果 RDS for PostgreSQL 資料庫叢集的 CopyTagsToSnapshot 參數設定為 false，則控制項會失敗。

將標籤複製到資料庫快照有助於維持跨備份資源的適當資源追蹤、控管和成本分配。這可在作用中資料庫及其快照之間實現一致的資源識別、存取控制和合規監控。正確標記的快照可確保備份資源繼承與其來源資料庫相同的中繼資料，以改善安全操作。

修補

如需有關設定 Amazon RDS for PostgreSQL 資料庫叢集以自動將標籤複製到資料庫快照的資訊，請參閱 [《Amazon Relational Database Service 使用者指南》](#) 中的標記 [Amazon RDS 資源](#)。Amazon Relational Database Service

【RDS.48】 RDS for MySQL 資料庫叢集應設定為將標籤複製到資料庫快照

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[rds-mysql-cluster-copy-tags-to-snapshot-check](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon RDS for MySQL 資料庫叢集是否設定為在建立快照時自動將標籤複製到資料庫叢集的快照。如果 RDS for MySQL 資料庫叢集的 CopyTagsToSnapshot 參數設定為 false，則控制項會失敗。

將標籤複製到資料庫快照有助於維持跨備份資源的適當資源追蹤、控管和成本分配。這可在作用中資料庫及其快照之間實現一致的資源識別、存取控制和合規監控。正確標記的快照可確保備份資源繼承與其來源資料庫相同的中繼資料，以改善安全操作。

修補

如需有關設定 Amazon RDS for MySQL 資料庫叢集以自動將標籤複製到資料庫快照的資訊，請參閱 [《Amazon Relational Database Service 使用者指南》](#) 中的標記 [Amazon RDS 資源](#)。Amazon Relational Database Service

【RDS.50】 RDS 資料庫叢集應設定足夠的備份保留期間

類別：復原 > 恢復 > 備份已啟用

嚴重性：中

資源類型：AWS::RDS::DBCluster

AWS Config 規則：[rds-cluster-backup-retention-check](#)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值	
minimumBackupRetentionPeriod	控制項要檢查的最短備份保留期間，以天為單位	Integer	7 至 35	7	

此控制項會檢查 RDS 資料庫叢集是否有最短的備份保留期間。如果備份保留期小於指定的參數值，則控制項會失敗。除非您提供自訂參數值，否則 Security Hub 會使用預設值 7 天。

此控制項會檢查 RDS 資料庫叢集是否有最短的備份保留期間。如果備份保留期小於指定的參數值，則控制項會失敗。除非您提供客戶參數值，否則 Security Hub 會使用預設值 7 天。此控制項適用於所有類型的 RDS 資料庫叢集，包括 Aurora 資料庫叢集、DocumentDB 叢集、NeptuneDB 叢集等。

修補

若要設定 RDS 資料庫叢集的備份保留期，請修改叢集設定，並將備份保留期設定為至少 7 天（或控制參數中指定的值）。如需詳細說明，請參閱《Amazon Relational Database Service 使用者指南》中的[備份保留期](#)。對於 Aurora 資料庫叢集，請參閱《Amazon [Aurora 使用者指南](#)》中的[備份和還原 Aurora 資料庫叢集](#)概觀。如需其他類型的資料庫叢集（例如 DocumentDB 叢集），請參閱對應的服務使用者指南，了解如何更新叢集的備份保留期間。

【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：高

資源類型：AWS::RDS::GlobalCluster

AWS Config 規則：[rds-global-cluster-aurora-mysql-supported-version](#)

排程類型：變更已觸發

參數：

- minSupportedEngineVersion：8.0.mysql_aurora.3.08.0 (不可自訂)
- longTermSupportVersion：8.0.mysql_aurora.3.04.0, 8.0.mysql_aurora.3.04.1, 8.0.mysql_aurora.3.04.2, 8.0.mysql_aurora.3.04.3 (不可自訂)

此控制項會檢查 Amazon Aurora MySQL 全域叢集是否在最低支援的引擎版本上執行。如果 Aurora MySQL 全域叢集引擎版本低於指定的最低支援版本，且未列在長期支援版本參數中，則控制項會失敗。

在支援的引擎版本上執行 Aurora MySQL 全域資料庫，有助於確保您可存取最新的安全修補程式、錯誤修正和效能改善。Aurora MySQL 次要版本已定義end-of-standard-support，之後就不會再收到重要的修補程式。執行不支援的版本可能會讓您的全域資料庫暴露在安全漏洞中，並可能導致 Amazon RDS 延長支援費用。由於 Aurora MySQL 遵循非連續的支援生命週期，其中長期支援 (LTS) 版本維持支援的時間超過後續的非 LTS 版本，因此此控制項也會檢查仍在標準支援的 LTS 版本。如需詳細資訊，請參閱 [Aurora MySQL 的 Amazon Aurora 版本備註](#) 中的 Amazon Aurora MySQL 版本行事曆。

修補

如需有關將 Aurora MySQL 全域資料庫升級至支援引擎版本的資訊，請參閱 [《Amazon Aurora 使用者指南》](#) 中的 [透過修改引擎版本來升級 Amazon Aurora 全域資料庫和升級 Aurora MySQL](#)。

Amazon Redshift 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Redshift 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【Redshift.1】 Amazon Redshift 叢集應禁止公開存取

相關需求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全網路組態 > 不可公開存取的資源

嚴重性：嚴重

資源類型：AWS::Redshift::Cluster

AWS Config 規則：[redshift-cluster-public-access-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Redshift 叢集是否可公開存取。它會評估叢集組態項目中的 PubliclyAccessible 欄位。

Amazon Redshift 叢集組態的 PubliclyAccessible 屬性會指出叢集是否可公開存取。當叢集 PubliclyAccessible 設定為 true，它是面向網際網路的執行個體，其具有可公開解析的 DNS 名稱，可解析為公有 IP 地址。

當叢集無法公開存取時，它是內部執行個體，其具有解析為私有 IP 地址的 DNS 名稱。除非您打算讓叢集可公開存取，否則叢集不應 PubliclyAccessible 設定為 true。

修補

若要更新 Amazon Redshift 叢集以停用公開存取，請參閱《Amazon Redshift 管理指南》中的[修改叢集](#)。將可公開存取設定為否。

【Redshift.2】與 Amazon Redshift 叢集的連線應在傳輸中加密

相關要求：NIST.800-53.r5 AC-4、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23、NIST.800-53.r5 SC-23(3)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-8、NIST.800-53.r5 SC-8(1)、NIST.800-53.r5 SC-8(2)、PCI DSS v4.0.1/4.2.1

類別：保護 > 資料保護 > data-in-transit

嚴重性：中

資源類型：AWS::Redshift::Cluster AWS::Redshift::ClusterParameterGroup

AWS Config 規則：[redshift-require-tls-ssl](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否需要連線至 Amazon Redshift 叢集，才能使用傳輸中的加密。如果 Amazon Redshift 叢集參數 `require_ssl` 未設定為 `True`，則檢查會失敗。

TLS 可用來協助防止潛在攻擊者使用 person-in-the-middle 或類似攻擊來竊聽或操控網路流量。應只允許透過 TLS 的加密連線。加密傳輸中的資料可能會影響效能。您應該使用此功能測試應用程式，以了解效能描述檔和 TLS 的影響。

修補

若要將 Amazon Redshift 參數群組更新為需要加密，請參閱《Amazon Redshift 管理指南》中的 [修改參數群組](#)。將 `require_ssl` 設定為 `True`。

【Redshift.3】 Amazon Redshift 叢集應該啟用自動快照

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-13(5)

類別：復原 > 恢復 > 備份已啟用

嚴重性：中

資源類型：AWS::Redshift::Cluster

AWS Config 規則：[redshift-backup-enabled](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
MinRetentionPeriod	最短快照保留期間，以天為單位	Integer	7 至 35	7

此控制項會檢查 Amazon Redshift 叢集是否已啟用自動快照，以及大於或等於指定時間範圍的保留期間。如果叢集未啟用自動快照，或保留期間小於指定的時間範圍，則控制項會失敗。除非您提供快照保留期間的自訂參數值，否則 Security Hub CSPM 會使用預設值 7 天。

備份可協助您更快地從安全事件中復原。它們可增強您系統的彈性。根據預設，Amazon Redshift 會定期拍攝快照。此控制項會檢查是否啟用自動快照並保留至少七天。如需 Amazon Redshift 自動化快照的詳細資訊，請參閱《Amazon Redshift 管理指南》中的[自動化快照](#)。

修補

若要更新 Amazon Redshift 叢集的快照保留期，請參閱《Amazon Redshift 管理指南》中的[修改叢集](#)。對於備份，將快照保留值設定為 7 或更高。

【Redshift.4】 Amazon Redshift 叢集應該啟用稽核記錄

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.2.1

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::Redshift::Cluster

AWS Config rule：redshift-cluster-audit-logging-enabled (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Redshift 叢集是否已啟用稽核記錄。

Amazon Redshift 稽核記錄提供叢集中連線和使用者活動的其他資訊。此資料可以在 Amazon S3 中存放和保護，並有助於安全稽核和調查。如需詳細資訊，請參閱《Amazon Redshift 管理指南》中的[資料庫稽核記錄](#)。

修補

若要設定 Amazon Redshift 叢集的稽核記錄，請參閱《Amazon Redshift 管理指南》中的[使用主控台設定稽核](#)。

【Redshift.6】 Amazon Redshift 應已啟用主要版本的自動升級

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)

類別：識別 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：AWS::Redshift::Cluster

AWS Config 規則：[redshift-cluster-maintenancesettings-check](#)

排程類型：已觸發變更

參數：

- allowVersionUpgrade = true (不可自訂)

此控制項會檢查是否已為 Amazon Redshift 叢集啟用自動主要版本升級。

啟用自動主要版本升級可確保在維護時段期間安裝 Amazon Redshift 叢集的最新主要版本更新。這些更新可能包括安全性修補程式和錯誤修正。隨時掌握修補程式安裝的最新資訊，是保護系統安全的重要步驟。

修補

若要從修復此問題 AWS CLI，請使用 Amazon Redshift `modify-cluster` 命令，並設定 `--allow-version-upgrade` 屬性。`clustername` 是 Amazon Redshift 叢集的名稱。

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

【Redshift.7】 Redshift 叢集應使用增強型 VPC 路由

相關需求：NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7(21)、NIST.800-53.r5 SC-7(4)、NIST.800-53.r5 SC-7(9)

類別：保護 > 安全網路組態 > API 私有存取

嚴重性：中

資源類型：AWS::Redshift::Cluster

AWS Config 規則：[redshift-enhanced-vpc-routing-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Redshift 叢集是否EnhancedVpcRouting已啟用。

增強型 VPC 路由會強制叢集COPY和資料儲存庫之間的所有 和 UNLOAD流量通過您的 VPC。然後，您可以使用安全群組和網路存取控制清單等 VPC 功能來保護網路流量的安全。您也可以使用 VPC 流程日誌來監控網路流量。

修補

如需詳細修復指示，請參閱《Amazon Redshift 管理指南》中的[啟用增強型 VPC 路由](#)。

【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

類別：識別 > 資源組態

嚴重性：中

資源類型：AWS::Redshift::Cluster

AWS Config 規則：[redshift-default-admin-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Redshift 叢集是否已從其預設值變更管理員使用者名稱。如果 Redshift 叢集的管理員使用者名稱設定為 `awsuser`，則此控制項會失敗。

建立 Redshift 叢集時，您應該將預設管理員使用者名稱變更為唯一值。預設使用者名稱是公有知識，應在組態時變更。變更預設使用者名稱可降低意外存取的風險。

修補

您無法在建立 Amazon Redshift 叢集之後變更其管理員使用者名稱。若要使用非預設使用者名稱建立新的叢集，請參閱 [《Amazon Redshift 入門指南》中的步驟 1：建立範例 Amazon Redshift 叢集](#)。

【Redshift.10】 應靜態加密 Redshift 叢集

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::Redshift::Cluster

AWS Config 規則：[redshift-cluster-kms-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon Redshift 叢集是否靜態加密。如果 Redshift 叢集未靜態加密，或加密金鑰與規則參數中提供的金鑰不同，則控制項會失敗。

在 Amazon Redshift 中，您可以為您的叢集開啟資料庫加密，以協助保護靜態資料。開啟叢集的加密時，叢集和其快照的資料區塊和系統中繼資料會加密。靜態資料加密是建議的最佳實務，因為它會為您的資料新增一層存取管理。加密靜態 Redshift 叢集可降低未經授權的使用者可以存取儲存在磁碟上的資料的風險。

修補

若要修改 Redshift 叢集以使用 KMS 加密，請參閱《Amazon Redshift 管理指南》中的[變更叢集加密](#)。

【Redshift.11】 應標記 Redshift 叢集

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Redshift::Cluster

AWS Config rule：tagged-redshift-cluster (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1-6 個符合 AWS 要求 的標籤金鑰。	No default value

此控制項會檢查 Amazon Redshift 叢集是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果叢集沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果叢集未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《[標記您的 AWS 資源](#)》中的 [AWS 一般參考](#)。

修補

若要將標籤新增至 Redshift 叢集，請參閱 [《Amazon Redshift 管理指南》中的在 Amazon Redshift 中標記資源](#)。

【Redshift.12】應標記 Redshift 事件通知訂閱

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Redshift::EventSubscription

AWS Config rule : tagged-redshift-eventsubscription (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	No default value

此控制項會檢查 Amazon Redshift 叢集快照是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果叢集快照沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果叢集快照未標記任何索引鍵，則 會失敗。系統會 aws: 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS ?](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Redshift 事件通知訂閱，請參閱《[Amazon Redshift 管理指南](#)》中的在 [Amazon Redshift 中標記資源](#)。

【Redshift.13】應標記 Redshift 叢集快照

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Redshift::ClusterSnapshot

AWS Config rule：tagged-redshift-clustersnapshot (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon Redshift 叢集快照是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果叢集快照沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果叢集快照未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Redshift 叢集快照，請參閱 [《Amazon Redshift 管理指南》](#) 中的在 Amazon Redshift 中標記資源。

【Redshift.14】應標記 Redshift 叢集子網路群組

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Redshift::ClusterSubnetGroup

AWS Config rule：tagged-redshift-clustersubnetgroup (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon Redshift 叢集子網路群組是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果叢集子網路群組沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果叢集子網路群組未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱 [《IAM 使用者指南》](#) 中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Redshift 叢集子網路群組，請參閱 [《Amazon Redshift 管理指南》中的在 Amazon Redshift 中標記資源](#)。

【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠

相關要求：PCI DSS v4.0.1/1.3.1

類別：保護 > 安全網路組態 > 安全群組組態

嚴重性：高

資源類型：AWS::Redshift::Cluster

AWS Config 規則：[redshift-unrestricted-port-access](#)

排程類型：定期

參數：無

此控制項會檢查與 Amazon Redshift 叢集相關聯的安全群組是否具有允許從網際網路 (0.0.0.0/0 或 ::/0) 存取叢集連接埠的輸入規則。如果安全群組傳入規則允許從網際網路存取叢集連接埠，則控制項會失敗。

允許不受限制的傳入存取 Redshift 叢集連接埠 (IP 地址加上 /0 尾碼) 可能會導致未經授權的存取或安全事件。我們建議您在建立安全群組和設定傳入規則時，套用最低權限存取的主體。

修補

若要將 Redshift 叢集連接埠上的輸入限制為受限原始伺服器，請參閱 [《Amazon VPC 使用者指南》中的使用安全群組規則](#)。更新連接埠範圍符合 Redshift 叢集連接埠且 IP 連接埠範圍為 0.0.0.0/0 的規則。

【Redshift.16】 Redshift 叢集子網路群組應具有來自多個可用區域的子網路

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::Redshift::ClusterSubnetGroup

AWS Config 規則：[redshift-cluster-subnet-group-multi-az](#)

排程類型：已觸發變更

參數：無

控制項會檢查 Amazon Redshift 叢集子網路群組是否有來自多個可用區域 (AZ) 的子網路。如果叢集子網路群組沒有至少兩個不同 AZs 子網路，則控制項會失敗。

跨多個 AZs 設定子網路有助於確保您的 Redshift 資料倉儲可以繼續操作，即使發生故障事件也一樣。

修補

若要修改 Redshift 叢集子網路群組以跨越多個 AZs，請參閱《Amazon Redshift 管理指南》中的[修改叢集子網路群組](#)。

【Redshift.17】 應標記 Redshift 叢集參數群組

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Redshift::ClusterParameterGroup

AWS Config 規則：[redshift-cluster-parameter-group-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon Redshift 叢集參數群組是否具有 `requiredKeyTags` 參數指定的標籤索引鍵。如果參數群組沒有任何標籤索引鍵，或沒有 `requiredKeyTags` 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 `requiredKeyTags` 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果參數群組沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 `aws:` 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需有關將標籤新增至 Amazon Redshift 叢集參數群組的資訊，請參閱《[Amazon Redshift 管理指南](#)》中的在 [Amazon Redshift 中標記資源](#)。

【Redshift.18】 Redshift 叢集應啟用異地同步備份部署

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::Redshift::Cluster

AWS Config 規則：[redshift-cluster-multi-az-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已為 Amazon Redshift 叢集啟用多個可用區域（多可用區域）部署。如果未為 Amazon Redshift 叢集啟用異地同步備份部署，則控制項會失敗。

Amazon Redshift 支援佈建叢集的多個可用區域（多可用區域）部署。如果為叢集啟用異地同步備份部署，當可用區域 (AZ) 發生意外事件時，Amazon Redshift 資料倉儲可以在失敗情況下繼續操作。異

地同步備份部署會在多個異地同步備份中部署運算資源，而且可以透過單一端點存取這些運算資源。如果整個 AZ 失敗，則另一個 AZ 中的剩餘運算資源可用於繼續處理工作負載。您可以將現有的單一可用區資料倉儲轉換為多可用區資料倉儲。其他運算資源接著會佈建在第二個可用區域中。

修補

如需為 Amazon Redshift 叢集設定異地同步備份部署的相關資訊，請參閱《Amazon Redshift 管理指南》中的[將單一異地同步備份資料倉儲轉換為異地同步備份資料倉儲](#)。

Amazon Redshift Serverless 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Redshift Serverless 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【RedshiftServerless.1】Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由

類別：保護 > 安全網路組態 > VPC 內的資源

嚴重性：高

資源類型：AWS::RedshiftServerless::Workgroup

AWS Config 規則：[redshift-serverless-workgroup-routes-within-vpc](#)

排程類型：定期

參數：無

此控制項會檢查是否已為 Amazon Redshift Serverless 工作群組啟用增強型 VPC 路由。如果工作群組的增強型 VPC 路由已停用，則控制項會失敗。

如果停用 Amazon Redshift Serverless 工作群組的增強型 VPC 路由，Amazon Redshift 會透過網際網路路由流量，包括網路中其他服務的流量 AWS。如果您為工作群組啟用增強型 VPC 路由，Amazon Redshift 會根據 Amazon VPC 服務，透過虛擬私有雲端 (VPC) 強制叢集與資料儲存庫之間的所有 COPY 和 UNLOAD 流量。透過增強型 VPC 路由，您可以使用標準 VPC 功能來控制 Amazon Redshift 叢集和其他資源之間的資料流程。這包括 VPC 安全群組和端點政策、網路存取控制清單 (ACLs) 和網域名稱系統 (DNS) 伺服器等功能。您也可以使用 VPC 流程日誌來監控 COPY 和 UNLOAD 流量。

修補

如需增強型 VPC 路由以及如何為工作群組啟用它的詳細資訊，請參閱《Amazon Redshift 管理指南》中的[使用 Redshift 增強型 VPC 路由控制網路流量](#)。

【RedshiftServerless.2】必須使用 SSL 連線到 Redshift Serverless 工作群組

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::RedshiftServerless::Workgroup

AWS Config 規則：[redshift-serverless-workgroup-encrypted-in-transit](#)

排程類型：定期

參數：無

此控制項會檢查是否需要與 Amazon Redshift Serverless 工作群組的連線，才能加密傳輸中的資料。如果工作群組的require_ssl組態參數設定為 false，則控制項會失敗。

Amazon Redshift Serverless 工作群組是運算資源的集合，可將運算資源分組，例如 RPU、VPC 子網路群組和安全群組。工作群組的屬性包括網路和安全設定。這些設定指定是否需要連線到工作群組，才能使用 SSL 來加密傳輸中的資料。

修補

如需將 Amazon Redshift Serverless 工作群組的設定更新為需要 SSL 連線的相關資訊，請參閱《[Amazon Redshift 管理指南](#)》中的連線至 Amazon Redshift Serverless。

【RedshiftServerless.3】Redshift Serverless 工作群組應禁止公開存取

類別：保護 > 安全網路組態 > 不可公開存取的資源

嚴重性：高

資源類型：AWS::RedshiftServerless::Workgroup

AWS Config 規則：[redshift-serverless-workgroup-no-public-access](#)

排程類型：定期

參數：無

此控制項會檢查是否停用 Amazon Redshift Serverless 工作群組的公有存取。它會評估 Redshift Serverless 工作群組的 publiclyAccessible 屬性。如果工作群組的公有存取已啟用 (true)，則控制項會失敗。

Amazon Redshift Serverless 工作群組的公有存取 (publiclyAccessible) 設定會指定工作群組是否可以從公有網路存取。如果工作群組的公有存取已啟用 (true)，Amazon Redshift 會建立彈性 IP 地址，讓工作群組可從 VPC 外部公開存取。如果您不希望工作群組可公開存取，請停用其公開存取。

修補

如需有關變更 Amazon Redshift Serverless 工作群組公有存取設定的資訊，請參閱《Amazon Redshift 管理指南》中的[檢視工作群組的屬性](#)。

【RedshiftServerless.4】Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys

相關要求：NIST.800-53.r5 AU-9、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::RedshiftServerless::Namespace

AWS Config 規則：[redshift-serverless-namespace-cmk-encryption](#)

排程類型：定期

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
kmsKeyArns	AWS KMS keys 要包含在評估中的 Amazon Resource Name (ARNs)清單。如果 Redshift Serverless 命名空間未使用清單中的 KMS 金鑰加密，控制項會	StringList (最多 3 個項目)	現有 KMS 金鑰的 1–3 ARNs。例如：arn:aws:kms:us-west-2:11112223333:kms:us-west-2:11112223333:key/1234abcd-12ab-34cd-56ef-	無預設值

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
	產生FAILED問題清單。		123456789 0ab 。	

此控制項會檢查 Amazon Redshift Serverless 命名空間是否使用客戶受管的靜態加密 AWS KMS key。如果 Redshift Serverless 命名空間未使用客戶受管 KMS 金鑰加密，則控制項會失敗。您可以選擇性地為控制項指定要包含在評估中的 KMS 金鑰清單。

在 Amazon Redshift Serverless 中，命名空間會定義資料庫物件的邏輯容器。此控制項會定期檢查命名空間的加密設定是否指定客戶受管 AWS KMS key，而非 AWS 受管 KMS 金鑰，以加密命名空間中的資料。使用客戶受管 KMS 金鑰，您可以完全控制金鑰。這包括定義和維護金鑰政策、管理授予、輪換密碼編譯材料、指派標籤、建立別名，以及啟用和停用金鑰。

修補

如需更新 Amazon Redshift Serverless 命名空間加密設定並指定客戶受管的詳細資訊 AWS KMS key，請參閱 [《Amazon Redshift 管理指南》中的變更命名空間 AWS KMS key 的](#)。

【RedshiftServerless.5】Redshift Serverless 命名空間不應使用預設的管理員使用者名稱

類別：識別 > 資源組態

嚴重性：中

資源類型：AWS::RedshiftServerless::Namespace

AWS Config 規則：[redshift-serverless-default-admin-check](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon Redshift Serverless 命名空間的管理員使用者名稱是否為預設的管理員使用者名稱 admin。如果 Redshift Serverless 命名空間的管理員使用者名為，則控制項會失敗admin。

建立 Amazon Redshift Serverless 命名空間時，您應該為命名空間指定自訂管理員使用者名稱。預設管理員使用者名為公有知識。例如，透過指定自訂管理員使用者名稱，您可以協助降低對命名空間的暴力攻擊風險或有效性。

修補

您可以使用 Amazon Redshift Serverless 主控台或 API 變更 Amazon Redshift Serverless 命名空間的管理員使用者名稱。若要使用主控台進行變更，請選擇命名空間組態，然後在動作功能表上選擇編輯管理員憑證。若要以程式設計方式變更，請使用 [UpdateNamespace](#) 操作，或者，如果您使用的是 AWS CLI，請執行 [update-namespace](#) 命令。如果您變更管理員使用者名稱，也必須同時變更管理員密碼。

【RedshiftServerless.6】Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::RedshiftServerless::Namespace

AWS Config 規則：[redshift-serverless-publish-logs-to-cloudwatch](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon Redshift Serverless 命名空間是否已設定為將連線和使用者日誌匯出至 Amazon CloudWatch Logs。如果未將 Redshift Serverless 命名空間設定為將日誌匯出至 CloudWatch Logs，則控制項會失敗。

如果您設定 Amazon Redshift Serverless 將連線日誌 (connectionlog) 和使用者日誌 (userlog) 資料匯出至 Amazon CloudWatch Logs 中的日誌群組，您可以將日誌記錄收集並存放在耐用的儲存體中，以支援安全性、存取和可用性檢閱和稽核。使用 CloudWatch Logs，您也可以執行日誌資料的即時分析，並使用 CloudWatch 建立警示和檢閱指標。

修補

若要將 Amazon Redshift Serverless 命名空間的日誌資料匯出至 Amazon CloudWatch Logs，必須在命名空間的稽核日誌組態設定中選取要匯出的個別日誌。如需更新這些設定的相關資訊，請參閱《Amazon Redshift 管理指南》中的[編輯安全性和加密](#)。

Route 53 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Route 53 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Route53.1】應標記 Route 53 運作狀態檢查

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Route53::HealthCheck

AWS Config rule：tagged-route53-healthcheck (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon Route 53 運作狀態檢查是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果運作狀態檢查沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果運作狀態檢查未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Route 53 運作狀態檢查，請參閱《Amazon Route 53 開發人員指南》中的[命名和標記運作狀態檢查](#)。

【Route53.2】Route 53 公有託管區域應記錄 DNS 查詢

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.8000-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.4.2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::Route53::HostedZone

AWS Config 規則：[route53-query-logging-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查是否已為 Amazon Route 53 公有託管區域啟用 DNS 查詢記錄。如果 Route 53 公有託管區域未啟用 DNS 查詢記錄，則控制項會失敗。

記錄 Route 53 託管區域的 DNS 查詢可解決 DNS 安全和合規要求，並授予可見性。日誌包含查詢的網域或子網域、查詢的日期和時間、DNS 記錄類型（例如 A 或 AAAA）和 DNS 回應代碼（例如 NoError 或 ServFail）。啟用 DNS 查詢記錄時，Route 53 會將日誌檔案發佈至 Amazon CloudWatch Logs。

修補

若要記錄 Route 53 公有託管區域的 DNS 查詢，請參閱《Amazon Route 53 開發人員指南》中的[設定 DNS 查詢的記錄](#)。

Amazon S3 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Simple Storage Service (Amazon S3) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定

相關要求： CIS AWS Foundations Benchmark v5.0.0/2.1.4、 CIS AWS Foundations Benchmark v3.0.0/2.1.4、 CIS AWS Foundations Benchmark v1.4.0/2.1.5、 NIST.800-53.r5 AC-21、 NIST.800-53.r5 AC-3、 NIST.800-53.r5 AC-3(7)、 NIST.800-53.r5 AC-4、 NIST.800-53.r5 AC-4(21)、 NIST.800-53.r5 AC-6、 NIST.800-53.r5 SC-7、 NIST.800-53.r5 SC-7)

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：[s3-account-level-public-access-blocks-periodic](#)

排程類型：定期

參數：

- ignorePublicAcls : true (不可自訂)
- blockPublicPolicy : true (不可自訂)
- blockPublicAcls : true (不可自訂)
- restrictPublicBuckets : true (不可自訂)

此控制項會檢查上述 Amazon S3 封鎖公有存取設定是否在 S3 一般用途儲存貯體的帳戶層級設定。如果一個或多個封鎖公開存取設定設定為 `false`，則控制項會失敗。

如果任何設定設定為 `false`，或如果任何設定未設定，則控制項會失敗。

Amazon S3 公有存取區塊旨在提供整個 AWS 帳戶 或個別 S3 儲存貯體層級的控制，以確保物件絕不具有公有存取。透過存取控制清單 (ACL)、儲存貯體政策或兩者來授予對儲存貯體和物件的公開存取許可。

除非您打算公開存取 S3 儲存貯體，否則您應該設定帳戶層級的 Amazon S3 封鎖公開存取功能。

若要進一步了解，請參閱 [《Amazon Simple Storage Service 使用者指南》](#) 中的 [使用 Amazon S3 封鎖公開存取](#)。

修補

若要為您的 啟用 Amazon S3 封鎖公開存取 AWS 帳戶，請參閱《Amazon Simple Storage Service 使用者指南》中的 [為您的帳戶設定封鎖公開存取設定](#)。

【S3.2】 S3 一般用途儲存貯體應封鎖公開讀取存取

相關要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-40-53.r50 NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-bucket-public-read-prohibited](#)

排程類型：定期觸發和變更

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否允許公開讀取存取。系統會評估封鎖公開存取的設定、儲存貯體政策和儲存貯體存取控制清單 (ACL)。如果儲存貯體允許公有讀取存取，則控制項會失敗。

Note

如果 S3 儲存貯體具有儲存貯體政策，則此控制項不會評估使用萬用字元或變數的政策條件。若要產生 PASSED 調查結果，儲存貯體政策中的條件只能使用固定值，這些值不包含萬用字元或政策變數。如需政策變數的相關資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[變數和標籤](#)。

有些使用案例可能需要網際網路上的每個人都能從您的 S3 儲存貯體讀取。然而，這類情況很少見。為了確保資料的完整性和安全，您的 S3 儲存貯體不應允許公開讀取。

修補

若要封鎖 Amazon S3 儲存貯體上的公有讀取存取，請參閱《Amazon Simple Storage Service 使用者指南》中的[設定 S3 儲存貯體的封鎖公有存取設定](#)。

【S3.3】 S3 一般用途儲存貯體應封鎖公有寫入存取

相關要求：PCI DSS v3.2.1/1.2.1、PCI DSS v3.2.1/1.3.1、PCI DSS v3.2.1/1.3.2、PCI DSS v3.2.1/1.3.4、PCI DSS v3.2.1/1.3.6、PCI DSS v3.2.1/7.2.1、NIST.800-53.r5 AC-21、NIST.800-53.r5

AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4(2)、NIST.800-53.r5 AC-65.r5
AC-4 NIST.800-53.r5 SC-7

類別：保護 > 安全網路組態

嚴重性：嚴重

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-bucket-public-write-prohibited](#)

排程類型：定期觸發和變更

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否允許公有寫入存取。系統會評估封鎖公開存取的設定、儲存貯體政策和儲存貯體存取控制清單 (ACL)。如果儲存貯體允許公有寫入存取，則控制項會失敗。

Note

如果 S3 儲存貯體具有儲存貯體政策，則此控制項不會評估使用萬用字元或變數的政策條件。若要產生 PASSED 調查結果，儲存貯體政策中的條件只能使用固定值，這些值不包含萬用字元或政策變數。如需政策變數的相關資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的[變數和標籤](#)。

某些使用案例需要網際網路上的每個人都能夠寫入您的 S3 儲存貯體。然而，這類情況很少見。為了確保資料的完整性和安全，您的 S3 儲存貯體不應允許公開寫入。

修補

若要封鎖 Amazon S3 儲存貯體上的公有寫入存取，請參閱《Amazon Simple Storage Service 使用者指南》中的[設定 S3 儲存貯體的封鎖公有存取設定](#)。

【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL

相關要求：CIS AWS Foundations Benchmark v5.0.0/2.1.1、CIS AWS Foundations Benchmark v3.0.0/2.1.1、CIS AWS Foundations Benchmark v1.4.0/2.1.2、NIST.800-53.r5 AC-17(2)、NIST.800-53.r5 AC-4、NIST.800-53.r5 IA-5(1)、NIST.800-53.r5

SC-12(3)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-23-SC-23NIST.800-53.r5 SC-7
NIST.800-53.r5 SC-8 SI-7 3.13.15

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-bucket-ssl-requests-only](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否有需要請求才能使用 SSL 的政策。如果儲存貯體政策不需要使用 SSL 的請求，則控制項會失敗。

S3 儲存貯體應具有要求所有請求 (Action: S3:*) 在 S3 資源政策中僅接受透過 HTTPS 傳輸資料的政策，以條件索引鍵表示aws:SecureTransport。

修補

若要更新 Amazon S3 儲存貯體政策以拒絕不安全的傳輸，請參閱 [《Amazon Simple Storage Service 使用者指南》](#) 中的使用 Amazon S3 主控台新增儲存貯體政策。

新增類似於下列政策的政策陳述式。amzn-s3-demo-bucket 將取代為您修改的儲存貯體名稱。

JSON

```
{
  "Id": "ExamplePolicy",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSSLRequestsOnly",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
```

```
        "Bool": {
            "aws:SecureTransport": "false"
        },
        "Principal": "*"
    }
}
```

如需詳細資訊，請參閱[我應該使用哪些 S3 儲存貯體政策來符合 AWS Config 規則 s3-bucket-ssl-requests-only](#)？AWS 官方知識中心。

【S3.6】 S3 一般用途儲存貯體政策應限制對其他 的存取 AWS 帳戶

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-171.r2 3.13.4

類別：保護 > 安全存取管理 > 敏感 API 操作動作受限

嚴重性：高

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-bucket-blacklisted-actions-prohibited](#)

排程類型：已觸發變更

參數：

- blacklistedactionpatterns : s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl (不可自訂)

此控制項會檢查 Amazon S3 一般用途儲存貯體政策是否阻止委託 AWS 帳戶 人對 S3 儲存貯體中的資源執行拒絕的動作。如果儲存貯體政策允許另一個 中委託人的一個或多個上述動作，則控制項會失敗 AWS 帳戶。

實作最低權限存取對於降低安全風險以及錯誤或惡意意圖的影響至關重要。如果 S3 儲存貯體政策允許從外部帳戶存取，可能會導致內部威脅或攻擊者資料外洩。

blacklistedactionpatterns 參數允許成功評估 S3 儲存貯體的規則。參數會將未包含在blacklistedactionpatterns清單中的動作模式存取權授予外部帳戶。

修補

若要更新 Amazon S3 儲存貯體政策以移除許可，請參閱《Amazon Simple Storage Service 使用者指南》中的[使用 Amazon S3 主控台新增儲存貯體政策](#)。

在編輯儲存貯體政策頁面的政策編輯文字方塊中，採取下列其中一個動作：

- 移除授予其他拒絕動作 AWS 帳戶 存取權的陳述式。
- 從陳述式中移除允許的拒絕動作。

【S3.7】 S3 一般用途儲存貯體應使用跨區域複寫

相關要求：PCI DSS v3.2.1/2.2、NIST.800-53.r5 AU-9(2)、NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-36(2)、NIST.800-53.r5 SC-5(2)、NIST.8000-5.r5 SI-13(5)

類別：保護 > 安全存取管理

嚴重性：低

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-bucket-cross-region-replication-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否已啟用跨區域複寫。如果儲存貯體未啟用跨區域複寫，則控制項會失敗。

複寫是在相同或不同的儲存貯體之間自動非同步複製物件 AWS 區域。複寫會將新建立的物件和物件更新從來源儲存貯體複製到目的地儲存貯體。AWS 最佳實務建議對相同擁有的來源和目的地儲存貯體進行複寫 AWS 帳戶。除了可用性之外，建議您考慮其他系統強化設定。

如果複寫目的地儲存貯體未啟用跨區域複寫，則此控制項會產生其 FAILED 調查結果。如果目的地儲存貯體不需要啟用跨區域複寫的合法原因，您可以隱藏此儲存貯體的問題清單。

修補

若要在 S3 儲存貯體上啟用跨區域複寫，請參閱《Amazon Simple Storage Service 使用者指南》中的[為相同帳戶擁有的來源和目的地儲存貯體設定複寫](#)。針對來源儲存貯體，選擇套用至儲存貯體中的所有物件。

【S3.8】 S3 一般用途儲存貯體應封鎖公開存取

相關要求：CIS AWS Foundations Benchmark v5.0.0/2.1.4、CIS AWS Foundations Benchmark v3.0.0/2.1.4、CIS AWS Foundations Benchmark v1.4.0/2.1.5、NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7。 NIST.800-53.r5 SC-7

類別：保護 > 安全存取控制 > 存取控制

嚴重性：高

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-bucket-level-public-access-prohibited](#)

排程類型：已觸發變更

參數：

- `excludedPublicBuckets`（不可自訂）– 以逗號分隔的已知允許公有 S3 儲存貯體名稱清單

此控制項會檢查 Amazon S3 一般用途儲存貯體是否封鎖儲存貯體層級的公開存取。如果下列任一設定設定為 `false`，則控制項會失敗：

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

S3 儲存貯體層級的封鎖公開存取提供控制項，以確保物件絕不具有公開存取。透過存取控制清單 (ACL)、儲存貯體政策或兩者來授予對儲存貯體和物件的公開存取許可。

除非您打算公開存取 S3 儲存貯體，否則您應該設定儲存貯體層級的 Amazon S3 封鎖公開存取功能。

修補

如需有關如何在儲存貯體層級移除公有存取權的資訊，請參閱 [《Amazon S3 使用者指南》中的封鎖對 Amazon S3 儲存體的公有存取權](#)。 Amazon S3

【S3.9】 S3 一般用途儲存貯體應啟用伺服器存取記錄

相關要求：NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7 SI-3 SI-4 SI-710.2.1

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-bucket-logging-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已為 Amazon S3 一般用途儲存貯體啟用伺服器存取記錄。如果未啟用伺服器存取記錄，則控制項會失敗。啟用記錄功能時，Amazon S3 會將來源儲存貯體的存取日誌傳送到選擇的目標儲存貯體。目標儲存貯體必須與來源儲存貯體位於相同的 AWS 區域中，且不得設定預設保留期。目標記錄儲存貯體不需要啟用伺服器存取記錄，而且您應該隱藏此儲存貯體的問題清單。

伺服器存取記錄提供對儲存貯體提出之請求的詳細記錄。伺服器存取日誌可協助安全和存取稽核。如需詳細資訊，請參閱 [Amazon S3 的安全最佳實務：啟用 Amazon S3 伺服器存取記錄](#)。

修補

若要啟用 Amazon S3 伺服器存取記錄，請參閱 [《Amazon S3 使用者指南》中的啟用 Amazon S3 伺服器存取記錄](#)。Amazon S3

【S3.10】 已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態

相關需求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-version-lifecycle-policy-check](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon S3 一般用途版本控制的儲存貯體是否具有生命週期組態。如果儲存貯體沒有生命週期組態，則控制項會失敗。

建議您為 S3 儲存貯體建立生命週期組態，以協助您定義您希望 Amazon S3 在物件生命週期內採取的動作。

 Tip

在沒有生命週期管理的情況下啟用版本控制可能會導致儲存成長不受限制並增加成本。每次物件修改都會建立無限期保留的新版本。設定 S3 生命週期規則，以自動將非最新版本轉換為更便宜的儲存類別，或在定義的保留期間後使它們過期。

修補

如需在 Amazon S3 儲存貯體上設定生命週期的詳細資訊，請參閱《Amazon [S3 使用者指南](#)》中的[使用 S3 版本控制搭配 S3 生命週期](#)、在[儲存貯體上設定生命週期組態](#)，以及[管理物件的生命週期](#)。

【S3.11】 S3 一般用途儲存貯體應啟用事件通知

相關需求：NIST.800-53.r5 CA-7、NIST.800-53.r5 SI-3(8)、NIST.800-53.r5 SI-4、NIST.800-53.r5 SI-4(4)、NIST.800-171.r2 3.3.8

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-event-notifications-enabled](#)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
eventTypes	偏好的 S3 事件類型清單	EnumList (最多 28 個項目)	s3: IntelligentTiering, s3:LifecycleExpiration:*, s3:LifecycleExpiration:Delete, s3:LifecycleExpiration:DeleteMarkerCreated, s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, , s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:P	無預設值

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
			ost, s3:Object Created:Put, s3:Object Removed:* , s3:Object Removed:Delete, s3:Object Removed:DeleteMark erCreated , s3:Object Restore:* , s3:Object Restore:Completed, s3:Object Restore:Delete, s3:Object Restore:Post, s3:Object Tagging:* , s3:Object Tagging:Delete,	

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
			s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold, s3:TestEvent	

此控制項會檢查 Amazon S3 一般用途儲存貯體上是否啟用 S3 事件通知。Amazon S3 如果未在儲存貯體上啟用 S3 事件通知，則控制項會失敗。如果您為 `eventTypes` 參數提供自訂值，則只有在為指定類型的事件啟用事件通知時，控制項才會傳遞。

當您啟用 S3 事件通知時，您會在發生影響 S3 儲存貯體的特定事件時收到提醒。例如，您可以收到物件建立、物件移除和物件還原的通知。這些通知可以提醒相關團隊，可能導致未經授權的資料存取的意外或刻意修改。

修補

如需有關偵測 S3 儲存貯體和物件變更的資訊，請參閱 [《Amazon S3 使用者指南》中的 Amazon S3 事件通知](#)。Amazon S3

【S3.12】 ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6

類別：保護 > 安全存取控制 > 存取控制

嚴重性：中

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-bucket-acl-prohibited](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否提供具有存取控制清單 (ACL) 的使用者許可。如果 ACL 設定為管理儲存貯體上的使用者存取權，則控制項會失敗。

ACLs 是早於 IAM 的舊版存取控制機制。建議使用 S3 儲存貯體政策或 AWS Identity and Access Management (IAM) 政策來管理對 S3 儲存貯體的存取，而不是 ACLs。

修補

若要傳遞此控制項，您應該停用 S3 儲存貯體 ACLs。如需說明，請參閱 [《Amazon Simple Storage Service 使用者指南》中的 控制物件的擁有權和停用儲存貯體 ACLs](#)。

若要建立 S3 儲存貯體政策，請參閱[使用 Amazon S3 主控台新增儲存貯體政策](#)。若要在 S3 儲存貯體上建立 IAM 使用者政策，請參閱[使用使用者政策控制對儲存貯體的存取](#)。

【S3.13】 S3 一般用途儲存貯體應具有生命週期組態

相關需求：NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-13(5)

類別：保護 > 資料保護

嚴重性：低

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-lifecycle-policy-check](#)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
targetTransitionDays	當物件轉換為指定的儲存類別時，物件建立後的天數	Integer	1 至 36500	無預設值
targetExpirationDays	刪除物件時，物件建立後的天數	Integer	1 至 36500	無預設值
targetTransitionStorageClasses	目的地 S3 儲存類別類型	列舉	STANDARD_IA, INTELLIGENT_TIERING, ONEZONE_IA, GLACIER, GLACIER_IR,	無預設值

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
			DEEP_ARCHIVE	

此控制項會檢查 Amazon S3 一般用途儲存貯體是否具有生命週期組態。如果儲存貯體沒有生命週期組態，則控制項會失敗。如果您為上述一或多個參數提供自訂值，則只有在政策包含指定的儲存類別、刪除時間或轉換時間時，控制項才會通過。

為 S3 儲存貯體建立生命週期組態會定義您希望 Amazon S3 在物件生命週期內採取的動作。例如，您可以將物件轉換至另一個儲存類別、封存物件，或在指定的期間內刪除物件。

修補

如需有關在 Amazon S3 儲存貯體上設定生命週期政策的資訊，請參閱在[儲存貯體上設定生命週期組態](#)，以及《Amazon S3 使用者指南》中的[管理您的儲存生命週期](#)。

【S3.14】 S3 一般用途儲存貯體應該已啟用版本控制

類別：保護 > 資料保護 > 資料刪除保護

相關要求：NIST.800-53.r5 AU-9(2)、NIST.800-53.r5 CP-10、NIST.800-53.r5 CP-6、NIST.800-53.r5 CP-6(1)、NIST.800-53.r5 CP-6(2)、NIST.800-53.r5 CP-9、NIST.800-53.r5 SC-5(2)、NIST.800-53.r5 SI-12、NIST.800-53.r5 SI-13(5)、NIST.800-171.r2 3.83.

嚴重性：低

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-bucket-versioning-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否已啟用版本控制。如果儲存貯體的版本控制已暫停，則控制項會失敗。

版本控制會將物件的多個變體保留在相同的 S3 儲存貯體中。您可以使用版本控制來保留、擷取和還原存放在 S3 儲存貯體中的所有物件版本。版本控制可協助您從意外的使用者動作和應用程式失敗中復原。

Tip

在沒有生命週期管理的情況下啟用版本控制可能會導致儲存成長不受限制並增加成本。每次物件修改都會建立無限期保留的新版本。設定 S3 生命週期規則，以自動將非最新版本轉換為更便宜的儲存類別，或在定義的保留期間後使它們過期。如需詳細資訊，請參閱[搭配 S3 生命週期使用 S3 版本控制](#)和管理[物件的生命週期](#)。

修補

若要在 S3 儲存貯體上使用版本控制，請參閱《Amazon S3 使用者指南》中的在[儲存貯體上啟用版本控制](#)。

【S3.15】 S3 一般用途儲存貯體應啟用物件鎖定

類別：保護 > 資料保護 > 資料刪除保護

相關要求：NIST.800-53.r5 CP-6(2)、PCI DSS v4.0.1/10.5.1

嚴重性：中

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-bucket-default-lock-enabled](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
mode	S3 物件鎖定保留模式	列舉	GOVERNANCE , COMPLIANCE	無預設值

此控制項會檢查 Amazon S3 一般用途儲存貯體是否已啟用物件鎖定。如果未針對儲存貯體啟用物件鎖定，則控制項會失敗。如果您為 mode 參數提供自訂值，則只有在 S3 物件鎖定使用指定的保留模式時，控制項才會通過。

您可以使用 S3 物件鎖定搭配「單寫多讀」(WORM) 模型來存放物件。物件鎖定有助於防止 S3 儲存貯體中的物件在固定時間內或無限期遭到刪除或覆寫。您可以使用 S3 物件鎖定，以滿足必須使用 WORM 儲存體的法規要求，或多加一道保護以免物件遭到變更和刪除。

修補

若要為新的和現有的 S3 儲存貯體設定物件鎖定，請參閱《Amazon [S3 使用者指南](#)》中的設定 S3 物件鎖定。 Amazon S3

【S3.17】 S3 一般用途儲存貯體應使用 靜態加密 AWS KMS keys

類別：保護 > 資料保護 > data-at-rest加密

相關要求：NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 SI-7(6)、NIST.800-53.r5 AU-9、NIST.800-17171.r2 1.800 3.13.11 3.13.16

嚴重性：中

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-default-encryption-kms](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon S3 一般用途儲存貯體是否使用 AWS KMS key (SSE-KMS 或 DSSE-KMS) 加密。如果使用預設加密 (SSE-S3) 加密儲存貯體，則控制項會失敗。

伺服器端加密 (SSE) 是接收資料的應用程式或服務在其目的地對資料的加密。除非您另有指定，否則 S3 儲存貯體預設會使用 Amazon S3 受管金鑰 (SSE-S3) 進行伺服器端加密。不過，若要新增控制項，您可以選擇將儲存貯體設定為使用伺服器端加密搭配 AWS KMS keys (SSE-KMS 或 DSSE-KMS)。Amazon S3 會在將資料寫入 AWS 資料中心的磁碟時，在物件層級加密資料，並在您存取資料時將其解密。

修補

若要使用 SSE-KMS 加密 S3 儲存貯體，請參閱《Amazon S3 使用者指南》中的[使用 AWS KMS \(SSE-KMS\) 指定伺服器端加密](#)。若要使用 DSSE-KMS 加密 S3 儲存貯體，請參閱《Amazon S3 使用者指南》中的[使用 AWS KMS keys \(DSSE-KMS\) 指定雙層伺服器端加密](#)。

【S3.19】 S3 存取點應啟用封鎖公開存取設定

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全存取管理 > 資源不可公開存取

嚴重性：嚴重

資源類型：AWS::S3::AccessPoint

AWS Config 規則：[s3-access-point-public-access-blocks](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon S3 存取點是否已啟用封鎖公開存取設定。如果未為存取點啟用封鎖公開存取設定，則控制項會失敗。

Amazon S3 封鎖公開存取功能可協助您在三個層級管理對 S3 資源的存取：帳戶、儲存貯體和存取點層級。每個層級的設定可以獨立設定，讓您可以為資料設定不同層級的公有存取限制。存取點設定無法個別覆寫較高層級的更嚴格設定（指派給存取點的帳戶層級或儲存貯體）。相反地，存取點層級的設定是累加的，這表示它們與其他層級的設定互補和搭配運作。除非您想要公開存取 S3 存取點，否則您應該啟用封鎖公開存取設定。

修補

Amazon S3 目前不支援在建立存取點後變更存取點的封鎖公開存取權限設定。當您建立新的存取點時，預設會啟用所有封鎖公開存取設定。建議您啟用所有設定，除非您知道您有特別需要停用任一設定。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[管理存取點的公有存取](#)。

【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除

相關要求：CIS AWS Foundations Benchmark v5.0.0/2.1.2、CIS AWS Foundations Benchmark v3.0.0/2.1.2、CIS AWS Foundations Benchmark v1.4.0/2.1.3、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-3、NIST.800-53.r5 SC-5(2)

類別：保護 > 資料保護 > 資料刪除保護

嚴重性：低

資源類型：AWS::S3::Bucket

AWS Config 規則：[s3-bucket-mfa-delete-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查是否已為 Amazon S3 一般用途儲存貯體啟用多重驗證 (MFA) 刪除。如果儲存貯體未啟用 MFA 刪除，則控制項會失敗。控制項不會針對具有生命週期組態的儲存貯體產生問題清單。

如果您啟用 S3 一般用途儲存貯體的版本控制，您可以選擇透過設定儲存貯體的 MFA 刪除來新增另一層安全性。如果您這樣做，儲存貯體擁有者必須在任何請求中包含兩種形式的身分驗證，以刪除儲存貯體中的物件版本或變更儲存貯體的版本控制狀態。例如，如果儲存貯體擁有者的安全登入資料遭到入侵，MFA 刪除可提供額外的安全性。MFA 刪除也有助於防止意外刪除儲存貯體，方法是要求啟動刪除動作的使用者使用 MFA 程式碼來證明 MFA 裝置的實體擁有，這會為刪除動作新增額外的摩擦層和安全性。

Note

只有在針對 S3 一般用途儲存貯體啟用 MFA 刪除時，此控制項才會產生 PASSED 調查結果。若要啟用儲存貯體的 MFA 刪除，也必須為儲存貯體啟用版本控制。儲存貯體版本控制是將 S3 物件的多種變化儲存在相同儲存貯體中的方法。此外，只有以根使用者身分登入的儲存貯體擁有者可以啟用 MFA 刪除，並在儲存貯體上執行刪除動作。您無法將 MFA 刪除與具有生命週期組態的儲存貯體搭配使用。

修補

如需有關啟用版本控制和設定 S3 儲存貯體 MFA 刪除的資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[設定 MFA 刪除](#)。

【S3.22】 S3 一般用途儲存貯體應記錄物件層級寫入事件

相關要求：CIS AWS Foundations Benchmark v5.0.0/3.8、CIS AWS Foundations Benchmark v3.0.0/3.8、PCI DSS v4.0.1/10.2.1

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：[cloudtrail-all-write-s3-data-event-check](#)

排程類型：定期

參數：無

此控制項會檢查 是否至少 AWS 帳戶 有一個 AWS CloudTrail 多區域線索，可記錄 Amazon S3 儲存貯體的所有寫入資料事件。如果帳戶沒有記錄 S3 儲存貯體寫入資料事件的多區域線索，則控制項會失敗。

S3 物件層級操作，例如 GetObject、DeleteObject 和 PutObject，稱為資料事件。根據預設，CloudTrail 不會記錄資料事件，但您可以設定追蹤來記錄 S3 儲存貯體的資料事件。當您啟用寫入資料事件的物件層級記錄時，您可以記錄 S3 儲存貯體中的每個個別物件（檔案）存取。啟用物件層級記錄可協助您符合資料合規要求、執行全面的安全分析、監控 中使用使用者行為的特定模式 AWS 帳戶，以及使用 Amazon CloudWatch Events 對 S3 儲存貯體中的物件層級 API 活動採取動作。如果您設定多區域線索來記錄所有 S3 儲存貯體的唯一讀或所有類型的資料事件，則此控制項會產生 PASSED 調查結果。

修補

若要啟用 S3 儲存貯體的物件層級記錄，請參閱《Amazon Simple Storage Service 使用者指南》中的 [啟用 S3 儲存貯體和物件的 CloudTrail 事件記錄](#)。

【S3.23】 S3 一般用途儲存貯體應記錄物件層級讀取事件

相關要求：CIS AWS Foundations Benchmark v5.0.0/3.9、CIS AWS Foundations Benchmark v3.0.0/3.9、PCI DSS v4.0.1/10.2.1

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：[cloudtrail-all-read-s3-data-event-check](#)

排程類型：定期

參數：無

此控制項會檢查 是否至少 AWS 帳戶 有一個 AWS CloudTrail 多區域線索，可記錄 Amazon S3 儲存貯體的所有讀取資料事件。如果帳戶沒有記錄 S3 儲存貯體讀取資料事件的多區域線索，則控制項會失敗。

S3 物件層級操作，例如 GetObject、DeleteObject 和 PutObject，稱為資料事件。根據預設，CloudTrail 不會記錄資料事件，但您可以設定追蹤來記錄 S3 儲存貯體的資料事件。當您為讀取資料事件啟用物件層級記錄時，您可以記錄 S3 儲存貯體中的每個個別物件（檔案）存取。啟用物件層級記錄可協助您符合資料合規要求、執行全面的安全分析、監控 中使用者行為的特定模式 AWS 帳戶，以及使用 Amazon CloudWatch Events 對 S3 儲存貯體中的物件層級 API 活動採取動作。如果您設定多區域線索記錄所有 S3 儲存貯體的唯一讀或所有類型的資料事件，則此控制項會產生 PASSED 調查結果。

修補

若要啟用 S3 儲存貯體的物件層級記錄，請參閱《Amazon Simple Storage Service 使用者指南》中的 [啟用 S3 儲存貯體和物件的 CloudTrail 事件記錄](#)。

【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定

相關要求：PCI DSS v4.0.1/1.4.4

類別：保護 > 安全網路組態 > 不可公開存取的資源

嚴重性：高

資源類型：AWS::S3::MultiRegionAccessPoint

AWS Config rule：s3-mrap-public-access-blocked (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon S3 多區域存取點是否已啟用封鎖公有存取設定。當多區域存取點未啟用封鎖公開存取設定時，控制項會失敗。

可公開存取的資源可能會導致未經授權的存取、資料外洩或漏洞遭到利用。透過身分驗證和授權措施限制存取有助於保護敏感資訊和維護資源的完整性。

修補

根據預設，會針對 S3 多區域存取點啟用所有封鎖公開存取設定。如需詳細資訊，請參閱《[Amazon Simple Storage Service 使用者指南](#)》中的[使用 Amazon S3 多區域存取點封鎖公開存取](#)。在建立多區域存取點的封鎖公開存取設定後，您便無法再變更設定。

【S3.25】 S3 目錄儲存貯體應該具有生命週期組態

類別：保護 > 資料保護

嚴重性：低

資源類型：AWS::S3Express::DirectoryBucket

AWS Config 規則：[s3express-dir-bucket-lifecycle-rules-check](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
targetExpirationDays	物件建立後，物件應過期的天數。	Integer	1 至 2147483647	無預設值

此控制項會檢查是否已為 S3 目錄儲存貯體設定生命週期規則。如果未針對目錄儲存貯體設定生命週期規則，或儲存貯體的生命週期規則指定與您選擇性指定的參數值不相符的過期設定，則控制項會失敗。

在 Amazon S3 中，生命週期組態是一組規則，定義 Amazon S3 要套用至儲存貯體中一組物件的動作。對於 S3 目錄儲存貯體，您可以建立生命週期規則，指定物件何時會根據存留期（以天為單位）過期。您也可以建立生命週期規則，刪除未完成的分段上傳。與其他類型的 S3 儲存貯體不同，例如一般用途儲存貯體，目錄儲存貯體不支援生命週期規則的其他動作類型，例如在儲存類別之間轉換物件。

修補

若要定義 S3 目錄儲存貯體的生命週期組態，請為儲存貯體建立生命週期規則。如需詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的[建立和管理目錄儲存貯體的生命週期組態](#)。

SageMaker AI 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon SageMaker AI 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【SageMaker.1】Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全網路組態

嚴重性：高

資源類型：AWS::SageMaker::NotebookInstance

AWS Config 規則：[sagemaker-notebook-no-direct-internet-access](#)

排程類型：定期

參數：無

此控制項會檢查 SageMaker AI 筆記本執行個體是否停用直接網際網路存取。如果為筆記本執行個體啟用 DirectInternetAccess 欄位，則控制項會失敗。

如果您在沒有 VPC 的情況下設定 SageMaker AI 執行個體，則執行個體預設會啟用直接網際網路存取。您應該使用 VPC 設定執行個體，並將預設設定變更為停用 - 透過 VPC 存取網際網路。若要從筆記本訓練或託管模型，您需要網際網路存取。若要啟用網際網路存取，您的 VPC 必須具有界面端點 (AWS PrivateLink) 或 NAT 閘道，以及允許傳出連線的安全群組。若要進一步了解如何將筆記本執行個體連線至 VPC 中的資源，請參閱《Amazon SageMaker AI 開發人員指南》中的[將筆記本執行個體連線至 VPC 中的資源](#)。您也應該確保對 SageMaker AI 組態的存取僅限於授權的使用者。限制允許使用者變更 SageMaker AI 設定和資源的 IAM 許可。

修補

您無法在建立筆記本執行個體後變更網際網路存取設定。反之，您可以停止、刪除和重新建立具有封鎖網際網路存取的執行個體。若要刪除允許直接網際網路存取的筆記本執行個體，請參閱《Amazon SageMaker AI 開發人員指南》中的[使用筆記本執行個體建置模型：清除](#)。若要重新建立拒絕網際網路存取的筆記本執行個體，請參閱[建立筆記本執行個體](#)。針對網路、直接網際網路存取，選擇停用 - 透過 VPC 存取網際網路。

【SageMaker.2】應在自訂 VPC 中啟動 SageMaker 筆記本執行個體

相關要求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7、

類別：保護 > 安全網路組態 > VPC 內的資源

嚴重性：高

資源類型：AWS::SageMaker::NotebookInstance

AWS Config 規則：[sagemaker-notebook-instance-inside-vpc](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon SageMaker AI 筆記本執行個體是否在自訂虛擬私有雲端 (VPC) 中啟動。如果 SageMaker AI 筆記本執行個體未在自訂 VPC 內啟動，或在 SageMaker AI 服務 VPC 中啟動，則此控制會失敗。

子網路是 VPC 內的 IP 地址範圍。我們建議您盡可能將資源保留在自訂 VPC 中，以確保基礎設施的安全網路保護。Amazon VPC 是您的專用虛擬網路 AWS 帳戶。使用 Amazon VPC，您可以控制 SageMaker AI Studio 和筆記本執行個體的網路存取和網際網路連線。

修補

您無法在建立筆記本執行個體之後變更 VPC 設定。反之，您可以停止、刪除和重新建立執行個體。如需說明，請參閱《Amazon SageMaker AI 開發人員指南》中的[使用筆記本執行個體建置模型：清除](#)。

【SageMaker.3】使用者不應擁有 SageMaker 筆記本執行個體的根存取權

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-6、NIST.800-53.r5 AC-6(10)、NIST.800-53.r5 AC-6(2)

類別：保護 > 安全存取管理 > 根使用者存取限制

嚴重性：高

資源類型：AWS::SageMaker::NotebookInstance

AWS Config 規則：[sagemaker-notebook-instance-root-access-check](#)

排程類型：變更已觸發

參數：無

此控制項會檢查是否已開啟 Amazon SageMaker AI 筆記本執行個體的根存取權。如果 SageMaker AI 筆記本執行個體的根存取已開啟，則控制項會失敗。

根據最低權限的主體，建議安全最佳實務是限制執行個體資源的根存取權，以避免意外過度佈建許可。

修補

若要限制對 SageMaker AI 筆記本執行個體的根存取權，請參閱 [《Amazon SageMaker AI 開發人員指南》](#) 中的控制對 SageMaker AI 筆記本執行個體的根存取權。Amazon SageMaker

【SageMaker.4】SageMaker 端點生產變體的初始執行個體計數應大於 1

相關要求：NIST.800-53.r5 CP-10、NIST.800-53.r5 SC-5、NIST.800-53.r5 SC-36、NIST.800-53.r5 SA-13

類別：復原 > 彈性 > 高可用性

嚴重性：中

資源類型：AWS::SageMaker::EndpointConfig

AWS Config 規則：[sagemaker-endpoint-config-prod-instance-count](#)

排程類型：定期

參數：無

此控制項會檢查 Amazon SageMaker AI 端點的生產變體是否具有大於 1 的初始執行個體計數。如果端點的生產變體只有 1 個初始執行個體，則控制項會失敗。

執行個體計數大於 1 的生產變體允許由 SageMaker AI 管理的多可用區域執行個體備援。在多個可用區域部署資源是 AWS 最佳實務，可在您的架構中提供高可用性。高可用性可協助您從安全事件中復原。

 Note

此控制項僅適用於執行個體型端點組態。

修補

如需端點組態參數的詳細資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的[建立端點組態](#)。

【SageMaker.5】SageMaker 模型應該啟用網路隔離

類別：保護 > 安全網路組態 > 資源不可公開存取

嚴重性：中

資源類型：AWS::SageMaker::Model

AWS Config 規則：[sagemaker-model-isolation-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon SageMaker AI 託管模型是否已啟用網路隔離。如果託管模型的 `EnableNetworkIsolation` 參數設定為 `False`，則控制項會失敗。

SageMaker AI 訓練和部署的推論容器預設可以使用網際網路。如果您不希望 SageMaker AI 提供訓練或推論容器的外部網路存取權，您可以啟用網路隔離。如果您啟用網路隔離，則無法對模型容器進行傳入或傳出網路呼叫，包括對其他容器進行呼叫 AWS 服務。此外，容器執行期環境不會提供任何 AWS 登入資料。啟用網路隔離有助於防止從網際網路意外存取 SageMaker AI 資源。

Note

2025 年 8 月 13 日，Security Hub CSPM 變更了此控制項的標題和描述。新的標題和描述更準確地反映控制項會檢查 Amazon SageMaker AI 託管模型 `EnableNetworkIsolation` 參數的設定。先前，此控制項的標題為：SageMaker models should block inbound traffic。

修補

如需 SageMaker AI 模型網路隔離的詳細資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的[以無網際網路模式執行訓練和推論容器](#)。建立模型時，您可以將 `EnableNetworkIsolation` 參數的值設定為 `True`，以啟用網路隔離。

【SageMaker.6】應標記 SageMaker 應用程式映像組態

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::SageMaker::AppImageConfig

AWS Config 規則：[sagemaker-app-image-config-tagged](#)

排程類型：變更已觸發

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	無預設值

此控制項會檢查 Amazon SageMaker AI 應用程式映像組態 (AppImageConfig) 是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果應用程式映像組態沒有任何標籤索引鍵，或沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果應用程式映像組態沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws: 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都是由必要的標籤索引鍵和選用的標籤值所組成。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多 存取 AWS 服務。它們不適用於私有或敏感資料。

修補

若要將標籤新增至 Amazon SageMaker AI 應用程式映像組態 (AppImageConfig)，您可以使用 SageMaker AI API 的 [AddTags](#) 操作，或者，如果您使用的是 AWS CLI，請執行 [add-tags](#) 命令。

【SageMaker.7】應標記 SageMaker 映像

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::SageMaker::Image

AWS Config 規則：[sagemaker-image-tagged](#)

排程類型：已觸發變更

參數：

參數	Description (描述)	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon SageMaker AI 映像是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果映像沒有任何標籤索引鍵，或沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果映像沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，系統標籤會自動套用並具有 aws: 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都是由必要的標籤索引鍵和選用的標籤值所組成。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多存取 AWS 服務。它們不適用於私有或敏感資料。

修補

若要將標籤新增至 Amazon SageMaker AI 映像，您可以使用 SageMaker AI API 的 [AddTags](#) 操作，或者，如果您使用的是 AWS CLI，請執行 [add-tags](#) 命令。

【SageMaker.8】SageMaker 筆記本執行個體應在支援的平台上執行

類別：偵測 > 漏洞、修補程式和版本管理

嚴重性：中

資源類型：AWS::SageMaker::NotebookInstance

AWS Config 規則：[sagemaker-notebook-instance-platform-version](#)

排程類型：定期

參數：

- supportedPlatformIdentifierVersions : notebook-al2-v3 (不可自訂)

此控制項會根據筆記本執行個體指定的平台識別碼，檢查 Amazon SageMaker AI 筆記本執行個體是否設定為在支援的平台上執行。如果筆記本執行個體設定為在不再支援的平台上執行，則控制項會失敗。

如果不再支援 Amazon SageMaker AI 筆記本執行個體的平台，則可能不會收到安全修補程式、錯誤修正或其他類型的更新。筆記本執行個體可能會繼續運作，但不會收到 SageMaker AI 安全性更新或重大錯誤修正。您承擔使用不支援平台的相關風險。如需詳細資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的 [JupyterLab 版本控制](#)。

修補

如需有關 Amazon SageMaker AI 目前支援的平台以及如何遷移到這些平台的資訊，請參閱《[Amazon SageMaker AI 開發人員指南](#)》中的 [Amazon Linux 2 筆記本執行個體](#)。Amazon SageMaker

【SageMaker.9】SageMaker 資料品質任務定義應該啟用容器間流量加密

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::SageMaker::DataQualityJobDefinition

AWS Config 規則：[sagemaker-data-quality-job-encrypt-in-transit](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon SageMaker AI 資料品質任務定義是否已啟用容器間流量的加密。如果監控資料品質和偏離的任務定義未針對容器間流量啟用加密，則控制項會失敗。

啟用容器間流量加密可在分散式處理期間保護敏感 ML 資料，以進行資料品質分析。

修補

如需 Amazon SageMaker AI 容器間流量加密的詳細資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的在[分散式訓練任務中保護 ML 運算執行個體之間的通訊](#)。建立資料品質任務定義時，您可以將 `EnableInterContainerTrafficEncryption` 參數的值設定為 `True`，以啟用容器間流量加密。

【SageMaker.10】SageMaker 模型可解釋性任務定義應啟用容器間流量加密

類別：保護 > 資料保護 > data-in-transit

嚴重性：中

資源類型：AWS::SageMaker::ModelExplainabilityJobDefinition

AWS Config 規則：[sagemaker-model-explainability-job-encrypt-in-transit](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon SageMaker 模型可解釋性任務定義是否已啟用容器間流量加密。如果模型可解釋性任務定義未啟用容器間流量加密，則控制項會失敗。

啟用容器間流量加密可在分散式處理期間保護敏感 ML 資料，例如模型資料、訓練資料集、中繼處理結果、參數和模型權重，以進行可解釋性分析。

修補

對於現有的 SageMaker 模型可解釋性任務定義，無法更新容器間流量加密。若要在啟用容器間流量加密的情況下建立新的 SageMaker 模型可解釋性任務定義，請使用 [API](#) 或 [CLI](#) 或 [CloudFormation](#)，並將 [EnableInterContainerTrafficEncryption](#) 設定為 `True`。

【SageMaker.11】SageMaker 資料品質任務定義應該啟用網路隔離

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::SageMaker::DataQualityJobDefinition

AWS Config 規則：[sagemaker-data-quality-job-isolation](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon SageMaker AI 資料品質監控任務定義是否已啟用網路隔離。如果監控資料品質和偏離的任務定義已停用網路隔離，則控制項會失敗。

網路隔離可減少攻擊。會浮現並防止外部存取，藉此防止未經授權的外部存取、意外資料暴露和潛在的資料外洩。

修補

如需 SageMaker AI 網路隔離的詳細資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的[以無網際網路模式執行訓練和推論容器](#)。建立資料品質任務定義時，您可以將 `EnableNetworkIsolation` 參數的值設定為 `True`，以啟用網路隔離。

【SageMaker.12】SageMaker 模型偏差任務定義應該啟用網路隔離

類別：保護 > 安全網路組態 > 資源政策組態

嚴重性：中

資源類型：AWS::SageMaker::ModelBiasJobDefinition

AWS Config 規則：[sagemaker-model-bias-job-isolation](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 SageMaker 模型偏差任務定義是否已啟用網路隔離。如果模型偏差任務定義未啟用網路隔離，則控制項會失敗。

網路隔離可防止 SageMaker 模型偏差任務透過網際網路與外部資源通訊。透過啟用網路隔離，您可以確保任務的容器無法進行傳出連線，減少攻擊面並保護敏感資料免於洩漏。這對處理受管制或敏感資料的任務特別重要。

修補

若要啟用網路隔離，您必須建立新的模型偏差任務定義，並將 `EnableNetworkIsolation` 參數設定為 `True`。建立任務定義後，無法修改網路隔離。若要建立新的模型偏差任務定義，請參閱《Amazon SageMaker AI 開發人員指南》中的 [CreateModelBiasJobDefinition](#)。

【SageMaker.13】SageMaker 模型品質任務定義應該啟用容器間流量加密

類別：保護 > 資料保護 > data-in-transit

嚴重性：中

資源類型：AWS::SageMaker::ModelQualityJobDefinition

AWS Config 規則：[ssagemaker-model-quality-job-encrypt-in-transit](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon SageMaker 模型品質任務定義是否針對容器間流量啟用傳輸中加密。如果模型品質任務定義未啟用容器間流量加密，則控制項會失敗。

容器間流量加密可在分散式模型品質監控任務期間保護容器之間傳輸的資料。根據預設，容器間流量不會加密。啟用加密有助於在處理期間維護資料機密性，並支援符合傳輸中資料保護的法規要求。

修補

若要為您的 Amazon SageMaker 模型品質任務定義啟用容器間流量加密，您必須使用適當的傳輸中加密組態重新建立任務定義。若要建立模型品質任務定義，請參閱《Amazon SageMaker AI 開發人員指南》中的 [CreateModelQualityJobDefinition](#)。

【SageMaker.14】SageMaker 監控排程應該啟用網路隔離

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::SageMaker::MonitoringSchedule

AWS Config 規則：[sagemaker-monitoring-schedule-isolation](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon SageMaker 監控排程是否已啟用網路隔離。如果監控排程將 `EnableNetworkIsolation` 設定為 `false` 或未設定，則控制項會失敗

網路隔離可防止監控任務進行傳出網路呼叫，透過消除容器的網際網路存取來減少攻擊面。

修補

如需在建立或更新監控排程時在 `NetworkConfig` 參數中設定網路隔離的相關資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的 [CreateMonitoringSchedule](#) 或 [UpdateMonitoringSchedule](#)。

【SageMaker.15】SageMaker 模型偏差任務定義應該啟用容器間流量加密

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::SageMaker::ModelBiasJobDefinition

AWS Config 規則：[sagemaker-model-bias-job-encrypt-in-transit](#)

排程類型：已觸發變更

參數：無

此控制項會檢查使用多個運算執行個體時，Amazon SageMaker 模型偏差任務定義是否已啟用容器間流量加密。如果 `EnableInterContainerTrafficEncryption` 設定為 `false`，或未針對執行個體計數為 2 或更高的任務定義設定，則控制項會失敗。

ELinter 容器流量加密可在分散式模型偏差監控任務期間保護運算執行個體之間傳輸的資料。加密可防止未經授權存取模型相關資訊，例如執行個體之間傳輸的權重。

修補

若要啟用 SageMaker 模型偏差任務定義的容器間流量加密，請在任務定義使用多個運算執行個體 `True` 時，將 `EnableInterContainerTrafficEncryption` 參數設定為 `True`。如需有關保護 ML 運

算執行個體之間通訊的資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的[保護分散式訓練任務中 ML 運算執行個體之間的通訊](#)。

【SageMaker.16】SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器

類別：保護 > 安全網路組態 > VPC 內的資源

嚴重性：中

資源類型：AWS::SageMaker::Model

AWS Config 規則：[sagemaker-model-private-registry-required](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon SageMaker AI 模型是否從主要容器 VPC 中的私有登錄檔提取容器映像。如果未設定映像或儲存庫存取模式為 `Private`，則控制項會失敗 Platform。

在 VPC for SageMaker 模型容器中使用私有 Docker 登錄檔，可確保從 VPC 中受信任、受控制的來源提取容器映像。此外，它可確保容器映像可透過 VPC 端點存取，而不會周遊公有網際網路。

修補

若要設定 SageMaker AI 即時推論容器的私有 Docker 登錄檔，請參閱《Amazon SageMaker AI 開發人員指南》中的[使用適用於即時推論容器的私有 Docker 登錄檔](#)。

【SageMaker.17】SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密

類別：保護 > 資料保護 > data-at-rest 加密

嚴重性：中

資源類型：AWS::SageMaker::FeatureGroup

AWS Config 規則：[sagemaker-featuregroup-encryption-at-rest](#)

排程類型：變更已觸發

參數：無

此控制項會檢查特徵群組的 Amazon SageMaker 離線存放區是否使用 AWS KMS 金鑰進行靜態加密。如果特徵群組的離線存放區 S3 儲存沒有使用 KMS 金鑰加密，則控制項會失敗。

在 SageMaker 功能群組離線存放區的其他位置使用客戶受管 AWS KMS keys 加密，可提供增強的安全性。客戶受管 KMS 金鑰可讓您完全控制加密金鑰生命週期和金鑰政策。此外，所有加密金鑰用量都可以透過 記錄和監控，AWS CloudTrail 以確保可稽核性。

修補

如需使用 AWS KMS 客戶受管金鑰為 SageMaker Feature Store 離線存放區啟用靜態加密的資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的[安全和存取控制](#)。

【SageMaker.18】使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密

相關要求：NIST.800-53.r5 AU-9、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-12(2)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SI-7(6)

類別：保護 – 資料保護 – 靜態資料加密

嚴重性：中

資源類型：AWS::SageMaker::FeatureGroup

AWS Config 規則：[sagemaker-featuregroup-online-store-encryption](#)

排程類型：變更已觸發

參數：無

此控制項會檢查具有標準儲存的功能群組的 Amazon SageMaker 線上儲存是否使用 AWS KMS 金鑰靜態加密。如果未為線上存放區設定 KMS 金鑰加密，則控制項會失敗。

使用客戶受管的 SageMaker 功能群組線上商店的其餘部分 AWS KMS keys 進行加密，可提供增強的安全性。客戶受管 KMS 金鑰可讓您完全控制加密金鑰生命週期和金鑰政策。此外，所有加密金鑰用量都可以透過 記錄和監控，AWS CloudTrail 以確保可稽核性。

修補

如需使用 AWS KMS 客戶受管金鑰為 SageMaker Feature Store 線上商店啟用靜態加密的資訊，請參閱《Amazon SageMaker AI 開發人員指南》中的[安全和存取控制](#)。

【SageMaker.19】SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道

類別：保護 > 安全網路組態 > VPC 內的資源

嚴重性：中

資源類型：AWS::SageMaker::Model

AWS Config 規則：[sagemaker-model-multicontainer-private-registry](#)

排程類型：變更已觸發

參數：無

此控制項會檢查具有多容器推論管道的 Amazon SageMaker AI 模型是否從 VPC 中的私有 Docker 登錄檔提取容器映像。如果任何容器定義沒有映像組態，或儲存庫存取模式設定為平台，則控制項會失敗。

在 VPC for SageMaker AI 多容器推論管道中使用私有 Docker 登錄檔，可確保從 VPC 中受信任、受控制的來源提取容器映像。這可確保容器映像可透過 VPC 端點存取，而不會周遊公有網際網路，從而降低供應鏈攻擊或映像竄改的風險。

修補

若要設定 SageMaker AI 即時推論容器的私有 Docker 登錄檔，請參閱《Amazon SageMaker AI 開發人員指南》中的[使用適用於即時推論容器的私有 Docker 登錄檔](#)。

Secrets Manager 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 AWS Secrets Manager 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【SecretsManager.1】Secrets Manager 秘密應該已啟用自動輪換

相關要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.3.9

類別：保護 > 安全開發

嚴重性：中

資源類型：AWS::SecretsManager::Secret

AWS Config 規則：[secretsmanager-rotation-enabled-check](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
maximumAllowedRotationFrequency	允許秘密輪換頻率的天數上限	Integer	1 至 365	無預設值

此控制項 AWS Secrets Manager 會檢查存放在 中的秘密是否已設定自動輪換。如果未使用自動輪換設定秘密，則控制項會失敗。如果您為 maximumAllowedRotationFrequency 參數提供自訂值，則只有在指定的時段內自動輪換秘密時，控制項才會通過。

Secrets Manager 可協助您改善組織的安全狀態。秘密包括資料庫登入資料、密碼和第三方 API 金鑰。您可以使用 Secrets Manager 集中存放秘密、自動加密秘密、控制對秘密的存取，以及安全自動輪換秘密。

Secrets Manager 可以輪換秘密。您可以使用輪換將長期秘密取代為短期秘密。輪換您的秘密會限制未經授權的使用者使用洩露秘密的時間長度。因此，您應該經常輪換秘密。若要進一步了解輪換，請參閱AWS Secrets Manager 《使用者指南》中的[輪換您的 AWS Secrets Manager 秘密](#)。

修補

若要開啟 Secrets Manager 秘密的自動輪換，請參閱AWS Secrets Manager 《使用者指南》中的[使用主控台設定 AWS Secrets Manager 秘密的自動輪換](#)。您必須選擇並設定 AWS Lambda 函數以進行輪換。

【SecretsManager.2】設定自動輪換的 Secrets Manager 秘密應能成功輪換

相關要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.3.9

類別：保護 > 安全開發

嚴重性：中

資源類型：AWS::SecretsManager::Secret

AWS Config 規則：[secretsmanager-scheduled-rotation-success-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS Secrets Manager 秘密是否根據輪換排程成功輪換。如果 `RotationOccurringAsScheduled` 為 `false`，則控制項會失敗。控制項只會評估已開啟輪換的秘密。

Secrets Manager 可協助您改善組織的安全狀態。秘密包括資料庫登入資料、密碼和第三方 API 金鑰。您可以使用 Secrets Manager 集中存放秘密、自動加密秘密、控制對秘密的存取，以及安全自動輪換秘密。

Secrets Manager 可以輪換秘密。您可以使用輪換將長期秘密取代為短期秘密。輪換您的秘密會限制未經授權的使用者使用洩露秘密的時間長度。因此，您應該經常輪換秘密。

除了將秘密設定為自動輪換之外，您也應該確保這些秘密會根據輪換排程成功輪換。

若要進一步了解輪換，請參閱AWS Secrets Manager 《使用者指南》中的[輪換您的 AWS Secrets Manager 秘密](#)。

修補

如果自動輪換失敗，則 Secrets Manager 可能遇到組態錯誤。若要在 Secrets Manager 中輪換秘密，您可以使用 Lambda 函數來定義如何與擁有秘密的資料庫或服務互動。

如需診斷和修正與秘密輪換相關的常見錯誤的說明，請參閱AWS Secrets Manager 《使用者指南》中的[對秘密 AWS Secrets Manager 輪換進行故障診斷](#)。

【SecretsManager.3】移除未使用的 Secrets Manager 秘密

相關需求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::SecretsManager::Secret

AWS Config 規則：[secretsmanager-secret-unused](#)

排程類型：定期

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
unusedFor Days	秘密可以保持未使用的天數上限	Integer	1 至 365	90

此控制項會檢查是否已在指定的時間範圍內存取 AWS Secrets Manager 秘密。如果秘密在指定的時間範圍內未使用，則控制項會失敗。除非您提供存取期間的自訂參數值，否則 Security Hub CSPM 會使用預設值 90 天。

刪除未使用的秘密與輪換秘密一樣重要。未使用的秘密可能會被其前使用者濫用，他們不再需要存取這些秘密。此外，隨著更多使用者可以存取秘密，有人可能會不當處理秘密並將其洩漏給未經授權的實體，進而增加濫用的風險。刪除未使用的秘密有助於從不再需要的使用者撤銷秘密存取。它也有助於降低使用 Secrets Manager 的成本。因此，定期刪除未使用的秘密至關重要。

修補

若要刪除非作用中的 Secrets Manager 秘密，請參閱AWS Secrets Manager 《使用者指南》中的[刪除 AWS Secrets Manager 秘密](#)。

【SecretsManager.4】Secrets Manager 秘密應在指定的天數內輪換

相關要求：NIST.800-53.r5 AC-2(1)、NIST.800-53.r5 AC-3(15)、PCI DSS v4.0.1/8.6.3、PCI DSS v4.0.1/8.3.9

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::SecretsManager::Secret

AWS Config 規則：[secretsmanager-secret-periodic-rotation](#)

排程類型：定期

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
maxDaysSinceRotation	秘密可保持不變的天數上限	Integer	1 至 180	90

此控制項會檢查 AWS Secrets Manager 秘密是否在指定的時間範圍內至少輪換一次。如果至少此頻率未輪換秘密，則控制項會失敗。除非您提供輪換期間的自訂參數值，否則 Security Hub CSPM 會使用預設值 90 天。

輪換秘密可協助您降低在 中未經授權使用秘密的風險 AWS 帳戶。範例包括資料庫登入資料、密碼、第三方 API 金鑰，甚至是任意文字。如果您長時間不變更秘密，則更有可能洩露秘密。

隨著更多使用者可以存取秘密，有人可能會不當處理秘密並將其洩漏給未經授權的實體。秘密可以透過日誌和快取資料洩漏。它們可以針對除錯目的共用，而在除錯完成之後未變更或撤銷。由於上述所有原因，秘密應該經常輪換。

您可以為 中的秘密設定自動輪換 AWS Secrets Manager。透過自動輪換，您可以將長期秘密取代為短期秘密，大幅降低入侵的風險。建議您為 Secrets Manager 秘密設定自動輪換。如需更多詳細資訊，請參閱 AWS Secrets Manager 使用者指南中的 [輪換 AWS Secrets Manager 密碼](#)。

修補

若要開啟 Secrets Manager 秘密的自動輪換，請參閱 AWS Secrets Manager 《使用者指南》中的 [使用主控台設定 AWS Secrets Manager 秘密的自動輪換](#)。您必須選擇並設定 AWS Lambda 函數以進行輪換。

【SecretsManager.5】Secrets Manager 秘密應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::SecretsManager::Secret

AWS Config rule : tagged-secretsmanager-secret (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 AWS Secrets Manager 秘密是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果秘密沒有任何標籤索引鍵，或如果它沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果秘密未標記任何索引鍵，則 會失敗。系統會忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Secrets Manager 秘密，請參閱 AWS Secrets Manager 《使用者指南》中的 [標籤 AWS Secrets Manager 秘密](#)。

的 Security Hub CSPM 控制項 AWS Service Catalog

此 AWS Security Hub CSPM 控制項會評估 AWS Service Catalog 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【ServiceCatalog.1】Service Catalog 產品組合只能在 AWS 組織內共用

相關需求：NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-6、NIST.800-53.r5 CM-8、NIST.800-53.r5 SC-7

類別：保護 > 安全存取管理

嚴重性：中

資源類型：AWS::ServiceCatalog::Portfolio

AWS Config 規則：[service-catalog-shared-within-organization](#)

排程類型：已觸發變更

參數：無

此控制項會在啟用與 AWS Organizations 的整合時，檢查 是否在組織內 AWS Service Catalog 共用產品組合。如果未在組織內共用產品組合，則控制項會失敗。

僅在 Organizations 內共用產品組合有助於確保產品組合不會與不正確的 共用 AWS 帳戶。若要與組織中的帳戶共用 Service Catalog 產品組合，Security Hub CSPM 建議使用 ORGANIZATION_MEMBER_ACCOUNT 而非 ACCOUNT。這透過管理在整個組織中授予帳戶的存取權來簡化管理。如果您有業務需要與外部帳戶共用 Service Catalog 產品組合，您可以[自動隱藏此控制項](#)的問題清單或[將其停用](#)。

修補

若要啟用與 共用產品組合 AWS Organizations，請參閱《AWS Service Catalog 管理員指南》中的[與共用 AWS Organizations](#)。

Amazon SES 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Simple Email Service (Amazon SES) 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【SES.1】 SES 聯絡人清單應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::SES::ContactList

AWS Config rule：tagged-ses-contactlist (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon SES 聯絡人清單是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果聯絡人清單沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果聯絡人清單未標記任何索引鍵，則 會失敗。系統會 aws: 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Amazon SES 聯絡人清單，請參閱《Amazon SES API v2 參考》中的 [TagResource](#)。

【SES.2】 SES 組態集應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::SES::ConfigurationSet

AWS Config rule：tagged-ses-configurationset (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 Amazon SES 組態設定是否具有具有參數 中定義之特定金鑰的標籤 requiredTagKeys。如果組態集沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果組態集未標記任何索引鍵，則 控制項會失敗。系統會 aws: 忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的 [標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 Amazon SES 組態設定，請參閱《Amazon SES API v2 參考》中的 [TagResource](#)。

【SES.3】 SES 組態集應啟用 TLS 以傳送電子郵件

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::SES::ConfigurationSet

AWS Config 規則：[ses-sending-tls-required](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon SES 組態設定是否需要 TLS 連線。如果組態設定的 TLS 政策未設定為 'REQUIRE'，則控制項會失敗。

根據預設，Amazon SES 使用機會式 TLS，這表示如果無法與接收郵件伺服器建立 TLS 連線，則可以未加密地傳送電子郵件。為電子郵件傳送強制執行 TLS 可確保訊息只有在可以建立安全加密連線時才會傳遞。這有助於在 Amazon SES 與收件人郵件伺服器之間的傳輸期間保護電子郵件內容的機密性和完整性。如果無法建立安全 TLS 連線，則不會傳送訊息，以防止可能暴露敏感資訊。

Note

雖然 TLS 1.3 是 Amazon SES 的預設交付方法，但不透過組態設定強制執行 TLS 要求，但如果 TLS 連線失敗，訊息可能會以純文字交付。若要傳遞此控制項，您必須在 SES 組態集的交付選項 'REQUIRE' 中將 TLS 政策設定為 。需要 TLS 時，只有在可與接收郵件伺服器建立 TLS 連線時，才會傳遞訊息。

修補

若要將 Amazon SES 設定為需要組態設定的 TLS 連線，請參閱 [《Amazon SES 開發人員指南》中的 Amazon SES 和安全性通訊協定](#)。Amazon SES

Amazon SNS 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Simple Notification Service (Amazon SNS) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【SNS.1】 SNS 主題應使用 進行靜態加密 AWS KMS

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)、NIST.800-171.r2 3.13.11、NIST.800-171.r2 3.13.16

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::SNS::Topic

AWS Config 規則：[sns-encrypted-kms](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon SNS 主題是否使用 AWS Key Management Service () 中管理的金鑰進行靜態加密AWS KMS。如果 SNS 主題不使用 KMS 金鑰進行伺服器端加密 (SSE)，則控制項會失敗。根據預設，SNS 會使用磁碟加密來存放訊息和檔案。若要傳遞此控制項，您必須選擇改用 KMS 金鑰進行加密。這增加了多一層的安全性，並提供更多的存取控制彈性。

加密靜態資料可降低未驗證的使用者存取磁碟上儲存的資料的風險 AWS。需要 API 許可才能解密資料，才能讀取資料。我們建議您使用 KMS 金鑰加密 SNS 主題，以增加一層安全性。

修補

若要為 SNS 主題啟用 SSE，請參閱 [《Amazon Simple Notification Service 開發人員指南》中的為 Amazon SNS 主題啟用伺服器端加密 \(SSE\)](#)。在使用 SSE 之前，您還必須設定 AWS KMS key 政

策，以允許加密主題和加密和解密訊息。如需詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的[設定 AWS KMS 許可](#)。

【SNS.2】應針對傳送至主題的通知訊息啟用傳遞狀態記錄

Important

Security Hub CSPM 已於 2024 年 4 月淘汰此控制項。如需詳細資訊，請參閱[Security Hub CSPM 控制項的變更日誌](#)。

相關要求：NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::SNS::Topic

AWS Config 規則：[sns-topic-message-delivery-notification-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查是否已針對傳送至端點 Amazon SNS 主題的通知訊息傳送狀態啟用記錄。如果未啟用訊息的傳遞狀態通知，則此控制項會失敗。

記錄是維護服務的可靠性、可用性和效能的重要部分。記錄訊息傳遞狀態有助於提供操作洞察，例如：

- 得知訊息是否已傳遞至 Amazon SNS 端點。
- 識別從 Amazon SNS 端點傳送至 Amazon SNS 的回應。
- 判斷訊息駐留時間（發佈時間戳記與遞交至 Amazon SNS 端點之間的時間）。

修補

若要設定主題的交付狀態記錄，請參閱[《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 訊息交付狀態](#)。

【SNS.3】 SNS 主題應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::SNS::Topic

AWS Config rule：tagged-sns-topic (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon SNS 主題是否具有具有參數中定義之特定金鑰的標籤requiredTagKeys。如果主題沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果主題未標記任何索引鍵，則會失敗。系統會aws:忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

若要將標籤新增至 SNS 主題，請參閱 [《Amazon Simple Notification Service 開發人員指南》](#) 中的 [設定 Amazon SNS 主題標籤](#)。

【SNS.4】 SNS 主題存取政策不應允許公開存取

類別：保護 > 安全網路組態 > 不可公開存取的資源

嚴重性：嚴重

資源類型：AWS::SNS::Topic

AWS Config 規則：[sns-topic-no-public-access](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon SNS 主題存取政策是否允許公開存取。如果 SNS 主題存取政策允許公開存取，則此控制會失敗。

您可以使用 Amazon SNS 存取政策搭配特定主題來限制誰可以使用該主題（例如，誰可以發佈訊息給該主題或誰可以訂閱該主題）。SNS 政策可以將存取權授予其他 AWS 帳戶或您自己的 中的使用者 AWS 帳戶。在主題政策的 Principal 欄位中提供萬用字元 (*)，且缺少限制主題政策的條件，可能會導致攻擊者洩漏資料、拒絕服務或意外地將訊息注入您的服務。

Note

此控制項不會評估使用萬用字元或變數的政策條件。若要產生 PASSED 調查結果，主題的 Amazon SNS 存取政策中的條件只能使用固定值，這些值不包含萬用字元或政策變數。如需政策變數的相關資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的 [變數和標籤](#)。

修補

若要更新 SNS 主題的存取政策，請參閱 [《Amazon Simple Notification Service 開發人員指南》](#) 中的 [在 Amazon SNS 中管理存取權的概觀](#)。

Amazon SQS 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon Simple Queue Service (Amazon SQS) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【SQS.1】 Amazon SQS 佇列應靜態加密

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-3(6)、NIST.800-53.r5 SC-13、NIST.800-53.r5 SC-28、NIST.800-53.r5 SC-28(1)、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SI-7(6)

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::SQS::Queue

AWS Config rule：sqs-queue-encrypted (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon SQS 佇列是否靜態加密。如果佇列未使用 SQS 受管金鑰 (SSE-SQS) 或 AWS Key Management Service (AWS KMS) 金鑰 (SSE-KMS) 加密，則控制項會失敗。

加密靜態資料可降低未經授權的使用者存取儲存在磁碟上的資料的風險。伺服器端加密 (SSE) 使用 SQS 受管加密金鑰 (SSE-SQS) 或 AWS KMS 金鑰 (SSE-KMS) 保護 SQS 佇列中的訊息內容。

修補

若要設定 SQS 佇列的 SSE，請參閱《Amazon Simple Queue Service 開發人員指南》中的[設定佇列的伺服器端加密 \(SSE\)](#)。

【SQS.2】 SQS 佇列應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::SQS::Queue

AWS Config rule：tagged-sqs-queue (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	No default value

此控制項會檢查 Amazon SQS 佇列是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果佇列沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果佇列未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的當責資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《[標記您的 AWS 資源](#)》中的 [標記您的 AWS 資源](#) 一般參考。

修補

若要使用 Amazon SQS 主控台將標籤新增至現有佇列，請參閱《Amazon Simple Queue Service 開發人員指南》中的 [設定 Amazon SQS 佇列（主控台）的成本分配標籤](#)。

【SQS.3】 SQS 佇列存取政策不應允許公開存取

類別：保護 > 安全存取管理 > 資源不可公開存取

嚴重性：嚴重

資源類型：AWS::SQS::Queue

AWS Config 規則：[sqs-queue-no-public-access](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon SQS 存取政策是否允許公開存取 SQS 佇列。如果 SQS 存取政策允許公開存取佇列，則控制項會失敗。

Amazon SQS 存取政策可以允許公開存取 SQS 佇列，這可能允許匿名使用者或任何已驗證的 AWS IAM 身分存取佇列。SQS 存取政策通常會透過在政策的 Principal 元素中指定萬用字元 (*) 來提供此存取，而不使用適當的條件來限制對佇列的存取，或同時指定兩者。如果 SQS 存取政策允許公開存取，第三方可能會執行任務，例如從佇列接收訊息、傳送訊息至佇列，或修改佇列的存取政策。這可能會導致資料外洩、拒絕服務或威脅行為者將訊息注入佇列等事件。

Note

此控制項不會評估使用萬用字元或變數的政策條件。若要產生 PASSED 調查結果，佇列的 Amazon SQS 存取政策中的條件只能使用固定值，這些值不包含萬用字元或政策變數。如需政策變數的相關資訊，請參閱 AWS Identity and Access Management 《使用者指南》中的 [變數和標籤](#)。

修補

如需有關為 SQS 佇列設定 SQS 存取政策的資訊，請參閱 [《Amazon Simple Queue Service 開發人員指南》中的搭配 Amazon SQS 存取政策語言使用自訂政策](#)。

Step Functions 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 AWS Step Functions 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【StepFunctions.1】Step Functions 狀態機器應該已開啟記錄

相關要求：PCI DSS v4.0.1/10.4.2

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::StepFunctions::StateMachine

AWS Config 規則：[step-functions-state-machine-logging-enabled](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
logLevel	最低記錄層級	列舉	ALL, ERROR, FATAL	無預設值

此控制項會檢查 AWS Step Functions 狀態機器是否已開啟記錄。如果狀態機器未開啟記錄，則控制項會失敗。如果您為 logLevel 參數提供自訂值，則只有在狀態機器已開啟指定的記錄層級時，控制項才會通過。

監控可協助您維護 Step Functions 的可靠性、可用性和效能。您應該從使用的 收集盡可能多 AWS 服務的監控資料，以便更輕鬆地偵錯多點失敗。為您的 Step Functions 狀態機器定義記錄組態可讓您追蹤 Amazon CloudWatch Logs 中的執行歷史記錄和結果。或者，您只能追蹤錯誤或嚴重事件。

修補

若要開啟 Step Functions 狀態機器的記錄，請參閱《AWS Step Functions 開發人員指南》中的[設定記錄](#)。

【StepFunctions.2】應標記 Step Functions 活動

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::StepFunctions::Activity

AWS Config rule：tagged-stepfunctions-activity (自訂 Security Hub CSPM 規則)

排程類型：已觸發變更

參數：

參數	說明	Type	允許的自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Step Functions 活動是否具有具有參數中定義之特定金鑰的標籤 requiredTagKeys。如果活動沒有任何標籤索引鍵，或沒有參數中指定的所有索引鍵，則控制項會失敗 requiredTagKeys。如果 requiredTagKeys 未提供參數，則控制項只會檢查標籤索引鍵是否存在，如果活動未標記任何索引鍵，則會失敗。系統會忽略自動套用並以開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的 [什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《[標記您的 AWS 資源](#)》中的 [AWS 一般參考](#)。

修補

若要將標籤新增至 Step Functions 活動，請參閱《[AWS Step Functions 開發人員指南](#)》中的 [Step Functions 中的標記](#)。

Systems Manager 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 AWS Systems Manager (SSM) 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱 [依區域的控制項可用性](#)。

【SSM.1】 Amazon EC2 執行個體應該由 管理 AWS Systems Manager

相關要求：PCI DSS v3.2.1/2.4、NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-8、NIST.800-53.r5 CM-8(1)、NIST.800-53.r5 CM-8(2)、NIST.800-53.r5 CM-8(3)、NIST.800-5.r5 SA-15(2)、NIST.800-SA-1550.r5 SA-3 SI-2

類別：識別 > 清查

嚴重性：中

評估的資源：AWS::EC2::Instance

必要的 AWS Config 錄製資源：AWS::EC2::Instance、
AWS::SSM::ManagedInstanceInventory

AWS Config 規則：[ec2-instance-managed-by-systems-manager](#)

排程類型：已觸發變更

參數：無

此控制項會檢查您帳戶中已停止和執行的 EC2 執行個體是否由 管理 AWS Systems Manager。Systems Manager 是 AWS 服務，可用來檢視和控制您的 AWS 基礎設施。

為了協助您維護安全性和合規性，Systems Manager 會掃描已停止和執行的受管執行個體。受管執行個體是設定為與 Systems Manager 搭配使用的機器。Systems Manager 接著會針對偵測到的任何政策違規進行報告或採取修正動作。Systems Manager 也可協助您設定和維護受管執行個體。若要進一步了解，請參閱 [AWS Systems Manager 使用者指南](#)。

Note

此控制項會針對由 管理的 AWS 彈性災難復原 複寫伺服器執行個體的 EC2 執行個體產生 FAILED 問題清單 AWS。Replication Server 執行個體是由 自動啟動的 EC2 執行個體 AWS 彈性災難復原，可支援來源伺服器的持續資料複寫。會 AWS 刻意從這些執行個體中移除 Systems Manager (SSM) 代理程式，以維持隔離並協助防止潛在的意外存取路徑。

修補

如需有關使用 管理 EC2 執行個體的資訊 AWS Systems Manager，請參閱 AWS Systems Manager [《使用者指南》中的 Amazon EC2 主機管理](#)。在 AWS Systems Manager 主控台的組態選項區段中，您可以保留預設設定，或視需要針對您偏好的組態進行變更。

【SSM.2】 Systems Manager 管理的 Amazon EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態

相關要求：NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 SI-2、NIST.800-53.r5 SI-2(2)、NIST.800-53.r5 SI-2(3)、NIST.800-53.r5 SI-2(4)、NIST.800-53.r5 SI-2(5)、NIST.800-171.r2 3.7.1、PCI DSS v3.2.1/6.2、PCI DSS v4.0.1/2.1/6.3.3.3

類別：偵測 > 偵測服務

嚴重性：高

資源類型：AWS::SSM::PatchCompliance

AWS Config 規則：[ec2-managedinstance-patch-compliance-status-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Systems Manager 修補程式合規的合規狀態是否在執行個體上安裝修補程式 COMPLIANT/NON_COMPLIANT 之後。如果合規狀態為 `NON_COMPLIANT`，則控制項會失敗。控制項只會檢查由 Systems Manager Patch Manager 管理的執行個體。

視需要修補 EC2 執行個體可減少您組織的受攻擊面 AWS 帳戶。

修補

Systems Manager 建議使用 [修補程式政策](#) 來設定受管執行個體的修補。您也可以使用 [Systems Manager 文件](#) 來修補執行個體，如下列程序所述。

修補不相容的修補程式

1. 在 <https://console.aws.amazon.com/systems-manager/> 開啟 AWS Systems Manager 主控台。
2. 針對節點管理，選擇執行命令，然後選擇執行命令。
3. 選擇 AWS-RunPatchBaseline 的選項。
4. 將 Operation (操作) 變更為 Install (安裝)。
5. 選擇手動選擇執行個體，然後選擇不合規的執行個體。
6. 選擇執行。
7. 命令完成後，若要監控修補執行個體的新合規狀態，請在導覽窗格中選擇合規。

【SSM.3】 Systems Manager 管理的 Amazon EC2 執行個體應具有 COMPLIANT 的關聯合規狀態

相關要求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2、NIST.800-53.r5 CM-2(2)、NIST.800-53.r5 CM-8、NIST.800-53.r5 CM-8(1)、NIST.800-53.r5 CM-8(3)、NIST.800-53.r5 SI-2(3)、PCI DSS v3.2.1/2.4、PCI DSS v4.0.1/2.2.1、PCI v4.0.1/6.3.3.3

類別：偵測 > 偵測服務

嚴重性：低

資源類型：AWS::SSM::AssociationCompliance

AWS Config 規則：[ec2-managedinstance-association-compliance-status-check](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS Systems Manager 關聯合規的狀態是 COMPLIANT 還是在執行個體上執行關聯NON_COMPLIANT之後。如果關聯合規狀態為 `NON_COMPLIANT`，則控制項會失敗NON_COMPLIANT。

狀態管理員關聯是指派給受管執行個體的組態。該組態會定義您想在執行個體上維持的狀態。例如，關聯可以指定必須在您的執行個體上安裝和執行防毒軟體，或特定連接埠必須關閉。

建立一或多個狀態管理員關聯後，您即可立即取得合規狀態資訊。您可以在主控台中檢視合規狀態，或回應 AWS CLI 命令或對應的 Systems Manager API 動作。對於關聯，組態合規會顯示合規狀態 (Compliant 或 Non-compliant)。它也會顯示指派給關聯的嚴重性等級，例如 Critical或 Medium。

若要進一步了解 State Manager 關聯合規，請參閱AWS Systems Manager 《使用者指南》中的[關於 State Manager 關聯合規](#)。

修補

失敗的關聯可以與不同的物件相關，包括目標和 Systems Manager 文件名稱。若要修復此問題，您必須先檢視關聯歷史記錄來識別和調查關聯。如需檢視關聯歷史記錄的說明，請參閱AWS Systems Manager 《使用者指南》中的[檢視關聯歷史記錄](#)。

調查之後，您可以編輯關聯以修正已識別的問題。您可以編輯關聯來指定新的名稱、排程、嚴重性層級或目標。編輯關聯後，會 AWS Systems Manager 建立新的版本。如需編輯關聯的指示，請參閱AWS Systems Manager 《使用者指南》中的[編輯和建立新版本的關聯](#)。

【SSM.4】 SSM 文件不應公開

相關需求：NIST.800-53.r5 AC-21、NIST.800-53.r5 AC-3、NIST.800-53.r5 AC-3(7)、NIST.800-53.r5 AC-4、NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 AC-6、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(20)、NIST.800-53.r5 SC-7 、

類別：保護 > 安全網路組態 > 不可公開存取的資源

嚴重性：嚴重

資源類型：AWS::SSM::Document

AWS Config 規則：[ssm-document-not-public](#)

排程類型：定期

參數：無

此控制項會檢查帳戶擁有 AWS Systems Manager 的文件是否為公有。如果擁有 Self 作為擁有者的 Systems Manager 文件為公有，則控制項會失敗。

Systems Manager 公有文件可能會允許意外存取您的文件。公有 Systems Manager 文件可以公開有關您的帳戶、資源和內部程序的寶貴資訊。

除非您的使用案例需要公開共用，否則建議您封鎖將 Self 做為擁有者的 Systems Manager 文件的公開共用。

修補

如需設定 Systems Manager 文件共用的相關資訊，請參閱AWS Systems Manager 《使用者指南》中的[共用 SSM 文件](#)。

【SSM.5】 SSM 文件應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::SSM::Document

AWS Config 規則：[ssm-document-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Systems Manager 文件是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果文件沒有任何標籤索引鍵，或者它沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果文件沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，系統標籤會自動套用並具有 aws：字首。控制項不會評估 Amazon 擁有的 Systems Manager 文件。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的 [根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱 [標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多存取 AWS 服務。它們不適用於私有或敏感資料。

修補

若要將標籤新增至 AWS Systems Manager 文件，您可以使用 AWS Systems Manager API 的 [AddTagsToResource](#) 操作，或者，如果您使用的是 AWS CLI，請執行 [add-tags-to-resource](#) 命令。您也可以使用 AWS Systems Manager 主控台。

【SSM.6】SSM Automation 應該啟用 CloudWatch 記錄

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::::Account

AWS Config 規則：[ssm-automation-logging-enabled](#)

排程類型：定期

參數：無

此控制項會檢查 AWS Systems Manager (SSM) 自動化是否已啟用 Amazon CloudWatch 記錄。如果未針對 SSM Automation 啟用 CloudWatch 記錄，則控制項會失敗。

SSM Automation 是一種 AWS Systems Manager 工具，可協助您建置自動化解決方案，以使用預先定義的或自訂 Runbook 大規模部署、設定和管理 AWS 資源。為了符合組織的營運或安全需求，您可能需要提供其執行指令碼的記錄。您可以設定 SSM Automation 將輸出從 Runbook 中的 `aws:executeScript` 動作傳送至您指定的 Amazon CloudWatch Logs 日誌群組。您可使用 CloudWatch Logs 從各種 AWS 服務中監控、存放及存取日誌檔案。

修補

如需有關為 SSM 自動化啟用 CloudWatch 記錄的資訊，請參閱 AWS Systems Manager 《使用者指南》中的 [使用 CloudWatch Logs 記錄自動化動作輸出](#)。

【SSM.7】SSM 文件應啟用封鎖公開共用設定

類別：保護 > 安全存取管理 > 資源不可公開存取

嚴重性：嚴重

資源類型：AWS::::Account

AWS Config 規則：[ssm-automation-block-public-sharing](#)

排程類型：定期

參數：無

此控制項會檢查是否已啟用文件的 AWS Systems Manager 封鎖公開共用設定。如果停用 Systems Manager 文件的封鎖公開共用設定，則控制項會失敗。

AWS Systems Manager (SSM) 文件的封鎖公開共用設定是帳戶層級設定。啟用此設定可防止對 SSM 文件進行不必要的存取。如果您啟用此設定，您的變更不會影響您目前與公眾共用的任何 SSM 文件。除非您的使用案例要求您與公有共享 SSM 文件，否則建議您啟用封鎖公有共享設定。每個的設定可能有所不同 AWS 區域。

修補

如需有關為 AWS Systems Manager (SSM) 文件啟用封鎖公開共用設定的資訊，請參閱AWS Systems Manager 《使用者指南》中的[封鎖 SSM 文件的公開共用](#)。

的 Security Hub CSPM 控制項 AWS Transfer Family

這些 AWS Security Hub CSPM 控制項會評估 AWS Transfer Family 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【Transfer.1】 AWS Transfer Family 工作流程應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Transfer::Workflow

AWS Config rule：tagged-transfer-workflow (自訂 Security Hub CSPM 規則)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredTagKeys	評估資源必須包含的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	No default value

此控制項會檢查 AWS Transfer Family 工作流程是否具有具有參數 中定義之特定金鑰的標籤requiredTagKeys。如果工作流程沒有任何標籤索引鍵，或沒有參數 中指定的所有索引鍵，則控制項會失敗requiredTagKeys。如果requiredTagKeys未提供 參數，則控制項只會檢查標籤索引鍵是否存在，如果工作流程未標記任何索引鍵，則 會失敗。系統會aws:忽略自動套用並以 開頭的系統標籤。

標籤是您指派給 AWS 資源的標籤，由索引鍵和選用值組成。您可建立標籤，以依照用途、擁有者、環境或其他條件分類資源。標籤可協助您識別、組織、搜尋和篩選資源。標記也可協助您追蹤動作和通知的責任資源擁有者。使用標記時，您可以實作屬性型存取控制 (ABAC) 做為授權策略，以根據標籤定義

許可。您可以將標籤連接至 IAM 實體（使用者或角色）和 AWS 資源。您可以為 IAM 主體建立單一 ABAC 政策或一組單獨的政策。您可以設計這些 ABAC 政策，以便在委託人的標籤符合資源標籤時允許操作。如需詳細資訊，請參閱《IAM 使用者指南》中的[什麼是 ABAC AWS？](#)。

Note

請勿在標籤中新增個人身分識別資訊 (PII) 或其他機密或敏感資訊。許多 都可以存取標籤 AWS 服務，包括 AWS Billing。如需更多標記最佳實務，請參閱《》中的[標記您的 AWS 資源](#) AWS 一般參考。

修補

將標籤新增至 Transfer Family 工作流程（主控台）

1. 開啟 AWS Transfer Family 主控台。
2. 在導覽窗格中，選擇 Workflows (工作流程)。然後，選取您要標記的工作流程。
3. 選擇管理標籤，然後新增標籤。

【Transfer.2】 Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線

相關要求：NIST.800-53.r5 CM-7、NIST.800-53.r5 IA-5、NIST.800-53.r5 SC-8、PCI DSS v4.0.1/4.2.1

類別：保護 > 資料保護 > data-in-transit加密

嚴重性：中

資源類型：AWS::Transfer::Server

AWS Config 規則：[transfer-family-server-no-ftp](#)

排程類型：定期

參數：無

此控制項會檢查 AWS Transfer Family 伺服器是否使用 FTP 以外的通訊協定進行端點連線。如果伺服器使用 FTP 通訊協定讓用戶端連線至伺服器的端點，則控制項會失敗。

FTP（檔案傳輸通訊協定）透過未加密的頻道建立端點連線，讓透過這些頻道傳送的資料容易遭到攔截。使用 SFTP (SSH 檔案傳輸通訊協定)、FTPS（檔案傳輸通訊協定安全）或 AS2（適用性聲明

2) 可加密傳輸中的資料，提供額外的安全層，並可用來協助防止潛在攻擊者使用 person-in-the-middle 或類似攻擊來竊聽或控制網路流量。

修補

若要修改 Transfer Family 伺服器的通訊協定，請參閱AWS Transfer Family 《使用者指南》中的[編輯檔案傳輸通訊協定](#)。

【Transfer.3】 Transfer Family 連接器應該已啟用記錄

相關要求：NIST.800-53.r5 AC-2(12)、NIST.800-53.r5 AC-2(4)、NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AC-6(9)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.8000-5.r5)、AU-6NIST.5 AU-9 CA-7 NIST.800-53.r5 SC-7 SI-3 SI-4 SI-7

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::Transfer::Connector

AWS Config 規則：[transfer-connector-logging-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查連接器是否已啟用 Amazon CloudWatch 記錄 AWS Transfer Family。如果未為連接器啟用 CloudWatch 記錄，則控制項會失敗。

Amazon CloudWatch 是一種監控和可觀測性服務，可讓您查看 AWS 資源，包括 AWS Transfer Family 資源。對於 Transfer Family，CloudWatch 提供工作流程進度和結果的合併稽核和記錄。這包括 Transfer Family 為工作流程定義的數個指標。您可以設定 Transfer Family 在 CloudWatch 中自動記錄連接器事件。若要這樣做，請為連接器指定記錄角色。對於記錄角色，您可以建立 IAM 角色和以資源為基礎的 IAM 政策，以定義角色的許可。

修補

如需有關為 Transfer Family 連接器啟用 CloudWatch 記錄的資訊，請參閱AWS Transfer Family 《使用者指南》中的[AWS Transfer Family 伺服器的 Amazon CloudWatch 記錄](#)。

【Transfer.4】 Transfer Family 協議應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Transfer::Agreement

AWS Config 規則：[transfer-agreement-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求 的標籤金鑰。	無預設值

此控制項會檢查 AWS Transfer Family 協議是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果協議沒有任何標籤索引鍵，或其沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果協議沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws: 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需有關將標籤新增至 AWS Transfer Family 協議的資訊，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[資源標記方法](#)。

【Transfer.5】 Transfer Family 憑證應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Transfer::Certificate

AWS Config 規則：[transfer-certificate-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Transfer Family 憑證是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果憑證沒有任何標籤索引鍵，或沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果憑證沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws: 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需有關將標籤新增至 AWS Transfer Family 憑證的資訊，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[資源標記方法](#)。

【Transfer.6】 Transfer Family 連接器應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Transfer::Connector

AWS Config 規則：[transfer-connector-tagged](#)

排程類型：已觸發變更

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Transfer Family 連接器是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果連接器沒有任何標籤索引鍵，或沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果連接器沒有任何標籤索引鍵，則會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws: 字首。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多 存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需將標籤新增至 AWS Transfer Family 連接器的詳細資訊，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[資源標記方法](#)。

【Transfer.7】 轉移系列設定檔應加上標籤

類別：識別 > 庫存 > 標記

嚴重性：低

資源類型：AWS::Transfer::Profile

AWS Config 規則：[transfer-profile-tagged](#)

排程類型：變更已觸發

參數：

參數	說明	Type	允許自訂值	Security Hub CSPM 預設值
requiredKeyTags	必須指派給評估資源的非系統標籤索引鍵清單。標籤金鑰會區分大小寫。	StringList (最多 6 個項目)	1–6 個符合 AWS 要求的標籤金鑰 。	無預設值

此控制項會檢查 AWS Transfer Family 設定檔是否具有 requiredKeyTags 參數指定的標籤索引鍵。如果設定檔沒有任何標籤索引鍵，或沒有 requiredKeyTags 參數指定的所有索引鍵，則控制項會失敗。如果您未指定 requiredKeyTags 參數的任何值，則控制項只會檢查標籤索引鍵是否存在，如果設定檔沒有任何標籤索引鍵，則 會失敗。控制項會忽略系統標籤，這些標籤會自動套用並具有 aws：字首。控制項會評估本機設定檔和合作夥伴設定檔。

標籤是您建立並指派給 AWS 資源的標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。您可以使用標籤，依用途、擁有者、環境或其他條件來分類資源。他們可以協助您識別、組織、搜尋和篩

選資源。他們也可以協助您追蹤資源擁有者的動作和通知。您也可以使用標籤來實作屬性型存取控制 (ABAC) 做為授權策略。如需 ABAC 策略的詳細資訊，請參閱《IAM 使用者指南》中的[根據具有 ABAC 授權的屬性定義許可](#)。如需標籤的詳細資訊，請參閱[標記 AWS 資源和標籤編輯器使用者指南](#)。

Note

請勿將個人識別資訊 (PII) 或其他機密或敏感資訊儲存在標籤中。標籤可從許多 存取 AWS 服務。它們不適用於私有或敏感資料。

修補

如需將標籤新增至 AWS Transfer Family 設定檔的詳細資訊，請參閱《標記 AWS 資源和標籤編輯器使用者指南》中的[資源標記方法](#)。

的 Security Hub CSPM 控制項 AWS WAF

這些 AWS Security Hub CSPM 控制項會評估 AWS WAF 服務和資源。控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【WAF.1】應啟用 AWS WAF 傳統全域 Web ACL 記錄

相關需求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(9)、NIST.800-53.r5 SI-7(8)、PCIv40.10.10.4.2。

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::WAF::WebACL

AWS Config 規則：[waf-classic-logging-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否啟用 AWS WAF 全域 Web ACL 的記錄。如果 Web ACL 未啟用記錄，則此控制項會失敗。

記錄是維護 AWS WAF 全域可靠性、可用性和效能的重要部分。這是許多組織的業務和合規要求，可讓您對應用程式行為進行疑難排解。它也提供所連接 Web ACL 所分析流量的詳細資訊 AWS WAF。

修補

若要啟用 AWS WAF Web ACL 的記錄，請參閱《AWS WAF 開發人員指南》中的[記錄 Web ACL 流量資訊](#)。

【WAF.2】 AWS WAF 傳統區域規則應至少有一個條件

相關要求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::WAFRegional::Rule

AWS Config 規則：[waf-regional-rule-not-empty](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 區域規則是否具有至少一個條件。如果規則中沒有條件，則控制項會失敗。

WAF 區域規則可以包含多個條件。規則的條件允許流量檢查，並採取定義的動作（允許、封鎖或計數）。如果沒有任何條件，流量會通過而不進行檢查。沒有條件但具有建議允許、封鎖或計數之名稱或標籤的 WAF 區域規則，可能會導致錯誤地假設發生其中一個動作。

修補

若要將條件新增至空白規則，請參閱《AWS WAF 開發人員指南》中的[在規則中新增和移除條件](#)。

【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則

相關需求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::WAFRegional::RuleGroup

AWS Config 規則：[waf-regional-rulegroup-not-empty](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 區域規則群組是否至少有一個規則。如果規則群組中沒有規則，則控制項會失敗。

WAF 區域規則群組可以包含多個規則。規則的條件允許流量檢查，並採取定義的動作（允許、封鎖或計數）。如果沒有任何規則，流量會通過而不進行檢查。沒有規則但具有建議允許、封鎖或計數之名稱或標籤的 WAF 區域規則群組，可能會導致錯誤的假設發生其中一個動作。

修補

若要將規則和規則條件新增至空白規則群組，請參閱《AWS WAF 開發人員指南》中的[從 AWS WAF Classic 規則群組新增和刪除規則](#)，以及[新增和移除規則中的條件](#)。

【WAF.4】AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::WAFRegional::WebACL

AWS Config 規則：[waf-regional-webacl-not-empty](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF Classic 區域性 Web ACL 是否包含任何 WAF 規則或 WAF 規則群組。如果 Web ACL 不包含任何 WAF 規則或規則群組，則此控制項會失敗。

WAF 區域 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 請求。如果 Web ACL 是空的，則 Web 流量可以通過，而不會被 WAF 偵測到或對其採取動作，具體取決於預設動作。

修補

若要將規則或規則群組新增至空白的 AWS WAF Classic Regional Web ACL，請參閱《AWS WAF 開發人員指南》中的[編輯 Web ACL](#)。

【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::WAF::Rule

AWS Config 規則：[waf-global-rule-not-empty](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 全域規則是否包含任何條件。如果規則中沒有條件，則控制項會失敗。

WAF 全域規則可以包含多個條件。規則的條件允許流量檢查，並採取定義的動作（允許、封鎖或計數）。如果沒有任何條件，流量會通過而不進行檢查。沒有條件但具有建議允許、封鎖或計數之名稱或標籤的 WAF 全域規則，可能會導致錯誤地假設發生其中一個動作。

修補

如需建立規則和新增條件的說明，請參閱《AWS WAF 開發人員指南》中的[建立規則和新增條件](#)。

【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::WAF::RuleGroup

AWS Config 規則：[waf-global-rulegroup-not-empty](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 全域規則群組是否至少有一個規則。如果規則群組中沒有規則，則控制項會失敗。

WAF 全域規則群組可以包含多個規則。規則的條件允許流量檢查，並採取定義的動作（允許、封鎖或計數）。如果沒有任何規則，流量會通過而不進行檢查。沒有規則但具有建議允許、封鎖或計數之名稱或標籤的 WAF 全域規則群組，可能會導致錯誤地假設發生其中一個動作。

修補

如需將規則新增至規則群組的指示，請參閱《AWS WAF 開發人員指南》中的[建立 AWS WAF Classic 規則群組](#)。

【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組

相關要求：NIST.800-53.r5 AC-4(21)、NIST.800-53.r5 SC-7、NIST.800-53.r5 SC-7(11)、NIST.800-53.r5 SC-7(16)、NIST.800-53.r5 SC-7(21)

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::WAF::WebACL

AWS Config 規則：[waf-global-webacl-not-empty](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 全域 Web ACL 是否包含至少一個 WAF 規則或 WAF 規則群組。如果 Web ACL 不包含任何 WAF 規則或規則群組，則控制項會失敗。

WAF 全域 Web ACL 可以包含規則和規則群組的集合，以檢查和控制 Web 請求。如果 Web ACL 是空的，則 Web 流量可以通過，而不會被 WAF 偵測到或對其採取動作，具體取決於預設動作。

修補

若要將規則或規則群組新增至空白的 AWS WAF 全域 Web ACL，請參閱《AWS WAF 開發人員指南》中的[編輯 Web ACL](#)。針對篩選條件，選擇全域 (CloudFront)。

【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組

相關需求：NIST.800-53.r5 CA-9(1)、NIST.800-53.r5 CM-2

類別：保護 > 安全網路組態

嚴重性：中

資源類型：AWS::WAFv2::WebACL

AWS Config 規則：[wafv2-webacl-not-empty](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 an AWS WAF V2 Web 存取控制清單 (Web ACL) 是否包含至少一個規則或規則群組。如果 Web ACL 不包含任何規則或規則群組，則控制項會失敗。

Web ACL 可讓您精細控制受保護資源回應的所有 HTTP(S) Web 請求。Web ACL 應包含規則和規則群組的集合，以檢查和控制 Web 請求。如果 Web ACL 是空的，AWS WAF 則 Web 流量可以通過，而不會被偵測到或由 根據預設動作採取動作。

修補

若要將規則或規則群組新增至空的 WAFV2 Web ACL，請參閱《AWS WAF 開發人員指南》中的[編輯 Web ACL](#)。

【WAF.11】應該啟用 AWS WAF Web ACL 記錄

相關要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(950.5)、NIST.50 SI-710.4.25

類別：識別 > 記錄日誌

嚴重性：低

資源類型：AWS::WAFv2::WebACL

AWS Config 規則：[wafv2-logging-enabled](#)

排程類型：定期

參數：無

此控制項會檢查是否針對 an AWS WAF V2 Web 存取控制清單 (Web ACL) 啟用記錄。如果 Web ACL 的記錄已停用，則此控制項會失敗。

 Note

此控制項不會檢查是否透過 Amazon Security Lake 為帳戶啟用 AWS WAF Web ACL 記錄。

記錄可維護的可靠性、可用性和效能 AWS WAF。此外，記錄是許多組織中的商業和合規要求。透過記錄 Web ACL 分析的流量，您可以對應用程式行為進行疑難排解。

修補

若要啟用 AWS WAF Web ACL 的記錄，請參閱《AWS WAF 開發人員指南》中的[管理 Web ACL 的記錄](#)。

【WAF.12】AWS WAF 規則應啟用 CloudWatch 指標

相關要求：NIST.800-53.r5 AC-4(26)、NIST.800-53.r5 AU-10、NIST.800-53.r5 AU-12、NIST.800-53.r5 AU-2、NIST.800-53.r5 AU-3、NIST.800-53.r5 AU-6(3)、NIST.800-53.r5 AU-6(4)、NIST.800-53.r5 CA-7、NIST.800-53.r5 SC-7(10)、NIST.800-53.r5 SC-7(9)、NIST.5050.5 SI-70

類別：識別 > 記錄日誌

嚴重性：中

資源類型：AWS::WAFv2::RuleGroup

AWS Config 規則：[wafv2-rulegroup-logging-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 AWS WAF 規則或規則群組是否已啟用 Amazon CloudWatch 指標。如果規則或規則群組未啟用 CloudWatch 指標，則控制項會失敗。

在 AWS WAF 規則和規則群組上設定 CloudWatch 指標可提供流量的可見性。您可以查看觸發哪些 ACL 規則，以及接受和封鎖哪些請求。此可見性可協助您識別相關聯資源上的惡意活動。

修補

若要在 AWS WAF 規則群組上啟用 CloudWatch 指標，請叫用 [UpdateRuleGroup](#) API。

若要在 AWS WAF 規則上啟用 CloudWatch 指標，請叫用 [UpdateWebACL](#) API。將

CloudWatchMetricsEnabled 欄位設定為 true。當您使用 AWS WAF 主控台建立規則或規則群組時，會自動啟用 CloudWatch 指標。

WorkSpaces 的 Security Hub CSPM 控制項

這些 AWS Security Hub CSPM 控制項會評估 Amazon WorkSpaces 服務和資源。

這些控制項可能無法全部使用 AWS 區域。如需詳細資訊，請參閱[依區域的控制項可用性](#)。

【WorkSpaces.1】應靜態加密 WorkSpaces 使用者磁碟區

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::WorkSpaces::Workspace

AWS Config 規則：[workspaces-user-volume-encryption-enabled](#)

排程類型：變更已觸發

參數：無

此控制項會檢查 Amazon WorkSpaces Workspace 中的使用者磁碟區是否靜態加密。如果 Workspace 使用者磁碟區未靜態加密，則控制項會失敗。

靜態資料是指存放在持久性、非揮發性儲存體中任何持續時間的資料。加密靜態資料可協助您保護其機密性，進而降低未經授權的使用者可存取資料的風險。

修補

若要加密 WorkSpaces 使用者磁碟區，請參閱《Amazon [WorkSpaces 管理指南](#)》中的加密 Workspace。Amazon WorkSpaces

【WorkSpaces.2】WorkSpaces 根磁碟區應靜態加密

類別：保護 > 資料保護 > data-at-rest加密

嚴重性：中

資源類型：AWS::WorkSpaces::Workspace

AWS Config 規則：[workspaces-root-volume-encryption-enabled](#)

排程類型：已觸發變更

參數：無

此控制項會檢查 Amazon WorkSpaces Workspace 中的根磁碟區是否靜態加密。如果 Workspace 根磁碟區未靜態加密，則控制項會失敗。

靜態資料是指存放在持久性、非揮發性儲存體中任何持續時間的資料。加密靜態資料可協助您保護其機密性，進而降低未經授權的使用者可存取資料的風險。

修補

若要加密 WorkSpaces 根磁碟區，請參閱《Amazon [WorkSpaces 管理指南](#)》中的[加密 Workspace](#)。Amazon WorkSpaces

在 Security Hub CSPM 中設定控制項所需的許可

若要檢視安全控制的相關資訊，並在標準中啟用和停用安全控制，您用來存取 AWS Security Hub CSPM 的 AWS Identity and Access Management (IAM) 角色需要許可，才能呼叫 Security Hub CSPM API 的下列操作。

若要取得必要的許可，您可以使用 [Security Hub CSPM 受管政策](#)。或者，您可以更新自訂 IAM 政策，以包含這些動作的許可。

- [BatchGetSecurityControls](#) – 傳回目前帳戶和之安全控制批次的相關資訊 AWS 區域。
- [ListSecurityControlDefinitions](#) – 傳回適用於指定標準之安全控制的相關資訊。
- [ListStandardsControlAssociations](#) – 識別帳戶中每個啟用的標準目前是否在 中啟用或停用安全控制。
- [BatchGetStandardsControlAssociations](#) – 對於一批安全控制項，會識別目前是否在指定的標準中啟用或停用每個控制項。
- [BatchUpdateStandardsControlAssociations](#) – 用來在包含控制項的標準中啟用安全控制項，或在標準中停用控制項。這是現有[UpdateStandardsControl](#)操作的批次取代。
- [BatchUpdateStandardsControlAssociations](#) – 用來啟用或停用包含控制項之標準中的一批安全控制項。這是現有[UpdateStandardsControl](#)操作的批次取代。
- [UpdateStandardsControl](#) – 用來啟用或停用包含控制項之標準中的單一安全控制項
- [DescribeStandardsControl](#) – 傳回指定安全控制的詳細資訊。

除了上述 APIs，您應該新增呼叫 BatchGetControlEvaluations IAM 角色的許可。檢視控制項的啟用和合規狀態、控制項的問題清單計數，以及 Security Hub CSPM 主控台上控制項的整體安全分數

時，需要此許可。由於只有主控台呼叫 `BatchGetControlEvaluations`，此許可不會直接對應至公開記錄的 Security Hub CSPM APIs 或 AWS CLI 命令。

在 Security Hub CSPM 中啟用控制項

在 AWS Security Hub CSPM 中，控制項是安全標準中的保護措施，可協助組織保護資訊的機密性、完整性和可用性。每個 Security Hub CSPM 控制項都與特定 AWS 資源相關。當您啟用控制項時，Security Hub CSPM 會開始執行控制項的安全檢查，並為其產生問題清單。計算安全分數時，Security Hub CSPM 也會考慮所有啟用的控制項。

您可以選擇在其套用的所有安全標準中啟用控制項。或者，您可以在不同的標準中以不同的方式設定啟用狀態。我們建議使用前一個選項，其中控制項的啟用狀態會與所有已啟用的標準保持一致。如需在套用控制項的所有標準中啟用控制項的指示，請參閱 [啟用跨標準的控制](#)。如需在特定標準中啟用控制項的指示，請參閱 [在特定標準中啟用控制項](#)。

如果您啟用跨區域彙總並登入彙總區域，Security Hub CSPM 主控台會顯示至少一個連結區域中可用的控制項。如果控制項可在連結區域中使用，但無法在彙總區域中使用，則您無法從彙總區域啟用或停用該控制項。

您可以使用 Security Hub CSPM 主控台、Security Hub CSPM API 或來啟用和停用每個區域中的控制項 AWS CLI。

啟用和停用控制項的指示會根據您是否使用[中央組態](#)而有所不同。本主題說明差異。整合 Security Hub CSPM 和的使用者可使用中央組態 AWS Organizations。建議使用中央組態來簡化在多帳戶、多區域環境中啟用和停用控制項的程序。如果您使用中央組態，您可以透過使用組態政策跨多個帳戶和區域啟用控制項。如果您不使用中央組態，則必須在每個區域和帳戶中分別啟用控制項。

啟用跨標準的控制

我們建議在套用控制項的所有標準中啟用 AWS Security Hub CSPM 控制。如果您開啟合併的控制項問題清單，即使控制項屬於多個標準，每個控制項檢查也會收到一個問題清單。

多帳戶、多區域環境中的跨標準啟用

若要跨多個 AWS 帳戶和啟用安全控制 AWS 區域，您必須登入委派的 Security Hub CSPM 管理員帳戶，並使用[中央組態](#)。

在中央組態下，委派管理員可以建立 Security Hub CSPM 組態政策，以跨已啟用的標準啟用指定的控制項。然後，您可以將組態政策與特定帳戶和組織單位 (OUs或根建立關聯。組態政策會在您的主要區域（也稱為彙總區域）和所有連結區域生效。

組態政策提供自訂功能。例如，您可以選擇在一個 OU 中啟用所有控制項，也可以選擇在另一個 OU 中僅啟用 Amazon Elastic Compute Cloud (EC2) 控制項。精細程度取決於組織中安全涵蓋範圍的預期目標。如需建立啟用跨標準指定控制項之組態政策的說明，請參閱 [建立和關聯組態政策](#)。

Note

委派管理員可以建立組態政策，以管理[服務受管標準以外的所有標準中的控制項](#)：[AWS Control Tower](#)此標準的控制項應在 AWS Control Tower 服務中設定。

如果您希望某些帳戶設定自己的控制項，而不是委派管理員，委派管理員可以將這些帳戶指定為自我管理。自我管理帳戶必須在每個區域中分別設定控制項。

單一帳戶和區域中的跨標準啟用

如果您不使用中央組態或 是自我管理帳戶，則無法使用組態政策在多個帳戶和區域中集中啟用控制項。不過，您可以使用下列步驟，在單一帳戶和區域中啟用控制項。

Security Hub CSPM console

在一個帳戶和區域中啟用跨標準的控制

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 從導覽窗格中選擇控制項。
3. 選擇已停用索引標籤。
4. 選擇控制項旁的選項。
5. 選擇啟用控制（此選項不會針對已啟用的控制項顯示）。
6. 在您要啟用控制項的每個區域中重複此步驟。

Security Hub CSPM API

在一個帳戶和區域中啟用跨標準的控制

1. 叫用 [ListStandardsControlAssociations](#) API。提供安全控制 ID。

請求範例：

```
{
```

```
"SecurityControlId": "IAM.1"
}
```

2. 叫用 [BatchUpdateStandardsControlAssociations](#) API。提供未啟用控制項的任何標準的 Amazon Resource Name (ARN)。若要取得標準 ARNs，請執行 [DescribeStandards](#)。
3. 將 AssociationStatus 參數設定為等於 ENABLED。如果您針對已啟用的控制項遵循這些步驟，API 會傳回 HTTP 狀態碼 200 回應。

請求範例：

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. 在您要啟用控制項的每個區域中重複此步驟。

AWS CLI

在一個帳戶和區域中啟用跨標準的控制

1. 執行 [list-standards-control-associations](#) 命令。提供安全控制 ID。

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. 執行 [batch-update-standards-control-associations](#) 命令。提供未啟用控制項的任何標準的 Amazon Resource Name (ARN)。若要取得標準 ARNs，請執行 describe-standards 命令。
3. 將 AssociationStatus 參數設定為等於 ENABLED。如果您針對已啟用的控制項遵循這些步驟，命令會傳回 HTTP 狀態碼 200 回應。

```
aws securityhub --region us-east-1 batch-update-standards-control-associations
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/v/1.4.0", "AssociationStatus": "ENABLED"}]'
```


4. 在您要啟用控制項的每個區域中重複此步驟。

在特定標準中啟用控制項

當您在 AWS Security Hub CSPM 中啟用標準時，所有適用於它的控制項都會在該標準中自動啟用（此服務的例外狀況是服務受管標準）。然後，您可以在標準中停用並重新啟用特定控制項。不過，我們建議您在所有啟用的標準中調整控制項的啟用狀態。如需跨所有標準啟用控制項的指示，請參閱 [啟用跨標準的控制](#)。

標準的詳細資訊頁面包含標準適用的控制項清單，以及目前在該標準中啟用和停用哪些控制項的相關資訊。

在標準詳細資訊頁面上，您也可以特定標準中啟用控制項。您必須在每個 AWS 帳戶和中分別啟用特定標準的控制項 AWS 區域。當您在特定標準中啟用控制項時，它只會影響目前的帳戶和區域。

若要在標準中啟用控制項，您必須先啟用至少一個控制項適用的標準。如需啟用標準的指示，請參閱 [啟用安全標準](#)。當您在一或多個標準中啟用控制項時，Security Hub CSPM 會開始為該控制項產生問題清單。Security Hub CSPM 在計算整體安全分數和標準安全分數時包含 [控制狀態](#)。即使您在多個標準中啟用控制，如果您開啟合併控制問題清單，則每個標準之間的安全檢查都會收到單一問題清單。如需了解更多資訊，請參閱 [合併的控制調查結果](#)。

若要在標準中啟用控制項，該控制項必須在您目前的區域中可用。如需詳細資訊，請參閱 [依區域控制可用性](#)。

請依照下列步驟，在特定標準中啟用 Security Hub CSPM 控制項。您也可以使用 [UpdateStandardsControl](#) API 動作來啟用特定標準的控制項，以取代下列步驟。如需在所有標準中啟用控制項的指示，請參閱 [單一帳戶和區域中的跨標準啟用](#)。

Security Hub CSPM console

在特定標準中啟用控制項

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 從導覽窗格中選擇安全標準。
3. 選擇 檢視相關標準的結果。
4. 選取控制項。

5. 選擇啟用控制（此選項不會針對已啟用的控制項顯示）。選擇啟用來確認。

Security Hub CSPM API

在特定標準中啟用控制項

1. 執行 [ListSecurityControlDefinitions](#)，並提供標準 ARN，以取得特定標準的可用控制項清單。若要取得標準 ARN，請執行 [DescribeStandards](#)。此 API 會傳回標準無關的安全控制 IDs，而非標準特定的控制 IDs。

請求範例：

```
{
  "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. 執行 [ListStandardsControlAssociations](#)，並提供特定的控制項 ID，以傳回每個標準中控制項的目前啟用狀態。

請求範例：

```
{
  "SecurityControlId": "IAM.1"
}
```

3. 執行 [BatchUpdateStandardsControlAssociations](#)。提供您要啟用控制項之標準 ARN。
4. 將 AssociationStatus 參數設定為等於 ENABLED。

請求範例：

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

在特定標準中啟用控制項

1. 執行 [list-security-control-definitions](#) 命令，並提供標準 ARN，以取得特定標準的可用控制項清單。若要取得標準 ARN，請執行 describe-standards。此命令會傳回標準無關的安全控制 IDs，而不是標準特定的控制 IDs。

```
aws securityhub --region us-east-1 list-security-control-definitions --  
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-  
security-best-practices/v/1.0.0"
```

2. 執行 [list-standards-control-associations](#) 命令，並提供特定的控制項 ID，以傳回每個標準中控制項的目前啟用狀態。

```
aws securityhub --region us-east-1 list-standards-control-associations --  
security-control-id CloudTrail.1
```

3. 執行 [batch-update-standards-control-associations](#) 命令。提供您要啟用控制項之標準 ARN。
4. 將 AssociationStatus 參數設定為等於 ENABLED。

```
aws securityhub --region us-east-1 batch-update-standards-control-associations  
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",  
"StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-  
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

在已啟用的標準中自動啟用新控制項

AWS Security Hub CSPM 會定期發行新的控制項，並將其新增至一或多個標準。您可以選擇是否要在已啟用的標準中自動啟用新控制項。

建議使用 Security Hub CSPM 中央組態來自動啟用新的安全控制。您可以建立組態政策，其中包含跨標準停用的控制項清單。預設會啟用所有其他控制項，包括新發行的控制項。或者，您可以建立政策，其中包含跨標準啟用的控制項清單。預設會停用所有其他控制項，包括新發行的控制項。如需詳細資訊，請參閱[了解 Security Hub CSPM 中的中央組態](#)。

當 Security Hub CSPM 新增至您尚未啟用的標準時，不會啟用新的控制項。

下列指示僅適用於您不使用中央組態的情況。

選擇您偏好的存取方法，並依照步驟在已啟用的標準中自動啟用新的控制項。

Note

當您使用以下指示自動啟用新控制項時，您可以在主控台中以程式設計方式在發行後立即與控制項互動。不過，自動啟用的控制項具有停用的暫時預設狀態。Security Hub CSPM 最多可能需要幾天的時間來處理控制項版本，並在您的帳戶中將控制項指定為已啟用。在處理期間，您可以手動啟用或停用控制項，無論是否已開啟自動控制啟用，Security Hub CSPM 都會維持該指定。

Security Hub CSPM console

自動啟用新的控制項

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇設定，然後選擇一般索引標籤。
3. 在控制項下，選擇編輯。
4. 在啟用的標準中開啟自動啟用新控制項。
5. 選擇儲存。

Security Hub CSPM API

自動啟用新的控制項

1. 執行 [UpdateSecurityHubConfiguration](#)。
2. 若要自動啟用啟用標準的新控制項，請將 `AutoEnableControls` 設定為 `true`。如果您不想自動啟用新的控制項，請將 `AutoEnableControls` 設定為 `false`。

AWS CLI

自動啟用新的控制項

1. 執行 [update-security-hub-configuration](#) 命令。

- 若要自動為已啟用的標準啟用新控制項，請指定 `--auto-enable-controls`。如果您不想自動啟用新的控制項，請指定 `--no-auto-enable-controls`。

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

範例命令

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

如果您不自動啟用新的控制項，則必須手動啟用它們。如需說明，請參閱[在 Security Hub CSPM 中啟用控制項](#)。

在 Security Hub CSPM 中停用控制項

為了減少調查結果雜訊，停用與您的環境無關的控制項會很有幫助。在 AWS Security Hub CSPM 中，您可以停用所有安全標準或僅針對特定標準的控制項。

如果您停用所有標準的控制項，會發生下列情況：

- 不再執行控制項的安全檢查。
- 不會為控制項產生其他問題清單。
- 控制項的現有問題清單不會再更新。
- 控制項的現有問題清單會自動封存，通常會在 3-5 天內盡力封存。
- Security Hub CSPM 會移除它為控制項建立的任何相關 AWS Config 規則。

如果您僅針對特定標準停用控制項，Security Hub CSPM 會停止僅針對這些標準執行控制項的安全檢查。這也會從計算每個標準的[安全分數](#)中移除控制。如果在其他標準中啟用控制項，如果適用，Security Hub CSPM 會保留相關聯的 AWS Config 規則，並繼續執行其他標準的控制項安全檢查。Security Hub CSPM 也會在計算其他每個標準的安全分數時包含控制項，這會影響您的摘要安全分數。

如果您停用標準，則適用於標準的所有控制項都會針對該標準自動停用。不過，在其他標準中可能會繼續啟用控制項。當您停用標準時，Security Hub CSPM 不會追蹤針對標準停用哪些控制項。因此，如果您稍後重新啟用相同的標準，則會自動啟用所有適用於它的控制項。如需停用標準的資訊，請參閱[停用標準](#)。

停用控制項不是永久動作。假設您停用控制項，然後啟用包含控制項的標準。接著會針對該標準啟用控制項。當您在 Security Hub CSPM 中啟用標準時，會自動啟用適用於標準的所有控制項。如需啟用標準的資訊，請參閱 [啟用標準](#)。

主題

- [停用跨標準的控制項](#)
- [在特定標準中停用控制項](#)
- [在 Security Hub CSPM 中停用的建議控制項](#)

停用跨標準的控制項

我們建議跨標準停用 AWS Security Hub CSPM 控制，以在整個組織中保持一致。如果您僅在特定標準中停用控制項，如果在其他標準中啟用控制項，您仍會繼續收到控制項的問題清單。

多個帳戶和區域中的跨標準停用

若要停用多個 AWS 帳戶 和 之間的安全控制 AWS 區域，您必須使用 [中央組態](#)。

當您使用中央組態時，委派管理員可以建立 Security Hub CSPM 組態政策，以停用跨啟用標準指定的控制項。然後，您可以將組態政策與特定帳戶、OUs 或根帳戶建立關聯。組態政策會在您的主要區域（也稱為彙總區域）和所有連結區域生效。

組態政策提供自訂功能。例如，您可以選擇停用一個 OU 中的所有 AWS CloudTrail 控制項，也可以選擇停用另一個 OU 中的所有 IAM 控制項。精細程度取決於組織中安全涵蓋範圍的預期目標。如需建立停用跨標準指定控制項之組態政策的說明，請參閱 [建立和關聯組態政策](#)。

Note

委派管理員可以建立組態政策，以管理 [服務受管標準以外的所有標準中的控制項：AWS Control Tower](#) 此標準的控制項應在 AWS Control Tower 服務中設定。

如果您希望某些帳戶設定自己的控制項，而不是委派管理員，委派管理員可以將這些帳戶指定為自我管理。自我管理帳戶必須在每個區域中分別設定控制項。

單一帳戶和區域中的跨標準停用

如果您不使用中央組態或 是自我管理帳戶，則無法使用組態政策來集中停用多個帳戶和區域中的控制項。不過，您可以在單一帳戶和區域中停用控制項。

Security Hub CSPM console

停用一個帳戶和區域中跨標準的控制項

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 從導覽窗格中選擇控制項。
3. 選擇控制項旁的選項。
4. 選擇停用控制。此選項不會針對已停用的控制項顯示。
5. 選取停用控制項的原因，然後選擇停用以確認。
6. 在您要停用控制項的每個區域中重複此動作。

Security Hub CSPM API

停用一個帳戶和區域中跨標準的控制項

1. 叫用 [ListStandardsControlAssociations](#) API。提供安全控制 ID。

請求範例：

```
{
  "SecurityControlId": "IAM.1"
}
```

2. 叫用 [BatchUpdateStandardsControlAssociations](#) API。提供啟用控制項的任何標準的 ARN。若要取得標準 ARNs，請執行 [DescribeStandards](#)。
3. 將 AssociationStatus 參數設定為等於 DISABLED。如果您針對已停用的控制項遵循這些步驟，API 會傳回 HTTP 狀態碼 200 回應。

請求範例：

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-
benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
"arn:aws:securityhub::standards/aws-foundational-security-best-practices/
v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
environment"}]}
```

```
}
```

4. 在您要停用控制項的每個區域中重複此動作。

AWS CLI

停用一個帳戶和區域中跨標準的控制項

1. 執行 [list-standards-control-associations](#) 命令。提供安全控制 ID。

```
aws securityhub --region us-east-1 list-standards-control-associations --  
security-control-id CloudTrail.1
```

2. 執行 [batch-update-standards-control-associations](#) 命令。提供啟用控制項的任何標準的 ARN。若要取得標準 ARNs，請執行 `describe-standards` 命令。
3. 將 `AssociationStatus` 參數設定為等於 `DISABLED`。如果您針對已停用的控制項遵循這些步驟，命令會傳回 HTTP 狀態碼 200 回應。

```
aws securityhub --region us-east-1 batch-update-standards-control-associations  
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",  
"StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/  
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable  
to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":  
"arn:aws:securityhub::standards/cis-aws-foundations-benchmark/v/1.4.0",  
"AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to  
environment"}]'
```

4. 在您要停用控制項的每個區域中重複此動作。

在特定標準中停用控制項

您只能在特定安全標準中停用控制項，而不是在所有標準中停用。如果控制項適用於其他已啟用的標準，AWS Security Hub CSPM 會繼續執行控制項的安全檢查，而且您會持續收到控制項的問題清單。

建議您在套用控制項的所有已啟用標準中，調整控制項的啟用狀態。如需停用適用於其所有標準之控制項的詳細資訊，請參閱 [停用跨標準的控制項](#)。

在標準詳細資訊頁面上，您也可以特定標準中停用控制項。您必須在每個 AWS 帳戶 和 中分別停用特定標準中的控制項 AWS 區域。當您在特定標準中停用控制項時，它只會影響目前的帳戶和區域。

選擇您偏好的方法，並依照下列步驟停用一或多個特定標準的控制項。

Security Hub CSPM console

停用特定標準中的控制項

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 從導覽窗格中選擇安全標準。選擇 檢視相關標準的結果。
3. 選取控制項。
4. 選擇停用控制。此選項不會針對已停用的控制項顯示。
5. 提供停用控制項的原因，然後選擇停用進行確認。

Security Hub CSPM API

停用特定標準中的控制項

1. 執行 [ListSecurityControlDefinitions](#)，並提供標準 ARN，以取得特定標準的可用控制項清單。若要取得標準 ARN，請執行 [DescribeStandards](#)。此 API 會傳回標準無關的安全控制 IDs，而非標準特定的控制 IDs。

請求範例：

```
{
  "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. 執行 [ListStandardsControlAssociations](#)，並提供特定的控制項 ID，以傳回每個標準中控制項的目前啟用狀態。

請求範例：

```
{
  "SecurityControlId": "IAM.1"
}
```

3. 執行 [BatchUpdateStandardsControlAssociations](#)。提供您要停用控制項之標準 ARN。

4. 將 `AssociationStatus` 參數設定為等於 `DISABLED`。如果您針對已停用的控制項遵循這些步驟，API 會傳回 HTTP 狀態碼 200 回應。

請求範例：

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to environment"}]
}
```

AWS CLI

停用特定標準中的控制項

1. 執行 [list-security-control-definitions](#) 命令，並提供標準 ARN，以取得特定標準的可用控制項清單。若要取得標準 ARN，請執行 `describe-standards`。此命令會傳回標準無關的安全控制 IDs，而不是標準特定的控制 IDs。

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. 執行 [list-standards-control-associations](#) 命令，並提供特定的控制項 ID，以傳回每個標準中控制項的目前啟用狀態。

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. 執行 [batch-update-standards-control-associations](#) 命令。提供您要停用控制項之標準 ARN。
4. 將 `AssociationStatus` 參數設定為等於 `DISABLED`。如果您針對已啟用的控制項遵循這些步驟，命令會傳回 HTTP 狀態碼 200 回應。

```
aws securityhub --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
  "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
  "UpdatedReason": "Not applicable to environment"}]'
```

在 Security Hub CSPM 中停用的建議控制項

我們建議您停用一些 AWS Security Hub CSPM 控制項，以減少調查結果的雜訊和使用成本。

使用全域資源的控制項

有些 AWS 服務支援全域資源，這表示您可以從任何存取資源 AWS 區域。若要節省的成本 AWS Config，您可以停用除一個區域以外的所有全域資源的記錄。不過，在您執行此操作之後，Security Hub CSPM 仍會在啟用控制項的所有區域中執行安全檢查，並根據每個區域的每個帳戶的檢查數量向您收費。因此，為了減少調查結果噪音並節省 Security Hub CSPM 的成本，您還應該停用在所有區域中涉及全域資源的控制項，除了記錄全域資源的區域以外。

如果控制項涉及全域資源，但僅在一個區域中可用，在該區域中停用它可防止您取得基礎資源的任何問題清單。在此情況下，建議您保持啟用控制項。使用跨區域彙總時，可使用控制項的區域應為彙總區域或其中一個連結區域。下列控制項涉及全域資源，但僅適用於單一區域：

- 所有 CloudFront 控制項 – 僅適用於美國東部（維吉尼亞北部）區域
- GlobalAccelerator.1 – 僅適用於美國西部（奧勒岡）區域
- Route53.2 – 僅適用於美國東部（維吉尼亞北部）區域
- WAF.1、WAF.6、WAF.7、WAF.8 – 僅適用於美國東部（維吉尼亞北部）區域

Note

如果您使用中央組態，Security Hub CSPM 會自動停用涉及主要區域以外所有區域中全域資源的控制項。您選擇在可用的所有區域中啟用組態政策時啟用的其他控制項。若要將這些控制項的問題清單限制為僅一個區域，您可以更新 AWS Config 記錄器設定，並關閉主要區域以外的所有區域中的全域資源記錄。

如果主區域不支援涉及全域資源的已啟用控制項，Security Hub CSPM 會嘗試在支援控制項的一個連結區域中啟用控制項。使用中央組態時，您無法涵蓋主要區域或任何連結區域中無法使用的控制項。

如需中央組態的詳細資訊，請參閱 [了解 Security Hub CSPM 中的中央組態](#)。

對於具有定期排程類型的控制項，需要在 Security Hub CSPM 中停用它們以防止計費。將 AWS Config 參數設定為 `includeGlobalResourceTypes false` 不會影響定期 Security Hub CSPM 控制項。

下列 Security Hub CSPM 控制項使用全域資源：

- [【Account.1】應針對提供安全性聯絡資訊 AWS 帳戶](#)
- [【Account.2】AWS 帳戶應該是 AWS Organizations 組織的一部分](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【IAM.1】IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.6】應為根使用者啟用硬體 MFA](#)
- [【IAM.7】IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.8】應移除未使用的 IAM 使用者登入資料](#)

- [【IAM.9】 應為根使用者啟用 MFA](#)
- [【IAM.10】 IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.11】 確保 IAM 密碼政策至少需要一個大寫字母](#)
- [【IAM.12】 確保 IAM 密碼政策至少需要一個小寫字母](#)
- [【IAM.13】 確保 IAM 密碼政策至少需要一個符號](#)
- [【IAM.14】 確保 IAM 密碼政策至少需要一個數字](#)
- [【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)
- [【IAM.16】 確保 IAM 密碼政策防止密碼重複使用](#)
- [【IAM.17】 確保 IAM 密碼政策在 90 天內過期密碼](#)
- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】 IAM 身分不應連接 AWSCloudShellFullAccess 政策](#)
- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

CloudTrail 記錄控制

[CloudTrail.2](#) 控制項會評估使用 AWS Key Management Service (AWS KMS) 來加密 AWS CloudTrail 追蹤日誌。如果您在集中式記錄帳戶中記錄這些線索，則只需要在帳戶中以及集中式記錄的發生 AWS 區域 位置啟用此控制項。

如果您使用[中央組態](#)，則控制項的啟用狀態會跨主要區域和連結區域對齊。您無法在某些區域中停用控制項，並在其他區域中啟用控制項。在此情況下，您可以抑制 CloudTrail.2 控制項的調查結果，以減少調查結果雜訊。

CloudWatch 警示控制

如果您偏好使用 Amazon GuardDuty 進行異常偵測，而不是使用 Amazon CloudWatch 警示，您可以停用下列控制項，專注於 CloudWatch 警示：

- [【CloudWatch.1】應該存在日誌指標篩選條件和警示以使用「根」使用者](#)
- [【CloudWatch.2】確保未經授權的 API 呼叫存在日誌指標篩選條件和警示](#)
- [【CloudWatch.3】確保沒有 MFA 的管理主控台登入存在日誌指標篩選條件和警示](#)
- [【CloudWatch.4】確保 IAM 政策變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.5】確保 CloudTrail 組態變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.6】確保 AWS 管理主控台 驗證失敗時存在日誌指標篩選條件和警示](#)
- [【CloudWatch.7】確保日誌指標篩選條件和警示存在，以停用或排程刪除客戶受管金鑰](#)
- [【CloudWatch.8】確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.9】確保 AWS Config 組態變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.10】確保安全群組變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.11】確定網路存取控制清單 \(NACL\) 的變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.12】確保網路閘道變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.13】確保路由表變更存在日誌指標篩選條件和警示](#)
- [【CloudWatch.14】確保 VPC 變更存在日誌指標篩選條件和警示](#)

了解 Security Hub CSPM 中的安全檢查和分數

對於您啟用的每個控制項，AWS Security Hub CSPM 會執行安全檢查。安全檢查會產生調查結果，告訴您特定 AWS 資源是否符合控制項包含的規則。

有些檢查會定期執行。其他檢查只會在資源狀態變更時執行。如需詳細資訊，請參閱[執行安全檢查的排程](#)。

許多安全檢查會使用 AWS Config 受管或自訂規則來建立合規要求。若要執行這些檢查，您必須設定 AWS Config 並開啟所需資源的資源記錄。如需設定的詳細資訊 AWS Config，請參閱[啟用和設定](#)

[AWS Config Security Hub CSPM](#)。如需您必須為每個標準記錄 AWS Config 的資源清單，請參閱 [控制問題清單所需的 AWS Config 資源](#)。其他控制項使用自訂 Lambda 函數，這些函數由 Security Hub CSPM 管理，不需要任何先決條件。

當 Security Hub CSPM 執行安全檢查時，會產生調查結果並為其指派合規狀態。如需合規狀態的詳細資訊，請參閱 [評估 Security Hub CSPM 調查結果的合規狀態](#)。

Security Hub CSPM 使用控制調查結果的合規狀態來判斷整體控制狀態。根據控制狀態，Security Hub CSPM 也會計算所有啟用控制項和特定標準的安全分數。如需詳細資訊，請參閱 [the section called “合規狀態和控制狀態”](#) 及 [the section called “計算安全分數”](#)。

如果您已開啟合併控制調查結果，即使控制項與多個標準相關聯，Security Hub CSPM 也會產生單一調查結果。如需詳細資訊，請參閱 [合併的控制問題清單](#)。

主題

- [控制問題清單所需的 AWS Config 資源](#)
- [執行安全檢查的排程](#)
- [產生和更新控制問題清單](#)
- [評估合規狀態和控制狀態](#)
- [計算安全分數](#)

控制問題清單所需的 AWS Config 資源

在 AWS Security Hub CSPM 中，某些控制項使用服務連結 AWS Config 規則來偵測 AWS 資源中的組態變更。若要讓 Security Hub CSPM 產生這些控制項的準確調查結果，您必須在其中啟用 AWS Config 和開啟資源錄製 AWS Config。如需 Security Hub CSPM 如何使用 AWS Config 規則以及如何啟用和設定的詳細資訊 AWS Config，請參閱 [啟用和設定 AWS Config Security Hub CSPM](#)。如需資源錄製的詳細資訊，請參閱《AWS Config 開發人員指南》中的 [使用組態記錄器](#)。

若要接收準確的控制調查結果，您必須為具有變更觸發排程類型的已啟用控制項開啟 AWS Config 資源記錄。有些具有定期排程類型的控制項也需要資源記錄。此頁面列出這些 Security Hub CSPM 控制項所需的資源。

Security Hub CSPM 控制項可以依賴受管 AWS Config 規則或自訂 Security Hub CSPM 規則。請確定沒有任何 AWS Identity and Access Management (IAM) 政策或 AWS Organizations 受管政策 AWS Config 會阻止 擁有記錄 資源的許可。Security Hub CSPM 控制項會直接評估資源組態，且不考慮 AWS Organizations 政策。

Note

在無法使用控制項 AWS 區域 的情況下，對應的資源無法使用 AWS Config。如需這些限制的清單，請參閱 [Security Hub CSPM 控制項的區域限制](#)。

主題

- [所有 Security Hub CSPM 控制項的必要資源](#)
- [AWS 基礎安全最佳實務標準的必要資源](#)
- [CIS AWS Foundations Benchmark 的必要資源](#)
- [NIST SP 800-53 修訂版 5 標準的必要資源](#)
- [NIST SP 800-171 修訂版 2 標準所需的資源](#)
- [PCI DSS v3.2.1 的必要資源](#)
- [資源標記標準所需的 AWS 資源](#)

所有 Security Hub CSPM 控制項的必要資源

若要讓 Security Hub CSPM 為已啟用並使用 AWS Config 規則的變更觸發控制項產生調查結果，您必須在其中記錄下列類型的資源 AWS Config。此資料表也會指出哪些控制項會評估特定類型的資源。單一控制項可能會評估一種以上的資源類型。

AWS 服務	資源類型	相關控制項
AWS Amplify	AWS::Amplify::App	Amplify.1
	AWS::Amplify::Branch	Amplify.2
Amazon API Gateway	AWS::ApiGateway::Stage	APIGateway.1
		APIGateway.2
		APIGateway.3
		APIGateway.4

AWS 服務	資源類型	相關控制項
		APIGateway.5
	AWS::ApiGatewayV2::Stage	APIGateway.1 APIGateway.9
	AWS::ApiGateway::DomainName	APIGateway.11
AWS AppConfig	AWS::AppConfig::Application	AppConfig.1
	AWS::AppConfig::ConfigurationProfile	AppConfig.2
	AWS::AppConfig::Environment	AppConfig.3
	AWS::AppConfig::ExtensionAssociation	AppConfig.4
Amazon AppFlow	AWS::AppFlow::Flow	AppFlow.1
AWS App Runner	AWS::AppRunner::Service	AppRunner.1
	AWS::AppRunner::VpcConnector	AppRunner.2

AWS 服務	資源類型	相關控制項
AWS AppSync	AWS::AppSync::GraphQLApi	AppSync.2 AppSync.4 AppSync.5
	AWS::AppSync::ApiCache	AppSync.1 AppSync.6
AWS Backup	AWS::Backup::BackupPlan	備份。5
	AWS::Backup::BackupVault	備份。3
	AWS::Backup::RecoveryPoint	備份。1 備份。2
	AWS::Backup::ReportPlan	備份。4
AWS Batch	AWS::Batch::ComputeEnvironment	Batch.3 Batch.4
	AWS::Batch::JobQueue	Batch.1
	AWS::Batch::SchedulingPolicy	Batch.2

AWS 服務	資源類型	相關控制項
Amazon Bedrock AgentCore	AWS::BedrockAgentCore::BrowserCustom	BedrockAgentCore.5 BedrockAgentCore.6
	AWS::BedrockAgentCore::Gateway	BedrockAgentCore.2 BedrockAgentCore.4
	AWS::BedrockAgentCore::Memory	BedrockAgentCore.3
	AWS::BedrockAgentCore::Runtime	BedrockAgentCore.1
AWS Certificate Manager (ACM)	AWS::ACM::Certificate	ACM.1 ACM.2 ACM.3
Amazon Athena	AWS::Athena::DataCatalog	Athena.2
	AWS::Athena::WorkGroup	Athena.3 Athena.4
AWS CloudFormation	AWS::CloudFormation::Stack	CloudFormation.2 CloudFormation.3 CloudFormation.4

AWS 服務	資源類型	相關控制項
Amazon CloudFront	AWS::CloudFront::Distribution	CloudFront.1
		CloudFront.3
		CloudFront.4
		CloudFront.5
		CloudFront.6
		CloudFront.7
		CloudFront.8
		CloudFront.9
		CloudFront.10
		CloudFront.13
		CloudFront.14
		CloudFront.15
		CloudFront.16
		CloudFront.17
AWS CloudTrail	AWS::CloudTrail::Trail	CloudTrail.9
	AWS::CloudTrail::EventDataStore	CloudTrail.11
Amazon CloudWatch	AWS::CloudWatch::Alarm	CloudWatch.15
		CloudWatch.17

AWS 服務	資源類型	相關控制項
AWS CodeArtifact	AWS::CodeArtifact::Repository	CodeArtifact.1
AWS CodeBuild	AWS::CodeBuild::Project	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4
	AWS::CodeBuild::ReportGroup	CodeBuild.7
Amazon CodeGuru Profiler	AWS::CodeGuruProfiler::ProfilingGroup	CodeGuruProfiler.1
Amazon CodeGuru Reviewer	AWS::CodeGuruReviewer::RepositoryAssociation	CodeGuruReviewer.1
Amazon Cognito	AWS::Cognito::IdentityPool	Cognito.2

AWS 服務	資源類型	相關控制項
	AWS::Cognito::UserPool	Cognito.1 Cognito.3 Cognito.4 Cognito.5 Cognito.6
	AWS::Connect::CustomerProfiles::ObjectType	Connect.1
	AWS::Connect::Instance	Connect.2
	AWS::DataSync::Task	DataSync.1 DataSync.2
	AWS::Detective::Graph	Detective.1
AWS Database Migration Service (AWS DMS)	AWS::DMS::Certificate	DMS.2
	AWS::DMS::Endpoint	DMS.9 DMS.10 DMS.11 DMS.12
	AWS::DMS::EventSubscription	DMS.3

AWS 服務	資源類型	相關控制項
	AWS::DMS: :ReplicationInstance	DMS.4 DMS.6 DMS.13
	AWS::DMS: :ReplicationSubnetGroup	DMS.5
	AWS::DMS: :ReplicationTask	DMS.7 DMS.8
Amazon DynamoDB	AWS::DynamoDB::Table	DynamoDB.1 DynamoDB.2 DynamoDB.5 DynamoDB.6
Amazon Elastic Compute Cloud (EC2)	AWS::EC2: :ClientVpnEndpoint	EC2.51
	AWS::EC2: :CustomerGateway	EC2.36
	AWS::EC2: :DHCPOptions	EC2.174
	AWS::EC2::EIP	EC2.12 EC2.37

AWS 服務	資源類型	相關控制項
	AWS::EC2: :FlowLog	EC2.48
	AWS::EC2: :Instance	EC2.4
		EC2.8
		EC2.9
		EC2.17
		EC2.24
		EC2.38
		EMR.1
		SSM.1
	AWS::EC2: :Internet Gateway	EC2.39
	AWS::EC2: :LaunchTe mplate	EC2.25
		EC2.170
		EC2.175
		EC2.181
	AWS::EC2: :NatGateway	EC2.40
	AWS::EC2: :NetworkAc1	EC2.16
		EC2.21
		EC2.41

AWS 服務	資源類型	相關控制項
	AWS::EC2: :NetworkInterface	EC2.22 EC2.35 EC2.180
	AWS::EC2: :PrefixList	EC2.176
	AWS::EC2: :RouteTable	EC2.42
	AWS::EC2: :SecurityGroup	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	AWS::EC2: :Snapshot BlockPublicAccess	EC2.182
	AWS::EC2: :SpotFleet	EC2.173
	AWS::EC2: :Subnet	EC2.15 EC2.44 ElastiCache.7

AWS 服務	資源類型	相關控制項
	AWS::EC2: :TrafficMirrorFilter	EC2.178
	AWS::EC2: :TrafficMirrorSession	EC2.177
	AWS::EC2: :TrafficMirrorTarget	EC2.179
	AWS::EC2: :TransitGateway	EC2.23 EC2.52
	AWS::EC2: :TransitGatewayAttachment	EC2.33
	AWS::EC2: :TransitGatewayRouteTable	EC2.34
	AWS::EC2: :Volume	EC2.3 EC2.45
	AWS::EC2::VPC	EC2.6 EC2.46

AWS 服務	資源類型	相關控制項
	AWS::EC2: :VPCBlock PublicAcc essOptions	EC2.172
	AWS::EC2: :VPCEndpo intService	EC2.47
	AWS::EC2: :VPCPeeri ngConnection	EC2.49
	AWS::EC2: :VPNConnection	EC2.20 EC2.171 EC2.183
AWS::EC2: :VPNGateway		EC2.50
Amazon EC2 Auto Scaling	AWS::Auto Scaling:: AutoScali ngGroup	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling.9 AutoScaling.10
	AWS::Auto Scaling:: LaunchCon figuration	AutoScaling.3 Autoscaling.5

AWS 服務	資源類型	相關控制項
Amazon EC2 Systems Manager (SSM)	AWS::SSM: :Associat ionCompliance	SSM.3
	AWS::SSM: :ManagedI nstanceIn ventory	SSM.1
	AWS::SSM: :PatchCom pliance	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR: :PublicRe pository	ECR.4
	AWS::ECR: :Repository	ECR.2
		ECR.3 ECR.5
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS: :Cluster	ECS.12
		ECS.14
	AWS::ECS: :Capacity Provider	ECS.19
	AWS::ECS: :Service	ECS.2
		ECS.10
		ECS.13

AWS 服務	資源類型	相關控制項
	AWS::ECS: :TaskDefinition	ECS.1 ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 ECS.15 ECS.17 ECS.18 ECS.20 ECS.21
AWS::ECS: :TaskSet	ECS.16	
Amazon Elastic File System (Amazon EFS)	AWS::EFS: :AccessPoint	EFS.3 EFS.4 EFS.5
	AWS::EFS: :FileSystem	EFS.7 EFS.8
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS: :Cluster	EKS.2 EKS.6 EKS.8

AWS 服務	資源類型	相關控制項
	AWS::EKS: :Identity ProviderConfig	EKS.7
	AWS::EKS: :Nodegroup	EKS.9
AWS Elastic Beanstalk	AWS::Elas ticBeanst alk::Envi ronment	ElasticBeanstalk.1
		ElasticBeanstalk.2
		ElasticBeanstalk.3
Elastic Load Balancing	AWS::Elas ticLoadBa lancing:: LoadBalancer	ELB.2
		ELB.3
		ELB.5
		ELB.7
		ELB.8
		ELB.9
		ELB.10
		ELB.14
	AWS::Elas ticLoadBa lancingV2 ::Listener	ELB.17
ELB.18		

AWS 服務	資源類型	相關控制項
	AWS::ElasticLoadBalancingV2::LoadBalancer	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16
ElasticSearch	AWS::Elasticsearch::Domain	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EMR	AWS::EMR::SecurityConfiguration	EMR.3 EMR.4
Amazon EventBridge	AWS::Events::EventBus	EventBridge.2 EventBridge.3
	AWS::Events::Endpoint	EventBridge.4

AWS 服務	資源類型	相關控制項
Amazon Fraud Detector	AWS::FraudDetector::EntityType	FraudDetector.1
	AWS::FraudDetector::Label	FraudDetector.2
	AWS::FraudDetector::Outcome	FraudDetector.3
	AWS::FraudDetector::Variable	FraudDetector.4
AWS Global Accelerator	AWS::GlobalAccelerator::Accelerator	GlobalAccelerator.1
AWS Glue	AWS::Glue::Job	Glue.1 Glue.4
	AWS::Glue::MLTransform	Glue.3
Amazon GuardDuty	AWS::GuardDuty::Detector	GuardDuty.4
	AWS::GuardDuty::Filter	GuardDuty.2
	AWS::GuardDuty::IPSet	GuardDuty.3

AWS 服務	資源類型	相關控制項
AWS Identity and Access Management (IAM)	AWS::IAM::Group	IAM.27 KMS.2
	AWS::IAM::Policy	IAM.1 IAM.21 KMS.1
	AWS::IAM::Role	IAM.24 IAM.27 KMS.2
	AWS::IAM::User	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 IAM.25 IAM.27 KMS.2
AWS Identity and Access Management Access Analyzer	AWS::AccessAnalyzer::Analyzer	IAM.23

AWS 服務	資源類型	相關控制項
Amazon Interactive Video Service (Amazon IVS)	AWS::IVS:PlaybackKeyPair	IVS.1
	AWS::IVS:RecordingConfiguration	IVS.2
	AWS::IVS:Channel	IVS.3
AWS IoT	AWS::IoT:Authorizer	IoT.4
	AWS::IoT:Dimension	IoT.3
	AWS::IoT:MitigationAction	IoT.2
	AWS::IoT:Policy	IoT.6
	AWS::IoT:RoleAlias	IoT.5
	AWS::IoT:SecurityProfile	IoT.1
AWS IoT 事件	AWS::IoTEvents::AlarmModel	IoTEvents.3

AWS 服務	資源類型	相關控制項
	AWS::IoTEvents::DetectorModel	IoTEvents.2
	AWS::IoTEvents::Input	IoTEvents.1
AWS IoT SiteWise	AWS::IoTSiteWise::AssetModel	IoTSiteWise.1
	AWS::IoTSiteWise::Dashboard	IoTSiteWise.2
	AWS::IoTSiteWise::Gateway	IoTSiteWise.3
	AWS::IoTSiteWise::Portal	IoTSiteWise.4
	AWS::IoTSiteWise::Project	IoTSiteWise.5
AWS IoT TwinMaker	AWS::IoTTwinMaker::Entity	IoTTwinMaker.4
	AWS::IoTTwinMaker::Scene	IoTTwinMaker.3

AWS 服務	資源類型	相關控制項
	AWS::IoTwinMaker:SyncJob	IoTwinMaker.1
	AWS::IoTwinMaker:Workspace	IoTwinMaker.2
AWS IoT Wireless	AWS::IoTWireless::MulticastGroup	IoTWireless.1
	AWS::IoTWireless::ServiceProfile	IoTWireless.2
	AWS::IoTWireless::FirmwareTask	IoTWireless.3
Amazon Keyspaces (適用於 Apache Cassandra)	AWS::Cassandra::Keyspace	鍵空間。1
Amazon Kinesis	AWS::Kinesis::Stream	Kinesis.1
		Kinesis.2
		Kinesis.3
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias	S3.17
	AWS::KMS::Key	KMS.3
		KMS.5
		S3.17

AWS 服務	資源類型	相關控制項
AWS Lambda	AWS::Lambda::Function	Lambda.1
		Lambda.2
		Lambda.3
		Lambda.5
		Lambda.6
		Lambda.7
Amazon MSK	AWS::MSK::Cluster	MSK.1
		MSK.2
		MSK.4
		MSK.6
	AWS::KafkaConnect::Connector	MSK.3
		MSK.5
Amazon MQ	AWS::AmazonMQ::Broker	MQ.2
		MQ.3
		MQ.4
		MQ.5
		MQ.6

AWS 服務	資源類型	相關控制項
AWS Network Firewall	AWS::NetworkFirewall::Firewall	NetworkFirewall.1
		NetworkFirewall.7
		NetworkFirewall.9
		NetworkFirewall.10
	AWS::NetworkFirewall::FirewallPolicy	NetworkFirewall.3
		NetworkFirewall.4
		NetworkFirewall.5
	AWS::NetworkFirewall::RuleGroup	NetworkFirewall.8
		NetworkFirewall.6

AWS 服務	資源類型	相關控制項
Amazon OpenSearch Service	AWS::OpenSearch::Domain	Opensearch.1
		Opensearch.2
		Opensearch.3
		Opensearch.4
		Opensearch.5
		Opensearch.6
		Opensearch.7
		Opensearch.8
		Opensearch.9
		Opensearch.10
		Opensearch.11
AWS 私有 CA	AWS::ACMPCA::CertificateAuthority	PCA.2

AWS 服務	資源類型	相關控制項
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster	DocumentDB.1
		DocumentDB.2
		DocumentDB.4
		DocumentDB.5
		Neptune.1
		Neptune.2
		Neptune.4
		Neptune.5
		Neptune.7
		Neptune.8
		Neptune.9
		RDS.7
		RDS.12
		RDS.14
		RDS.15
		RDS.16
		RDS.24
		RDS.27
		RDS.28
		RDS.34
		RDS.35

AWS 服務	資源類型	相關控制項
		RDS.37
		RDS.47
		RDS.48
	AWS::RDS: :DBClusterSnapshot	DocumentDB.3
		Neptune.3
		Neptune.6
		RDS.1
		RDS.4
		RDS.29

AWS 服務	資源類型	相關控制項
	AWS::RDS: DBInstance	RDS.2
		RDS.3
		RDS.5
		RDS.6
		RDS.8
		RDS.9
		RDS.10
		RDS.11
		RDS.13
		RDS.17
		RDS.18
		RDS.23
		RDS.25
		RDS.30
		RDS.36
		RDS.40
	AWS::RDS: DBSecurityGroup	RDS.31

AWS 服務	資源類型	相關控制項
	AWS::RDS: :DBSnapshot	RDS.1
		RDS.4
		RDS.32
	AWS::RDS: :DBSubnetGroup	RDS.33
	AWS::RDS: :EventSubscription	RDS.19
		RDS.20
		RDS.21
		RDS.22
	AWS::RDS: :GlobalCluster	RDS.51
	Amazon Redshift AWS::Redshift::Cluster	Redshift.1
		Redshift.2
		Redshift.3
		Redshift.4
		Redshift.6
		Redshift.7
		Redshift.8
		Redshift.10
		Redshift.11
		Redshift.18

AWS 服務	資源類型	相關控制項
	AWS::Redshift::ClusterParameterGroup	Redshift.2 Redshift.17
	AWS::Redshift::ClusterSnapshot	Redshift.13
	AWS::Redshift::ClusterSubnetGroup	Redshift.14 Redshift.16
	AWS::Redshift::EventSubscription	Redshift.12
Amazon Route 53	AWS::Route53::HostedZone	Route53.2
	AWS::Route53::HealthCheck	Route53.1
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint	S3.19
	AWS::S3::AccountPublicAccessBlock	S3.2 S3.3

AWS 服務	資源類型	相關控制項
	AWS::S3::Bucket	CloudTrail.6
		CloudTrail.7
		S3.2
		S3.3
		S3.5
		S3.6
		S3.7
		S3.8
		S3.9
		S3.10
		S3.11
		S3.12
		S3.13
		S3.14
		S3.15
		S3.17
		S3.20
	AWS::S3::MultiRegionAccessPoint	S3.24

AWS 服務	資源類型	相關控制項
	AWS::S3Express::DirectoryBucket	S3.25
Amazon SageMaker AI	AWS::SageMaker::AppImageConfig	SageMaker.6
	AWS::SageMaker::Image	SageMaker.7
	AWS::SageMaker::Model	SageMaker.5
		SageMaker.16
		SageMaker.19
	AWS::SageMaker::NotebookInstance	SageMaker.2 SageMaker.3
	AWS::SageMaker::FeatureGroup	SageMaker.17 SageMaker.18
AWS Secrets Manager	AWS::SecretsManager::Secret	SecretsManager.1
		SecretsManager.2
		SecretsManager.5
AWS Service Catalog	AWS::ServiceCatalog::Portfolio	ServiceCatalog.1
Amazon Simple Email Service (Amazon SES)	AWS::SES::ConfigurationSet	SES.2
		SES.3

AWS 服務	資源類型	相關控制項
	AWS::SES: :ContactList	SES.1
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic	SNS.1 SNS.3 SNS.4
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue	SQS.1 SQS.2 SQS.3
AWS Step Functions	AWS::Step Functions ::StateMachine	StepFunctions.1
	AWS::Step Functions ::Activity	StepFunctions.2
AWS Systems Manager (SSM)	AWS::SSM: :Document	SSM.5
AWS Transfer Family	AWS::Transfer::Agreement	Transfer.4
	AWS::Transfer::Certificate	Transfer.5
	AWS::Transfer::Connector	Transfer.3 Transfer.6

AWS 服務	資源類型	相關控制項
	AWS::Transfer::Profile	Transfer.7
	AWS::Transfer::Workflow	Transfer.1
AWS WAF	AWS::WAF::Rule	WAF.6
	AWS::WAF::RuleGroup	WAF.7
	AWS::WAF::WebACL	WAF.1 WAF.8
	AWS::WAFRegional::Rule	WAF.2
	AWS::WAFRegional::RuleGroup	WAF.3
	AWS::WAFRegional::WebACL	WAF.4
	AWS::WAFv2::RuleGroup	WAF.12
	AWS::WAFv2::WebACL	WAF.10 WAF.11
Amazon WorkSpaces	AWS::WorkSpaces::Workspace	WorkSpaces.1 WorkSpaces.2

AWS 基礎安全最佳實務標準的必要資源

若要讓 Security Hub CSPM 準確報告適用於 AWS 基礎安全最佳實務標準 (v.1.0.0) 的變更觸發控制項的問題清單，並啟用並使用 AWS Config 規則，您必須在其中記錄下列類型的資源 AWS Config。如需此標準的資訊，請參閱 [AWS Security Hub CSPM 中的基礎安全最佳實務標準](#)。

AWS 服務	資源類型
Amazon API Gateway	AWS::ApiGateway::DomainName , AWS::ApiGateway::Stage , AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::ApiCache , AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint
Amazon Bedrock AgentCore	AWS::BedrockAgentCore::BrowserCustom , AWS::BedrockAgentCore::Gateway , AWS::BedrockAgentCore::Runtime
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
AWS CodeBuild	AWS::CodeBuild::Project , AWS::CodeBuild::ReportGroup
Amazon Cognito	AWS::Cognito::IdentityPool , AWS::Cognito::UserPool
AWS CloudTrail	AWS::CloudTrail::EventDataStore
Amazon Connect 客戶	AWS::Connect::Instance
AWS DataSync	AWS::DataSync::Task

AWS 服務	資源類型
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint , AWS::DMS::ReplicationInstance , AWS::DMS::ReplicationTask
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance , AWS::SSM::ManagedInstanceInventory , AWS::SSM::PatchCompliance
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::Instance , AWS::EC2::LaunchTemplate , AWS::EC2::NetworkAcl , AWS::EC2::NetworkInterface , AWS::EC2::SecurityGroup , AWS::EC2::SnapshotBlockPublicAccess , AWS::EC2::SpotFleet , AWS::EC2::Subnet , AWS::EC2::TransitGateway , AWS::EC2::VPCElasticLoadBalancingOptions , AWS::EC2::VPNConnection , AWS::EC2::Volume
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup , AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::CapacityProvider , AWS::ECS::Cluster , AWS::ECS::Service , AWS::ECS::TaskDefinition , AWS::ECS::TaskSet

AWS 服務	資源類型
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint , AWS::EFS::FileSystem
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS::Cluster , AWS::EKS::Nodegroup
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer , AWS::ElasticLoadBalancingV2::Listener , AWS::ElasticLoadBalancingV2::LoadBalancer
ElasticSearch	AWS::Elasticsearch::Domain
Amazon EMR	AWS::EMR::SecurityConfiguration
AWS Glue	AWS::Glue::Job , AWS::Glue::MLTransform
AWS Identity and Access Management (IAM)	AWS::IAM::Group , AWS::IAM::Policy , AWS::IAM::Role , AWS::IAM::User
Amazon Kinesis	AWS::Kinesis::Stream
AWS Key Management Service (AWS KMS)	AWS::KMS::Key
AWS Lambda	AWS::Lambda::Function
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	AWS::MSK::Cluster , AWS::KafkaConnect::Connector
AWS Network Firewall	AWS::NetworkFirewall::Firewall , AWS::NetworkFirewall::FirewallPolicy , AWS::NetworkFirewall::RuleGroup

AWS 服務	資源類型
Amazon OpenSearch Service	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster , AWS::RDS::DBClusterSnapshot , AWS::RDS::DBInstance , AWS::RDS::DBProxy , AWS::RDS::DBSnapshot , AWS::RDS::EventSubscription , AWS::RDS::GlobalCluster
Amazon Redshift	AWS::Redshift::Cluster , AWS::Redshift::ClusterSubnetGroup
Amazon Redshift Serverless	AWS::RedshiftServerless::Workgroup
Amazon Route 53	AWS::Route53::HostedZone
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint , AWS::S3::AccountPublicAccessBlock , AWS::S3::Bucket , AWS::S3::MultiRegionAccessPoint , AWS::S3Express::DirectoryBucket
Amazon SageMaker AI	AWS::SageMaker::FeatureGroup , AWS::SageMaker::Model , AWS::SageMaker::NotebookInstance
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
AWS Secrets Manager	AWS::SecretsManager::Secret
AWS Step Functions	AWS::StepFunctions::StateMachine
AWS Transfer Family	AWS::Transfer::Connector

AWS 服務	資源類型
AWS WAF	AWS::WAF::Rule , AWS::WAF::RuleGroup , AWS::WAF::WebACL , AWS::WAFRegional::Rule , AWS::WAFRegional::RuleGroup , AWS::WAFRegional::WebACL , AWS::WAFv2::RuleGroup , AWS::WAFv2::WebACL
Amazon WorkSpaces	AWS::WorkSpaces::Workspace

CIS AWS Foundations Benchmark 的必要資源

若要針對適用於網際網路安全中心 (CIS) AWS 基準基準的已啟用控制項執行安全檢查，Security Hub CSPM 會執行針對檢查指定的確切稽核步驟，或使用特定 AWS Config 受管規則。如需 Security Hub CSPM 中此標準的資訊，請參閱 [Security Hub CSPM 中的 CIS AWS Foundations 基準](#)。

CIS v5.0.0 的必要資源

若要讓 Security Hub CSPM 準確報告使用 AWS Config 規則的已啟用 CIS v5.0.0 變更觸發控制項的問題清單，您必須在 中記錄下列類型的資源 AWS Config。

AWS 服務	資源類型
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::Instance , AWS::EC2::NetworkAcl , AWS::EC2::SecurityGroup , AWS::EC2::VPC
Amazon Elastic File System (Amazon EFS)	AWS::EFS::FileSystem
AWS Identity and Access Management (IAM)	AWS::IAM::Group , AWS::IAM::User , AWS::IAM::Role
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBInstance , AWS::RDS::DBCluster
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket

CIS v3.0.0 的必要資源

若要讓 Security Hub CSPM 準確報告使用 AWS Config 規則的已啟用 CIS v3.0.0 變更觸發控制項的問題清單，您必須在 中記錄下列類型的資源 AWS Config。

AWS 服務	資源類型
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::Instance , AWS::EC2::NetworkAcl , AWS::EC2::SecurityGroup , AWS::EC2::VPC
AWS Identity and Access Management (IAM)	AWS::IAM::Group , AWS::IAM::User , AWS::IAM::Role
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBInstance
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket

CIS v1.4.0 的必要資源

若要讓 Security Hub CSPM 準確報告使用 AWS Config 規則的已啟用 CIS v1.4.0 變更觸發控制項的問題清單，您必須在 中記錄下列類型的資源 AWS Config。

AWS 服務	資源類型
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::NetworkAcl , AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBInstance
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket

CIS v1.2.0 的必要資源

若要讓 Security Hub CSPM 準確報告使用 AWS Config 規則的已啟用 CIS v1.2.0 變更觸發控制項的問題清單，您必須在 中記錄下列類型的資源 AWS Config。

AWS 服務	資源類型
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User

NIST SP 800-53 修訂版 5 標準的必要資源

若要讓 Security Hub CSPM 準確報告適用於 NIST SP 800-53 修訂版 5 標準的變更觸發控制項的問題清單，啟用並使用 AWS Config 規則，您必須在其中記錄下列類型的資源 AWS Config。如需此標準的資訊，請參閱 [Security Hub CSPM 中的 NIST SP 800-53 修訂版 5](#)。

AWS 服務	資源類型
Amazon API Gateway	AWS::ApiGateway::Stage , AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint
Amazon Bedrock AgentCore	AWS::BedrockAgentCore::Gateway , AWS::BedrockAgentCore::Memory
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
AWS CodeBuild	AWS::CodeBuild::Project

AWS 服務	資源類型
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint , AWS::DMS::ReplicationInstance , AWS::DMS::ReplicationTask
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::EIP , AWS::EC2::Instance , AWS::EC2::LaunchTemplate , AWS::EC2::NetworkAcl , AWS::EC2::NetworkInterface , AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::TransitGateway , AWS::EC2::VPNConnection , AWS::EC2::Volume
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup , AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster , AWS::ECS::Service , AWS::ECS::TaskDefinition
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS::Cluster
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment

AWS 服務	資源類型
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer , AWS::ElasticLoadBalancingV2::Listener , AWS::ElasticLoadBalancingV2::LoadBalancer
Amazon ElasticSearch	AWS::Elasticsearch::Domain
Amazon EMR	AWS::EMR::SecurityConfiguration
Amazon EventBridge	AWS::Events::Endpoint , AWS::Events::EventBus
AWS Glue	AWS::Glue::Job
AWS Identity and Access Management (IAM)	AWS::IAM::Group , AWS::IAM::Policy , AWS::IAM::Role , AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias , AWS::KMS::Key
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	AWS::MSK::Cluster
Amazon MQ	AWS::AmazonMQ::Broker
AWS Network Firewall	AWS::NetworkFirewall::Firewall , AWS::NetworkFirewall::FirewallPolicy , AWS::NetworkFirewall::RuleGroup
Amazon OpenSearch Service	AWS::OpenSearch::Domain

AWS 服務	資源類型
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster , AWS::RDS::DBClusterSnapshot , AWS::RDS::DBInstance , AWS::RDS::DBSnapshot , AWS::RDS::EventSubscription
Amazon Redshift	AWS::Redshift::Cluster , AWS::Redshift::ClusterSubnetGroup
Amazon Route 53	AWS::Route53::HostedZone
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint , AWS::S3::AccountPublicAccessBlock , AWS::S3::Bucket
AWS Service Catalog	AWS::ServiceCatalog::Portfolio
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance , AWS::SSM::ManagedInstanceInventory , AWS::SSM::PatchCompliance
Amazon SageMaker AI	AWS::SageMaker::FeatureGroup , AWS::SageMaker::NotebookInstance
AWS Secrets Manager	AWS::SecretsManager::Secret
AWS Transfer Family	AWS::Transfer::Connector

AWS 服務	資源類型
AWS WAF	AWS::WAF::Rule , AWS::WAF::RuleGroup , AWS::WAF::WebACL , AWS::WAFRegional::Rule , AWS::WAFRegional::RuleGroup , AWS::WAFRegional::WebACL , AWS::WAFv2::RuleGroup , AWS::WAFv2::WebACL

NIST SP 800-171 修訂版 2 標準所需的資源

若要讓 Security Hub CSPM 準確報告適用於 NIST SP 800-171 修訂版 2 標準、已啟用並使用 AWS Config 規則的變更觸發控制項問題清單，您必須在其中記錄下列類型的資源 AWS Config。如需此標準的資訊，請參閱 [Security Hub CSPM 中的 NIST SP 800-171 修訂版 2](#)。

AWS 服務	資源類型
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
Amazon API Gateway	AWS::ApiGateway::Stage
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::ClientVpnEndpoint , AWS::EC2::NetworkAcl , AWS::EC2::SecurityGroup , AWS::EC2::VPC , AWS::EC2::VPNConnection
Elastic Load Balancing	AWS::ElasticLoadBalancing::LoadBalancer
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Alias , AWS::KMS::Key

AWS 服務	資源類型
AWS Network Firewall	AWS::NetworkFirewall::FirewallPolicy , AWS::NetworkFirewall::RuleGroup
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
AWS Systems Manager (SSM)	AWS::SSM::PatchCompliance
AWS WAF	AWS::WAFv2::RuleGroup

PCI DSS v3.2.1 的必要資源

若要讓 Security Hub CSPM 準確報告適用於支付卡產業資料安全標準 (PCI DSS) v3.2.1 的控制項問題清單，啟用 並使用 AWS Config 規則，您必須在其中記錄下列類型的資源 AWS Config。如需此標準的資訊，請參閱 [Security Hub CSPM 中的 PCI DSS](#)。

AWS 服務	資源類型
AWS CodeBuild	AWS::CodeBuild::Project
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::EIP , AWS::EC2::Instance , AWS::EC2::SecurityGroup
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScalingGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy , AWS::IAM::User
AWS Lambda	AWS::Lambda::Function
Amazon OpenSearch Service	AWS::OpenSearch::Domain

AWS 服務	資源類型
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBClusterSnapshot , AWS::RDS::DBInstance , AWS::RDS::DBSnapshot
Amazon Redshift	AWS::Redshift::Cluster
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccountPublicAccessBlock , AWS::S3::Bucket
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance , AWS::SSM::ManagedInstanceInventory , AWS::SSM::PatchCompliance

資源標記標準所需的 AWS 資源

套用至 AWS 資源標記標準的所有控制項都會觸發變更並使用 AWS Config 規則。若要讓 Security Hub CSPM 準確報告這些控制項的問題清單，您必須在其中記錄下列類型的資源 AWS Config。如需此標準的資訊，請參閱 [AWS Security Hub CSPM 中的資源標記標準](#)。

AWS 服務	資源類型
AWS Amplify	AWS::Amplify::App , AWS::Amplify::Branch
Amazon AppFlow	AWS::AppFlow::Flow
AWS App Runner	AWS::AppRunner::Service , AWS::AppRunner::VpcConnector
AWS AppConfig	AWS::AppConfig::Application , AWS::AppConfig::ConfigurationProfile , AWS::AppConfig::Environment , AWS::AppConfig::ExtensionAssociation

AWS 服務	資源類型
AWS AppSync	AWS::AppSync::GraphQLApi
Amazon Athena	AWS::Athena::DataCatalog , AWS::Athena::WorkGroup
AWS Backup	AWS::Backup::BackupPlan , AWS::Backup::BackupVault , AWS::Backup::RecoveryPlan , AWS::Backup::ReportPlan
AWS Batch	AWS::Batch::ComputeEnvironment , AWS::Batch::JobQueue , AWS::Batch::SchedulingPolicy
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
AWS CloudTrail	AWS::CloudTrail::Trail
AWS CodeArtifact	AWS::CodeArtifact::Repository
Amazon CodeGuru	AWS::CodeGuruProfiler::ProfilingGroup , AWS::CodeGuruReviewer::RepositoryAssociation
Amazon Connect 客戶	AWS::CustomerProfiles::ObjectType
AWS Database Migration Service (AWS DMS)	AWS::DMS::Certificate , AWS::DMS::EventSubscription AWS::DMS::ReplicationInstance , AWS::DMS::ReplicationSubnetGroup
AWS DataSync	AWS::DataSync::Task

AWS 服務	資源類型
Amazon Detective	AWS::Detective::Graph
Amazon DynamoDB	AWS::DynamoDB::Trail
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::CustomerGateway , AWS::EC2::DHCPOptions , AWS::EC2: :EIP , AWS::EC2::FlowLog , AWS::EC2: :Instance , AWS::EC2::Internet Gateway , AWS::EC2::LaunchTe mplate , AWS::EC2::NatGateway , AWS::EC2::NetworkAcl , AWS::EC2: :NetworkInterface , AWS::EC2: :PrefixList , AWS::EC2::RouteTab le , AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2: :TrafficMirrorFilter , AWS::EC2: :TrafficMirrorSession , AWS::EC2: :TrafficMirrorTarget , AWS::EC2: :TransitGateway , AWS::EC2: :TransitGatewayAttachment , AWS::EC2::TransitGatewayRou teTable , AWS::EC2::Volume , AWS::EC2::VPC , AWS::EC2::VPCEndpo intService , AWS::EC2::VPCPeeri ngConnection , AWS::EC2::VPNGatew ay
Amazon EC2 Auto Scaling	AWS::AutoScaling::AutoScali ngGroup
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::PublicRepository

AWS 服務	資源類型
Amazon Elastic Container Service (Amazon ECS)	<code>AWS::ECS::Cluster</code> , <code>AWS::ECS::Service</code> , <code>AWS::ECS::TaskDefinition</code>
Amazon Elastic File System (Amazon EFS)	<code>AWS::EFS::AccessPoint</code>
Amazon Elastic Kubernetes Service (Amazon EKS)	<code>AWS::EKS::Cluster</code> , <code>AWS::EKS::IdentityProviderConfig</code>
AWS Elastic Beanstalk	<code>AWS::ElasticBeanstalk::Environment</code>
ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EventBridge	<code>AWS::Events::EventBus</code>
Amazon Fraud Detector	<code>AWS::FraudDetector::EntityType</code> , <code>AWS::FraudDetector::Label</code> <code>AWS::FraudDetector::Outcome</code> , <code>AWS::FraudDetector::Variable</code>
AWS Global Accelerator	<code>AWS::GlobalAccelerator::Accelerator</code>
AWS Glue	<code>AWS::Glue::Job</code>
Amazon GuardDuty	<code>AWS::GuardDuty::Detector</code> , <code>AWS::GuardDuty::Filter</code> , <code>AWS::GuardDuty::IPSet</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Role</code> , <code>AWS::IAM::User</code>
AWS Identity and Access Management Access Analyzer (IAM Access Analyzer)	<code>AWS::AccessAnalyzer::Analyzer</code>

AWS 服務	資源類型
AWS IoT	AWS::IoT::Authorizer , AWS::IoT::Dimension , AWS::IoT::MitigationAction , AWS::IoT::Policy , AWS::IoT::RoleAlias , AWS::IoT::SecurityProfile
AWS IoT 活動	AWS::IoTEvents::AlarmModel , AWS::IoTEvents::DetectorModel , AWS::IoTEvents::Input
AWS IoT SiteWise	AWS::IoTSiteWise::Dashboard , AWS::IoTSiteWise::Gateway , AWS::IoTSiteWise::Portal , AWS::IoTSiteWise::Project
AWS IoT TwinMaker	AWS::IoTTwinMaker::Entity , AWS::IoTTwinMaker::Scene , AWS::IoTTwinMaker::SyncJob , AWS::IoTTwinMaker::Workspace
AWS IoT 無線	AWS::IoTWireless::FirmwareTask , AWS::IoTWireless::MulticastGroup , AWS::IoTWireless::ServiceProfile
Amazon Interactive Video Service (Amazon IVS)	AWS::IVS::Channel , AWS::IVS::PlaybackKeyPair , AWS::IVS::RecordingConfiguration
Amazon Keyspaces (適用於 Apache Cassandra)	AWS::Cassandra::Keyspace
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
Amazon MQ	AWS::AmazonMQ::Broker

AWS 服務	資源類型
AWS Network Firewall	AWS::NetworkFirewall::Firewall , AWS::NetworkFirewall::FirewallPolicy
Amazon OpenSearch Service	AWS::OpenSearch::Domain
AWS 私有憑證授權單位	AWS::ACMPCA::CertificateAuthority
Amazon Relational Database Service	AWS::RDS::DBCluster , AWS::RDS::DBClusterSnapshot , AWS::RDS::DBInstance , AWS::RDS::DBSecurityGroup , AWS::RDS::DBSnapshot , AWS::RDS::DBSubnetGroup
Amazon Redshift	AWS::Redshift::Cluster , AWS::Redshift::ClusterParameterGroup , AWS::Redshift::ClusterSnapshot , AWS::Redshift::ClusterSubnetGroup , AWS::Redshift::EventSubscription
Amazon Route 53	AWS::Route53::HealthCheck
Amazon SageMaker AI	AWS::SageMaker::AppImageConfig , AWS::SageMaker::Image
AWS Secrets Manager	AWS::SecretsManager::Secret
Amazon Simple Email Service (Amazon SES)	AWS::SES::ConfigurationSet , AWS::SES::ContactList
Amazon Simple Notification Service (Amazon SNS)	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue

AWS 服務	資源類型
AWS Step Functions	AWS::StepFunctions::Activity
AWS Systems Manager (SSM)	AWS::SSM::Document
AWS Transfer Family	AWS::Transfer::Agreement , AWS::Transfer::Certificate , AWS::Transfer::Connector , AWS::Transfer::Profile , AWS::Transfer::Workflow

執行安全檢查的排程

啟用安全標準後，AWS Security Hub CSPM 會在兩小時內開始執行所有檢查。大多數檢查會在 25 分鐘內開始執行。Security Hub CSPM 透過評估控制項基礎的規則來執行檢查。在控制項完成第一次執行檢查之前，其狀態為無資料。

當您啟用新標準時，Security Hub CSPM 最多可能需要 24 小時才能產生控制項的調查結果，這些控制項使用與其他啟用標準中已啟用的控制項相同的基礎 AWS Config 服務連結規則。例如，如果您在 AWS 基礎安全最佳實務 (FSBP) 標準中啟用 [Lambda.1](#) 控制項，Security Hub CSPM 會建立服務連結規則，通常在幾分鐘內產生問題清單。之後，如果您在支付卡產業資料安全標準 (PCI DSS) 中啟用 Lambda.1 控制項，Security Hub CSPM 最多可能需要 24 小時才能產生控制項的問題清單，因為它使用相同的服務連結規則。

初次檢查後，每個控制項的排程可以定期或觸發變更。對於以受管 AWS Config 規則為基礎的控制項，控制項描述包含《AWS Config 開發人員指南》中規則描述的連結。該描述指定規則是觸發還是定期變更。

定期安全檢查

定期安全檢查會在最近一次執行後的 12 或 24 小時內自動執行。Security Hub CSPM 會決定週期性，您無法變更。定期控制反映檢查執行時的評估。

如果您更新定期控制調查結果的工作流程狀態，然後在下次檢查調查結果的合規狀態保持不變，工作流程狀態會保持修改狀態。例如，如果您的 [KMS.4](#) 控制項問題清單失敗 (AWS KMS key 應該啟用輪換)，然後修復問題清單，Security Hub CSPM 會將工作流程狀態從 變更為 NEW RESOLVED。如果您在下一次定期檢查之前停用 KMS 金鑰輪換，則調查結果的工作流程狀態會保持 RESOLVED。

使用 Security Hub CSPM 自訂 Lambda 函數的檢查是定期的。

變更觸發的安全檢查

當關聯的資源變更狀態時，會執行變更觸發的安全性檢查。AWS Config 您可以在持續記錄資源狀態的變更和每日記錄之間進行選擇。如果您選擇每日錄製，如果資源狀態發生變更，會在每 24 小時期間結束時 AWS Config 傳送資源組態資料。如果沒有變更，則不會交付任何資料。這可能會延遲 Security Hub CSPM 調查結果的產生，直到 24 小時期間完成為止。無論您選擇的記錄期間為何，Security Hub CSPM 至少每 24 小時檢查一次，以確保沒有 AWS Config 遺漏來自的資源更新。

一般而言，Security Hub CSPM 會盡可能使用變更觸發的規則。若要讓資源使用變更觸發的規則，它必須支援 AWS Config 組態項目。

產生和更新控制問題清單

AWS 當 Security Hub CSPM 針對安全控制執行檢查時，會產生和更新控制問題清單。控制問題清單使用[AWS 安全問題清單格式 \(ASFF\)](#)。

Security Hub CSPM 通常會針對控制項的每個安全檢查收取費用。不過，如果多個控制項使用相同的 AWS Config 規則，Security Hub CSPM 只會針對每個針對規則的檢查收取一次費用。例如，CIS AWS Foundations Benchmark 標準和 AWS 基礎安全最佳實務標準中的多個控制項會使用 AWS Config iam-password-policy 規則。每次 Security Hub CSPM 針對該規則執行檢查時，都會為每個相關控制項產生個別的控制調查結果，但檢查只會收取一次費用。

如果控制項調查結果的大小超過 240 KB 的上限，Security Hub CSPM 會從調查結果中移除 Resource.Details 物件。對於資源 AWS Config 支援的控制項，您可以使用 AWS Config 主控台來檢閱資源詳細資訊。

主題

- [合併的控制問題清單](#)
- [產生、更新和封存控制問題清單](#)
- [自動化和抑制控制問題清單](#)
- [控制問題清單的合規詳細資訊](#)
- [控制問題清單的 ProductFields 詳細資訊](#)
- [控制問題清單的嚴重性等級](#)

合併的控制問題清單

如果您的帳戶已啟用合併控制調查結果，即使控制項適用於多個已啟用的標準，Security Hub CSPM 仍會為每個控制項的安全檢查產生單一調查結果或調查結果更新。如需控制項及其適用的標準清單，請參閱 [Security Hub CSPM 的控制項參考](#)。我們建議您啟用合併控制調查結果，以減少調查結果的雜訊。

如果您在 2023 年 2 月 23 日 AWS 帳戶日之前為 啟用 Security Hub CSPM，您可以按照本節稍後的說明啟用合併控制問題清單。如果您在 2023 年 2 月 23 日或之後啟用 Security Hub CSPM，則會自動為您的帳戶啟用合併控制問題清單。

如果您透過[手動邀請程序](#)使用 [Security Hub CSPM 與 或受邀成員帳戶整合 AWS Organizations](#)，則只有在成員帳戶啟用管理員帳戶時，才會為成員帳戶啟用合併控制問題清單。如果停用管理員帳戶的功能，則會停用成員帳戶的功能。此行為適用於新的和現有的成員帳戶。此外，如果管理員使用[中央組態](#)來管理多個帳戶的 Security Hub CSPM，則無法使用中央組態政策來啟用或停用帳戶的合併控制問題清單。

如果您停用帳戶的合併控制問題清單，Security Hub CSPM 會為每個已啟用且包含控制項的標準產生或更新個別的控制問題清單。例如，如果您啟用四個共用控制項的標準，您會在控制項安全檢查後收到四個單獨的問題清單。如果您啟用合併控制調查結果，則只會收到一個調查結果。

當您啟用合併控制調查結果時，Security Hub CSPM 會建立新的標準獨立調查結果，並封存原始標準型調查結果。有些控制項問題清單欄位和值將會變更，這可能會影響您現有的工作流程。如需這些變更的詳細資訊，請參閱 [合併控制調查結果 – ASFF 變更](#)。啟用合併控制調查結果也可能影響整合的第三方產品從 Security Hub CSPM 收到的調查結果。如果您使用 [v2 AWS .0.0 上的自動安全回應](#)解決方案，請注意它支援合併的控制問題清單。

若要啟用或停用合併控制調查結果，您必須登入管理員帳戶或獨立帳戶。

Note

啟用合併控制調查結果後，Security Hub CSPM 最多可能需要 24 小時才能產生新的合併調查結果，並封存現有的標準型調查結果。同樣地，停用合併控制問題清單後，Security Hub CSPM 最多可能需要 24 小時才能產生新的標準問題清單，並封存現有的合併問題清單。在這些期間，您可能會在帳戶中看到標準無關和標準型問題清單的混合。

Security Hub CSPM console

啟用或停用合併控制問題清單

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，於 Settings (設定) 下選擇 General (一般)。
3. 在控制項區段中，選擇編輯。
4. 使用合併控制問題清單切換來啟用或停用合併控制問題清單。
5. 選擇儲存。

Security Hub CSPM API

若要以程式設計方式啟用或停用合併控制問題清單，請使用 Security Hub CSPM API [UpdateSecurityHubConfiguration](#) 的操作。或者，如果您使用的是 AWS CLI，請執行 [update-security-hub-configuration](#) 命令。

針對 `control-finding-generator` 參數，指定 `SECURITY_CONTROL` 以啟用合併的控制項問題清單。若要停用合併控制調查結果，請指定 `STANDARD_CONTROL`。

例如，下列 AWS CLI 命令會啟用合併的控制問題清單。

```
$ aws securityhub --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

下列 AWS CLI 命令會停用合併的控制問題清單。

```
$ aws securityhub --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

產生、更新和封存控制問題清單

Security Hub CSPM 會依[排程](#)執行安全檢查。第一次 Security Hub CSPM 執行控制項的安全檢查時，它會為控制項檢查的每個 AWS 資源產生新的問題清單。每次 Security Hub CSPM 隨後執行控制項的安全檢查時，都會更新現有的調查結果以報告檢查結果。這表示您可以使用個別調查結果提供的資料，根據特定控制項追蹤特定資源的合規變更。

例如，如果特定控制項的資源合規狀態從 變更為 FAILED PASSED，Security Hub CSPM 不會產生新的調查結果。相反地，Security Hub CSPM 會更新控制項和資源的現有問題清單。在調查結果中，Security Hub CSPM 會將合規狀態 (Compliance.Status) 欄位的值變更為 PASSED。Security Hub CSPM 也會更新其他欄位的值，以反映檢查的結果，例如嚴重性標籤、工作流程狀態和時間戳記，指出 Security Hub CSPM 最近何時執行檢查並更新調查結果。

報告合規狀態變更時，Security Hub CSPM 可能會更新控制調查結果中的下列任何欄位：

- `Compliance.Status` – 指定控制項之資源的新合規狀態。
- `FindingProviderFields.Severity.Label` – 問題清單嚴重性的新定性表示法，例如 LOW、MEDIUM 或 HIGH。
- `FindingProviderFields.Severity.Original` – 調查結果嚴重性的新量化表示，例如 0 合規資源。
- `FirstObservedAt` – 資源的合規狀態最近變更時。
- `LastObservedAt` – 當 Security Hub CSPM 最近針對指定的控制項和資源執行安全檢查時。
- `ProcessedAt` – Security Hub CSPM 最近開始處理問題清單時。
- `ProductFields.PreviousComplianceStatus` – 指定控制項之資源的先前合規狀態 (`Compliance.Status`)。
- `UpdatedAt` – Security Hub CSPM 最近更新問題清單時。
- `Workflow.Status` – 根據指定控制項之資源的新合規狀態，調查調查結果的狀態。

Security Hub CSPM 是否會更新欄位，主要取決於適用控制項和資源的最新安全性檢查結果。例如，如果特定控制項的資源合規狀態從 PASSED 變更為 FAILED，Security Hub CSPM 會將調查結果的工作流程狀態變更為 NEW。若要追蹤個別問題清單的更新，您可以參考問題清單的歷史記錄。如需調查結果中個別欄位的詳細資訊，請參閱[AWS 安全調查結果格式 \(ASFF\)](#)。

在某些情況下，Security Hub CSPM 會為控制項的後續檢查產生新的問題清單，而不是更新現有的問題清單。如果支援控制項的 AWS Config 規則發生問題，就可能發生這種情況。如果發生這種情況，Security Hub CSPM 會封存現有的問題清單，並為每個檢查產生新的問題清單。在新調查結果中，合規狀態為 NOT_AVAILABLE，記錄狀態為 ARCHIVED。解決 AWS Config 規則的問題後，Security Hub CSPM 會產生新的問題清單，並開始更新這些問題清單，以追蹤個別資源的合規狀態後續變更。

除了產生和更新控制調查結果之外，Security Hub CSPM 也會自動封存符合特定條件的控制調查結果。如果停用控制項、刪除指定的資源，或指定的資源不再存在，Security Hub CSPM 會封存問題清

單。資源可能不再存在，因為已不再使用相關聯的服務。更具體地說，如果問題清單符合下列其中一項條件，Security Hub CSPM 會自動封存控制問題清單：

- 問題清單已有 3-5 天未更新。請注意，基於此時間範圍的封存是以最佳努力為基礎，不保證。
- 針對指定資源的NOT_APPLICABLE合規狀態傳回的相關聯 AWS Config 評估。

若要判斷問題清單是否已封存，您可以參考問題清單的記錄狀態 (RecordState) 欄位。如果問題清單已封存，此欄位的值為 ARCHIVED。

Security Hub CSPM 會將封存的控制調查結果存放 30 天。30 天後，問題清單會過期，而 Security Hub CSPM 會永久刪除問題清單。為了判斷封存的控制項調查結果是否已過期，Security Hub CSPM 會根據調查結果UpdatedAt欄位的值來計算。

若要存放封存的控制調查結果超過 30 天，您可以將調查結果匯出至 S3 儲存貯體。您可以搭配 Amazon EventBridge 規則使用自訂動作來執行此操作。如需詳細資訊，請參閱[使用 EventBridge 進行自動回應和修復](#)。

Note

在 2025 年 7 月 3 日之前，當控制項的資源合規狀態變更時，Security Hub CSPM 會以不同的方式產生和更新控制項調查結果。先前，Security Hub CSPM 建立了新的控制調查結果，並封存了資源的現有調查結果。因此，您可能會針對特定控制項和資源有多個封存的問題清單，直到這些問題清單過期為止 (30 天後)。

自動化和抑制控制問題清單

您可以使用 Security Hub CSPM 自動化規則來更新或隱藏特定控制問題清單。如果您隱藏問題清單，您可以繼續存取問題清單。不過，隱藏表示您相信不需要採取任何動作來解決問題清單。

透過抑制問題清單，您可以減少問題清單的雜訊。例如，您可能會隱藏測試帳戶中產生的控制問題清單。或者，您可以隱藏與特定資源相關的問題清單。若要進一步了解自動更新或隱藏問題清單，請參閱[了解 Security Hub CSPM 中的自動化規則](#)。

當您想要更新或隱藏特定控制問題清單時，自動化規則是適當的。不過，如果控制項與您的組織或使用案例無關，建議您[停用控制項](#)。如果您停用控制項，Security Hub CSPM 不會對其執行安全檢查，也不會向您收取費用。

控制問題清單的合規詳細資訊

在控制項安全檢查所產生的調查結果中，AWS 安全調查結果格式 (ASFF) 中的[合規](#)物件和欄位會提供控制項檢查之個別資源的合規詳細資訊。這包括以下資訊：

- **AssociatedStandards** – 啟用控制項的已啟用標準。
- **RelatedRequirements** – 所有啟用標準中控制項的相關需求。這些要求衍生自 控制項的第三方安全架構，例如支付卡產業資料安全標準 (PCI DSS) 或 NIST SP 800-171 修訂版 2 標準。
- **SecurityControlId** – Security Hub CSPM 支援跨標準控制的識別符。
- **Status** – Security Hub CSPM 為控制項執行的最新檢查結果。先前檢查的結果會保留在調查結果的歷史記錄中。
- **StatusReasons** – 列出 Status 欄位指定值原因的陣列。對於每個原因，這包括原因代碼和描述。

下表列出問題清單可能包含在StatusReasons陣列中的原因代碼和描述。修復步驟會根據哪個控制項產生具有指定原因碼的問題清單而有所不同。若要檢閱控制項的修補指引，請參閱 [Security Hub CSPM 的控制項參考](#)。

原因代碼	合規狀態	Description
CLOUDTRAIL_METRIC_FILTER_NOT_VALID	FAILED	多區域 CloudTrail 追蹤沒有有效的指標篩選條件。
CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT	FAILED	多區域 CloudTrail 追蹤沒有指標篩選條件。
CLOUDTRAIL_MULTI_REGION_NOT_PRESENT	FAILED	帳戶沒有具有所需組態的多區域 CloudTrail 追蹤。
CLOUDTRAIL_REGION_INVALID	WARNING	多區域 CloudTrail 追蹤不在目前的區域中。
CLOUDWATCH_ALARM_ACTIONS_NOT_VALID	FAILED	沒有有效的警示動作。
CLOUDWATCH_ALARMS_NOT_PRESENT	FAILED	CloudWatch 警示不存在於帳戶中。

原因代碼	合規狀態	Description
CONFIG_ACCESS_DENIED	NOT_AVAILABLE AWS Config 狀態為 ConfigError	AWS Config 存取遭拒。 確認 AWS Config 已啟用，且已獲得足夠的許可。
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config 根據 規則評估您的 資源。 此規則不適用於其範圍內 AWS 的資源、已刪除指定的資源，或已刪除評估結果。
CONFIG_RECORDER_CUSTOM_ROLE	FAILED (適用於 Config.1)	AWS Config 記錄器使用自訂 IAM 角色而非 AWS Config 服務連結角色，而且 Config.1 的includeConfigServiceLinkedRoleCheck 自訂參數未設定為 false。
CONFIG_RECORDER_DISABLED	FAILED (適用於 Config.1)	AWS Config 未在組態記錄器開啟的情況下啟用。
CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES	FAILED (適用於 Config.1)	AWS Config 不會記錄對應至已啟用 Security Hub CSPM 控制項的所有資源類型。開啟下列資源的錄製：#### ##。

原因代碼	合規狀態	Description
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	合規狀態為 <code>NOT_AVAILABLE</code> 因為 AWS Config 傳回的狀態為不適用。 AWS Config 不提供狀態的原因。以下是不適用狀態的一些可能原因： - 資源已從 AWS Config 規則的範圍中移除。 - 已刪除 AWS Config 規則。 - 資源已刪除。 - AWS Config 規則邏輯可以產生不適用狀態。
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE AWS Config 狀態為 <code>ConfigError</code>	這個原因代碼用於數種不同類型的評估錯誤。 此描述會提供特定的原因資訊。錯誤類型可以是下列其中一項： - 由於缺乏許可，因此無法執行評估。此描述提供遺失的特定許可。 - 缺少或無效的參數值。此描述提供參數和參數值的需求。 - 從 S3 儲存貯體讀取時發生錯誤。此描述可識別儲存貯體並提供特定的錯誤。 - 缺少 AWS 訂閱。 - 評估的一般逾時。 - 遭停權的帳戶。

原因代碼	合規狀態	Description
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE AWS Config 狀態為 ConfigError	AWS Config 規則正在建立中。
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	發生未知的錯誤。
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	FAILED	Security Hub CSPM 無法針對自訂 Lambda 執行時間執行檢查。
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	調查結果處於 WARNING 狀態，因為與此規則相關聯的 S3 儲存貯體位於不同的區域或帳戶中。 此規則不支援跨區域或跨帳戶檢查。 建議您在此區域或帳戶中停用此控制項。只能在資源所在的區域或帳戶中執行。
SNS_SUBSCRIPTION_NOT_PRESENT	FAILED	CloudWatch Logs 指標篩選條件沒有有效的 Amazon SNS 訂閱。
SNS_TOPIC_CROSS_ACCOUNT	WARNING	問題清單處於 WARNING 狀態。 與此規則相關聯的 SNS 主題由不同的帳戶擁有。目前帳戶無法取得訂閱資訊。 擁有 SNS 主題的帳戶必須將 SNS 主題的 <code>sns:ListSubscriptionsByTopic</code> 許可授予目前帳戶。

原因代碼	合規狀態	Description
SNS_TOPIC_CROSS_AC COUNT_CROSS_REGION	WARNING	調查結果處於 WARNING 狀態，因為與此規則相關聯的 SNS 主題位於不同的區域或帳戶中。 此規則不支援跨區域或跨帳戶檢查。 建議您在此區域或帳戶中停用此控制項。只能在資源所在的區域或帳戶中執行。
SNS_TOPIC_INVALID	FAILED	與此規則相關聯的 SNS 主題無效。
THROTTLING_ERROR	NOT_AVAILABLE	相關 API 操作超過允許的速率。

控制問題清單的 ProductFields 詳細資訊

在 控制項安全檢查產生的調查結果中，AWS 安全調查結果格式 (ASFF) 中的 [ProductFields](#) 屬性可包含下列欄位。

ArchivalReasons:0/Description

說明 Security Hub CSPM 封存問題清單的原因。

例如，Security Hub CSPM 會在您停用控制項或標準時封存現有的問題清單，或者啟用或停用[合併的控制項問題清單](#)。

ArchivalReasons:0/ReasonCode

指定 Security Hub CSPM 封存問題清單的原因。

例如，Security Hub CSPM 會在您停用控制項或標準時封存現有的問題清單，或者啟用或停用[合併的控制項問題清單](#)。

PreviousComplianceStatus

指定控制項之資源的先前合規狀態 (Compliance.Status)，截至調查結果的最近更新為止。如果資源的合規狀態未在最近的更新期間變更，則此值與調查結果 Compliance.Status 欄位的值相同。如需可能值的清單，請參閱 [評估合規狀態和控制狀態](#)。

StandardsGuideArn 或 StandardsArn

與控制項相關聯的標準 ARN。

針對 CIS AWS Foundations Benchmark 標準，欄位為 StandardsGuideArn。對於 PCI DSS 和 AWS 基礎安全最佳實務標準，欄位為 StandardsArn。

Compliance.AssociatedStandards 如果您啟用[合併控制問題清單](#)，這些欄位會移除。

StandardsGuideSubscriptionArn 或 StandardsSubscriptionArn

帳戶對標準的訂閱 ARN。

針對 CIS AWS Foundations Benchmark 標準，欄位為 StandardsGuideSubscriptionArn。對於 PCI DSS 和 AWS 基礎安全最佳實務標準，欄位為 StandardsSubscriptionArn。

如果您啟用[合併控制調查結果](#)，則會移除這些欄位。

RuleId 或 ControlId

控制項的識別符。

對於 CIS AWS Foundations Benchmark 標準的 1.2.0 版，欄位為 RuleId。對於其他標準，包括後續版本的 CIS AWS Foundations Benchmark 標準，欄位為 ControlId。

Compliance.SecurityControlId 如果您啟用[合併的控制問題清單](#)，這些欄位會移除。

RecommendationUrl

控制項的修補資訊 URL。Remediation.Recommendation.Url 如果您啟用[合併的控制問題清單](#)，則此欄位會移除。

RelatedAWSResources:0/name

與調查結果相關聯的資源名稱。

RelatedAWSResource:0/type

與控制項相關聯的資源類型。

StandardsControlArn

組態的 ARN。如果您啟用[合併控制調查結果](#)，則會移除此欄位。

aws/securityhub/ProductArn

對於控制項調查結果，產品名稱為 Security Hub。

aws/securityhub/CompanyName

對於控制項調查結果，公司名稱為 AWS。

aws/securityhub/annotation

控制項所發現問題的描述。

aws/securityhub/FindingId

調查結果的識別符。

如果您啟用[合併控制調查結果](#)，則此欄位不會參考標準。

控制問題清單的嚴重性等級

指派給 Security Hub CSPM 控制項的嚴重性表示控制項的重要性。控制項的嚴重性決定指派給控制項調查結果的嚴重性標籤。

嚴重性條件

控制項的嚴重性取決於下列條件的評估：

- 威脅行為者利用與控制項相關聯的組態弱點有多困難？難度取決於使用弱點來執行威脅案例所需的複雜程度或複雜性。
- 弱點對您的 AWS 帳戶 或 資源造成損害的可能性有多高？入侵您的 AWS 帳戶 或 資源意味著資料或 AWS 基礎設施的機密性、完整性或可用性在某種程度上受損。入侵的可能性表示威脅案例造成 AWS 服務 或 資源中斷或違規的可能性。

例如，請考慮下列組態弱點：

- 使用者存取金鑰不會每 90 天輪換一次。
- IAM 根使用者金鑰存在。

對手也同樣難以利用這兩個弱點。在這兩種情況下，對手都可以使用憑證盜竊或其他方法來取得使用者金鑰。然後，他們可以使用它，以未經授權的方式存取您的資源。

不過，如果威脅行為者取得根使用者存取金鑰，則入侵的可能性會更高，因為這樣可以讓他們存取更多。因此，根使用者金鑰弱點的嚴重性較高。

嚴重性不會考慮基礎資源的重要性。關鍵性是與調查結果相關聯之資源的重要性層級。例如，與關鍵任務應用程式相關聯的資源比與非生產測試相關聯的資源更重要。若要擷取資源關鍵性資訊，請使用 AWS 安全調查結果格式 (ASFF) Criticality 的欄位。

下表映射了難以利用以及入侵安全標籤的可能性。

	極有可能遭到入侵	可能遭到入侵	不太可能遭到入侵	極不可能入侵
非常容易利用	嚴重	嚴重	高	中
有點容易利用	嚴重	高	中	中
有些難以利用	高	中	中	低
非常難以利用	中	中	低	低

嚴重性定義

嚴重性標籤的定義如下。

嚴重 – 問題應該立即修復，以避免升級。

舉例來說，開啟的 S3 儲存貯體將視作重大嚴重性問題。由於有許多威脅執行者會掃描開啟的 S3 儲存貯體，因此公開的 S3 儲存貯體中的資料可能會被其他人探索和存取。

一般而言，可公開存取的資源會被視為重大安全問題。您應該最緊迫地處理關鍵問題清單。您也應該考慮資源的重要性。

高 – 問題必須以短期優先順序處理。

例如，如果預設 VPC 安全群組開放給傳入和傳出流量，則會被視為高嚴重性。威脅行為者使用此方法入侵 VPC 有點容易。一旦資源位於 VPC 中，威脅行為者也可能能夠中斷或滲透資源。

Security Hub CSPM 建議您將高嚴重性的問題清單視為短期優先順序。您應該立即採取修復步驟。您也應該考慮資源的重要性。

中 – 問題應該以中期優先順序處理。

例如，缺少傳輸中資料的加密會被視為中等嚴重性的問題清單。它需要複雜的 man-in-the-middle 攻擊，才能利用此弱點。換句話說，這有點困難。如果威脅案例成功，某些資料可能會遭到入侵。

Security Hub CSPM 建議您儘早調查隱含資源。您也應該考慮資源的重要性。

低 – 問題不需要自行執行動作。

例如，未能收集鑑識資訊視為低嚴重性。此控制有助於防止未來的入侵，但缺少鑑識不會直接導致入侵。

您不需要對低嚴重性的問題清單立即採取動作，但這些問題可在您與其他問題相互關聯時提供內容。

資訊 – 找不到組態弱點。

換句話說，狀態為 PASSED、WARNING 或 NOT AVAILABLE。

沒有任何建議的動作。參考性問題清單能協助客戶證明自己處於合規狀態。

評估合規狀態和控制狀態

安全性 AWS 調查結果格式 `Compliance.Status` 的欄位說明控制調查結果的結果。AWS Security Hub CSPM 使用控制調查結果的合規狀態來判斷整體控制狀態。控制項狀態會顯示在 Security Hub CSPM 主控台上控制項的詳細資訊頁面上。

評估 Security Hub CSPM 調查結果的合規狀態

每個調查結果的合規狀態會指派下列其中一個值：

- PASSED – 表示控制項已通過調查結果的安全檢查。這會自動將 Security Hub CSPM `Workflow.Status` 設定為 RESOLVED。
- FAILED – 表示控制項未通過調查結果的安全檢查。
- WARNING – 表示 Security Hub CSPM 無法判斷資源是否處於 PASSED 或 FAILED 狀態。例如，對應的 [AWS Config 資源類型不會開啟資源記錄](#)。
- NOT_AVAILABLE – 表示無法完成檢查，因為伺服器失敗、資源已刪除，或 AWS Config 評估結果為 NOT_APPLICABLE。如果 AWS Config 評估結果為 NOT_APPLICABLE，Security Hub CSPM 會自動封存問題清單。

如果調查結果的合規狀態從 變更為 PASSED FAILED、WARNING 或 NOT_AVAILABLE，且 `Workflow.Status` 為 NOTIFIED 或 RESOLVED，則 Security Hub CSPM 會自動 `Workflow.Status` 變更為 NEW。

如果您沒有與控制項對應的資源，Security Hub CSPM 會在帳戶層級產生 PASSED 問題清單。如果您有對應至控制項的資源，但接著刪除資源，Security Hub CSPM 會建立 NOT_AVAILABLE 問題清單並立即將其封存。18 小時後，您會收到 PASSED 調查結果，因為您不再有與控制項對應的資源。

從合規狀態衍生控制狀態

Security Hub CSPM 會從控制調查結果的合規狀態衍生整體控制狀態。判斷控制狀態時，Security Hub CSPM 會忽略具有 RecordState 的調查結果，ARCHIVED 以及具有 Workflow.Status 的調查結果 SUPPRESSED。

控制狀態會獲指派下列其中一個值：

- 已傳遞 – 表示所有調查結果的合規狀態為 PASSED。
- 失敗 – 表示至少一個調查結果的合規狀態為 FAILED。
- 未知 – 表示至少一個調查結果的合規狀態為 WARNING 或 NOT_AVAILABLE。沒有任何調查結果的合規狀態為 FAILED。
- 無資料 – 表示沒有控制項的問題清單。例如，新啟用的控制項具有此狀態，直到 Security Hub CSPM 開始為其產生問題清單為止。如果控制項的所有調查結果都為 SUPPRESSED 或目前中無法使用，則控制項也會有此狀態 AWS 區域。
- 已停用 – 表示控制項在目前帳戶和區域中已停用。目前未針對目前帳戶和區域中的此控制項執行任何安全檢查。不過，停用控制項的調查結果在停用後最多 24 小時內可能會有合規狀態的值。

對於管理員帳戶，控制狀態會反映管理員帳戶和成員帳戶的控制狀態。具體而言，如果控制項在管理員帳戶或任何成員帳戶中有一或多個失敗的問題清單，則控制項的整體狀態會顯示為失敗。如果您已設定彙總區域，則彙總區域中的控制項狀態會反映彙總區域和連結區域中的控制項狀態。具體而言，如果控制項在彙總區域或任何連結區域中有一或多個失敗的問題清單，則控制項的整體狀態會顯示為失敗。

Security Hub CSPM 通常會在您第一次造訪 Security Hub CSPM 主控台的摘要頁面或安全標準頁面後 30 分鐘內產生初始控制狀態。您必須設定 [AWS Config 資源記錄](#)，控制項狀態才會出現。第一次產生控制狀態之後，Security Hub CSPM 會根據過去 24 小時的調查結果，每 24 小時更新一次控制狀態。控制項詳細資訊頁面上的時間戳記指出上次更新控制項狀態的時間。

Note

第一次啟用控制項後，在中國區域和 中產生控制項狀態最多可能需要 24 小時 AWS GovCloud (US) Region。

計算安全分數

在 AWS Security Hub CSPM 主控台上，摘要頁面和控制頁面會顯示所有已啟用標準的摘要安全分數。在安全標準頁面上，Security Hub CSPM 也會為每個啟用的標準顯示 0-100% 的安全分數。

當您第一次啟用 Security Hub CSPM 時，Security Hub CSPM 會在您第一次造訪主控台的摘要或安全標準頁面後 30 分鐘內計算摘要安全分數和標準安全分數。只會針對您在主控台上造訪這些頁面時啟用的標準產生分數。此外，AWS Config 必須設定資源記錄，才能顯示分數。摘要安全分數是標準安全分數的平均值。若要檢閱目前啟用的標準清單，您可以使用 Security Hub CSPM API 的 [GetEnabledStandards](#) 操作。

第一次產生分數後，Security Hub CSPM 會每 24 小時更新一次安全分數。Security Hub CSPM 會顯示時間戳記，指出上次更新安全分數的時間。請注意，在中國區域和中，首次產生安全分數最多可能需要 24 小時 AWS GovCloud (US) Regions。

如果您開啟[合併控制問題清單](#)，可能需要長達 24 小時才能更新您的安全分數。此外，啟用新的彙總區域或更新連結的區域會重設現有的安全分數。Security Hub CSPM 最多可能需要 24 小時才能產生新的安全分數，其中包含來自更新區域的資料。

計算安全分數的方法

安全性分數代表已通過控制項與已啟用控制項的比例。分數會以百分比顯示，四捨五入或向下到最接近的整數。

Security Hub CSPM 會計算所有已啟用標準的摘要安全分數。Security Hub CSPM 也會計算每個已啟用標準的安全分數。為了計算分數，啟用的控制項包括狀態為通過、失敗和未知的控制項。狀態為 的控制項 分數計算不會排除任何資料。

計算控制狀態時，Security Hub CSPM 會忽略封存和隱藏的問題清單。這可能會影響安全分數。例如，如果您隱藏控制項的所有失敗調查結果，則其狀態會變成通過，進而改善您的安全分數。如需控制狀態的詳細資訊，請參閱 [評估合規狀態和控制狀態](#)。

評分範例：

標準	傳遞控制項	失敗的控制項	不明控制項	標準分數
AWS 基礎安全最佳實務 1.0.0 版	168	22	0	88%
CIS AWS Foundations Benchmark 1.4.0 版	8	29	0	22%
CIS AWS Foundations	6	35	0	15%

標準	傳遞控制項	失敗的控制項	不明控制項	標準分數
Benchmark 1.2.0 版				
NIST 特別出版物 800-53 修訂版 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

計算摘要安全分數時，Security Hub CSPM 只會跨標準計算每個控制項一次。例如，如果您已啟用套用至三個已啟用標準的控制項，則它只會計為一個已啟用的控制項，以供評分之用。

在此範例中，雖然跨已啟用標準啟用的控制項總數為 528，但 Security Hub CSPM 只會針對評分目的計算每個唯一控制項一次。唯一啟用的控制項數量可能低於 528。如果我們假設唯一啟用的控制項數目為 515，而唯一傳遞的控制項數目為 357，則摘要分數為 69%。此分數的計算方式是將唯一傳遞的控制項數量除以唯一啟用的控制項數量。

您可能有一個與標準安全分數不同的摘要分數，即使您在目前區域中只啟用了帳戶中的一個標準。如果您登入管理員帳戶，且成員帳戶已啟用其他標準或不同標準，則可能會發生這種情況。如果您從彙總區域檢視分數，並在連結區域中啟用其他標準或不同標準，也會發生這種情況。

管理員帳戶的安全分數

如果您已登入管理員帳戶，則管理員帳戶和所有成員帳戶中的控制狀態的摘要安全分數和標準分數帳戶。

如果甚至一個成員帳戶中的控制項狀態為失敗，則其在管理員帳戶中的狀態為失敗，並影響管理員帳戶分數。

如果您已登入管理員帳戶，且正在檢視彙總區域中的分數，則安全分數會考慮所有成員帳戶和所有連結區域中的控制狀態。

如果您已設定彙總區域，安全性分數

如果您已設定彙總 AWS 區域，則摘要安全分數和標準分數會考慮所有 中的控制狀態連結的區域。

如果甚至一個連結區域中的控制項狀態為失敗，則其狀態在彙總區域中為失敗，並影響彙總區域分數。

如果您已登入管理員帳戶，且正在檢視彙總區域中的分數，則安全分數會考慮所有成員帳戶和所有連結區域中的控制狀態。

Security Hub CSPM 中的控制類別

每個控制項都會指派一個類別。控制項的類別會反映控制項套用的安全性功能。

類別值包含類別、類別內的子類別，以及可選擇的子類別內的分類器。例如：

- 識別 > 庫存
- 保護 > 資料保護 > 加密傳輸中的資料

以下是可用類別、子類別和分類器的說明。

識別

發展組織理解，以管理系統、資產、資料和能力的網路安全風險。

Inventory

該服務是否實施了正確的資源標記策略？此標記策略是否包括資源擁有者？

服務使用哪些資源？這些資源是此服務已核准的資源嗎？

您是否可以查看已核准的庫存？例如，您是否使用 Amazon EC2 Systems Manager 和 Service Catalog 等服務？

日誌

您是否安全地啟用了該服務的所有相關日誌記錄？日誌檔案的範例包括下列項目：

- Amazon VPC 流程日誌
- Elastic Load Balancing 存取日誌
- Amazon CloudFront 日誌
- Amazon CloudWatch Logs
- Amazon Relational Database Service 記錄
- Amazon OpenSearch Service 慢索引日誌
- X-Ray 追蹤
- AWS Directory Service 日誌

- AWS Config 項目
- 快照

保護

制定和實施適當的保護措施，以確保提供關鍵基礎設施服務和安全編碼實務。

安全存取管理

服務是否在其 IAM 或資源政策中使用最低權限實務？

密碼和私密的複雜性是否足夠？它們是否適當輪換？

此服務是否使用多重因素認證 (MFA)？

服務是否避免根使用者？

以資源為基礎的政策是否允許公開存取？

安全網路組態

此服務是否避免公有和不安全的遠端網路存取？

此服務是否正確使用 VPC？例如，是否需要在 VPC 中執行任務？

此服務是否正確地分割並隔離敏感資源？

資料保護

靜態資料加密 – 服務是否加密靜態資料？

傳輸中的資料加密 – 服務是否會加密傳輸中的資料？

資料完整性 – 服務是否驗證資料完整性？

資料刪除保護 – 服務是否保護資料免於意外刪除？

資料管理/使用 – 您是否使用 Amazon Macie 等服務來追蹤敏感資料的位置？

API 保護

服務是否使用 AWS PrivateLink 來保護服務 API 操作？

保護服務

正確的保護服務是否已就緒？他們是否提供正確的涵蓋範圍？

保護服務可協助您擺脫針對服務的攻擊和入侵。中的保護服務範例 AWS 包括 AWS Control Tower、AWS WAF AWS Shield Advanced、Vanta、Secrets Manager、IAM Access Analyzer 和 AWS Resource Access Manager。

安全開發

您使用安全的編碼實務嗎？

您是否避免了諸如開放式 Web 應用程式安全專案 (OWASP) 前十個等漏洞？

偵測

制定和實施適當的活動，以識別網路安全事件的發生。

偵測服務

正確的偵測服務是否已就緒？

他們是否提供正確的涵蓋範圍？

AWS 偵測服務的範例包括 Amazon GuardDuty、AWS Security Hub CSPM、Amazon Inspector、Amazon Detective AWS IoT Device Defender、Amazon CloudWatch Alarms 和 AWS Trusted Advisor。

回應

制定並實施適當的活動，以針對偵測到的網路安全事件採取行動。

回應動作

您是否迅速回應安全性事件？

您是否有任何作用中的嚴重或高嚴重性問題清單？

鑑識

您可以安全地取得服務的鑑識資料嗎？例如，您是否取得與真陽性問題清單相關聯的 Amazon EBS 快照？

您是否設立一個鑑識帳戶？

復原

制定和實施適當的活動，以維持恢復計劃，並恢復因網路安全事件而受損的任何功能或服務。

恢復能力

服務組態是否支援正常容錯移轉、彈性擴展和高可用性？

您是否已建立備份？

檢閱 Security Hub CSPM 中控制項的詳細資訊

在控制項頁面或 Security Hub CSPM 主控台的標準詳細資訊頁面上選取控制項，將帶您前往控制項詳細資訊頁面。

控制項詳細資訊頁面頂端指出控制項狀態。控制項狀態會根據控制項調查結果的合規狀態，摘要說明控制項的效能。Security Hub CSPM 通常會在您第一次造訪 Security Hub CSPM 主控台的摘要頁面或安全標準頁面後 30 分鐘內產生初始控制狀態。狀態僅適用於您造訪這些頁面時啟用的控制項。

控制項詳細資訊頁面也提供過去 24 小時內控制項調查結果的合規狀態明細。如需控制狀態和合規狀態的詳細資訊，請參閱 [評估合規狀態和控制狀態](#)。

AWS Config 必須設定資源記錄，才能顯示控制項狀態。第一次產生控制狀態之後，Security Hub CSPM 會根據過去 24 小時的調查結果，每 24 小時更新一次控制狀態。

管理員帳戶會看到管理員帳戶和成員帳戶中的彙總控制狀態。如果您已設定彙總區域，控制狀態會包含所有連結區域的調查結果。如需控制狀態的詳細資訊，請參閱 [the section called “合規狀態和控制狀態”](#)。

您也可以從控制項詳細資訊頁面啟用或停用控制項。

Note

在中國區域和中啟用第一次控制狀態的控制後，最多可能需要 24 小時的時間 AWS GovCloud (US) Regions。

標準和要求索引標籤列出可以啟用控制項的標準，以及與來自不同合規架構的控制項相關的要求。

Checks 索引標籤會列出過去 24 小時內控制項的作用中問題清單。當 Security Hub CSPM 執行控制項的安全檢查時，會產生和更新控制項調查結果。此索引標籤上的清單不包含封存的問題清單。

對於每個調查結果，清單會提供調查結果詳細資訊的存取權，例如合規狀態和相關資源。您也可以設定每個調查結果的工作流程狀態，並將調查結果傳送至自訂動作。如需詳細資訊，請參閱[檢閱和管理控制問題清單](#)。

檢視控制項的詳細資訊

選擇您偏好的存取方法，然後依照下列步驟檢閱控制項的詳細資訊。詳細資訊適用於目前的帳戶和區域，並包含下列項目：

- 控制項的標題和描述。
- 失敗控制問題清單的修復指引連結。
- 控制項的嚴重性。
- 控制項的狀態。

在主控台上，您也可以檢閱控制項的最新調查結果清單。若要以程式設計方式執行此操作，您可以使用 Security Hub CSPM API [GetFindings](#) 的操作。

Security Hub CSPM console

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中選擇控制項。
3. 選取控制項。

Security Hub CSPM API

1. 執行 [ListSecurityControlDefinitions](#)，並提供一或多個標準 ARNs，以取得該標準的控制 IDs 清單。若要取得標準 ARNs，請執行 [DescribeStandards](#)。如果您未提供標準 ARN，此 API 會傳回所有 Security Hub CSPM IDs。此 API 會傳回標準無關的安全控制 IDs，而不是在這些功能版本之前存在的標準型控制 IDs。

請求範例：

```
{
  "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```


2. 執行 [BatchGetSecurityControls](#) 以取得目前 AWS 帳戶 和 中一或多個控制項的詳細資訊 AWS 區域。

請求範例：

```
{
  "SecurityControlIds": ["Config.1", "IAM.1"]
}
```

AWS CLI

1. 執行 [list-security-control-definitions](#) 命令，並提供一或多個標準 ARNs 以取得控制項 IDs 清單。若要取得標準 ARNs，請執行 `describe-standards` 命令。如果您未提供標準 ARN，此命令會傳回所有 Security Hub CSPM 控制 IDs。此命令會傳回標準無關的安全控制 IDs，而不是在這些功能版本之前存在的標準型控制 IDs。

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. 執行 [batch-get-security-controls](#) 命令以取得目前 AWS 帳戶 和 中一或多個控制項的詳細資訊 AWS 區域。

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

在 Security Hub CSPM 中篩選和排序控制項

在 AWS Security Hub CSPM 主控台上，您可以使用控制項頁面來檢閱目前 中可用的控制項資料表 AWS 區域。例外狀況是彙總區域。如果您已 [設定彙總區域](#) 並登入該區域，主控台會顯示彙總區域或一或多個連結區域中可用的控制項。

若要專注於特定的控制項子集，您可以排序和篩選控制項資料表。資料表旁的依選項篩選可協助您快速專注於這些特定子集：

- 所有啟用的控制項，都是在至少一個啟用的標準中啟用的控制項。
- 所有停用的控制項，這是在所有標準中停用的控制項。

- 具有特定控制項狀態的所有已啟用控制項，例如失敗。無資料選項只會顯示目前沒有問題清單的控制項。如需控制狀態的資訊，請參閱 [評估合規狀態和控制狀態](#)。

除了依選項篩選之外，您還可以在資料表上方的篩選條件控制方塊中輸入篩選條件來篩選資料表。例如，您可以依控制項 ID 或嚴重性進行篩選。

根據預設，狀態為失敗的控制項會依嚴重性以遞減順序列出。您可以選擇不同的欄標題來變更排序順序。

Tip

如果您有根據控制調查結果的自動化工作流程，建議您使用 `SecurityControlId` 或 `SecurityControlArn` [ASFF 欄位](#) 做為篩選條件，而非 `Title` 或 `Description` 欄位。後者欄位可能會偶爾變更，而控制項 ID 和 ARN 是靜態識別符。

如果您已登入 Security Hub CSPM 管理員帳戶，啟用的控制項包含至少一個成員帳戶中啟用的控制項。如果您已設定彙總區域，則已啟用的控制項包括在至少一個連結區域中啟用的控制項。

如果您選取已啟用控制項旁的選項，則會顯示面板，並顯示目前啟用控制項的標準。您也可以查看目前停用控制項的標準。在此面板中，您可以在所有標準中停用控制項。如需詳細資訊，請參閱 [在 Security Hub CSPM 中停用控制項](#)。對於管理員帳戶，面板中的資訊會反映所有成員帳戶的設定。

若要以程式設計方式擷取控制項清單，您可以使用 Security Hub CSPM API [ListSecurityControlDefinitions](#) 的操作。若要擷取個別控制項的詳細資訊，請使用 [BatchGetSecurityControls](#) 操作。

了解 Security Hub CSPM 中的控制參數

AWS Security Hub CSPM 中的某些控制項使用會影響控制項評估方式的參數。一般而言，這類控制項會根據 Security Hub CSPM 定義的預設參數值進行評估。不過，對於這些控制項的子集，您可以修改參數值。當您修改控制項參數值時，Security Hub CSPM 會開始針對您指定的值評估控制項。如果控制項基礎的資源滿足自訂值，Security Hub CSPM 會產生 PASSED 問題清單。如果資源不符合自訂值，Security Hub CSPM 會產生 FAILED 問題清單。

透過自訂控制參數，您可以精簡 Security Hub CSPM 建議和監控的安全最佳實務，以符合您的業務需求和安全期望。您可以自訂一個或多個參數來取得符合您安全需求的調查結果，而不是隱藏控制項的問題清單。

以下是修改控制參數和設定自訂值的一些範例使用案例：

- **【CloudWatch.16】** – CloudWatch 日誌群組應保留一段指定的時間

您可以指定保留期間。

- **【IAM.7】** – IAM 使用者的密碼政策應具有強大的組態

您可以指定與密碼強度相關的參數。

- **【EC2.18】** – 安全群組應僅允許授權連接埠不受限制的傳入流量

您可以指定授權哪些連接埠允許不受限制的傳入流量。

- **【Lambda.5】** – VPC Lambda 函數應在多個可用區域中運作

您可以指定產生傳遞調查結果的可用區域數量下限。

本節涵蓋修改控制參數時要考量的事項。

修改控制參數值的效果

當您變更參數值時，也會觸發新的安全檢查，根據新值評估控制項。然後，Security Hub CSPM 會根據新值產生新的控制調查結果。在控制問題清單的定期更新期間，Security Hub CSPM 也會使用新的參數值。如果您變更控制項的參數值，但尚未啟用包含控制項的任何標準，Security Hub CSPM 不會使用新值執行任何安全檢查。您必須為 Security Hub CSPM 啟用至少一個相關標準，才能根據新的參數值評估控制項。

控制項可以有一或多個可自訂的參數。每個控制參數的可能資料類型包括下列項目：

- Boolean
- Double
- 列舉
- EnumList
- Integer
- IntegerList
- String
- StringList

自訂參數值適用於已啟用的標準。您無法自訂目前區域中不支援之控制項的參數。如需個別控制項的區域限制清單，請參閱 [Security Hub CSPM 控制項的區域限制](#)。

對於某些控制項，可接受的參數值必須落在指定的範圍內才有效。在這些情況下，Security Hub CSPM 會提供可接受的範圍。

Security Hub CSPM 選擇預設參數值，偶爾可能會更新它們。自訂控制參數之後，其值會繼續是您為參數指定的值，除非您變更它。也就是說，即使參數的自訂值符合 Security Hub CSPM 定義的目前預設值，參數仍會停止追蹤預設 Security Hub CSPM 值的更新。以下是控制項 **【ACM.1】** 的範例 – 匯入和 ACM 發行的憑證應在指定的時段後續約：

```
{
  "SecurityControlId": "ACM.1",
  "Parameters": {
    "daysToExpiration": {
      "ValueType": "CUSTOM",
      "Value": {
        "Integer": 30
      }
    }
  }
}
```

在上述範例中，daysToExpiration 參數的自訂值為 30。此參數目前的預設值也是 30。如果 Security Hub CSPM 將預設值變更為 14，則此範例中的參數不會追蹤該變更。它將保留的值 30。

如果您想要追蹤參數的預設 Security Hub CSPM 值的更新，請將 ValueType 欄位設定為 `DEFAULT` 而不是 `CUSTOM`。如需詳細資訊，請參閱[還原至單一帳戶和區域中的預設控制參數](#)。

支援自訂參數的控制項

如需支援自訂參數的安全控制清單，請參閱 Security Hub CSPM 主控台的控制頁面或 [Security Hub CSPM 的控制項參考](#)。若要以程式設計方式擷取此清單，您可以使用 [ListSecurityControlDefinitions](#) 操作。在回應中，CustomizableProperties 物件會指出哪些控制項支援可自訂的參數。

檢閱目前的控制項參數值

修改控制參數之前，了解控制參數的目前值會很有幫助。

您可以檢閱帳戶中個別控制參數的目前值。如果您使用中央組態，委派的 AWS Security Hub CSPM 管理員也可以檢閱組態政策中指定的參數值。

選擇您偏好的方法，然後依照步驟檢閱目前的控制參數值。

Security Hub CSPM console

若要檢閱目前的控制參數值（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇控制項。選擇控制項。
3. 選擇參數索引標籤。此標籤顯示控制項目前的參數值。

Security Hub CSPM API

若要檢閱目前的控制參數值 (API)

叫用 [BatchGetSecurityControls](#) API，並提供一或多個安全控制 IDs 或 ARNs。回應中的 `Parameters` 物件會顯示指定控制項的目前參數值。

例如，下列 AWS CLI 命令會顯示 `APIGateway.1`、`CloudWatch.15` 和 `IAM.7` 的目前參數值。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

選擇您偏好的方法，以檢視中央組態政策中的目前參數值。

Security Hub CSPM console

若要檢閱組態政策中的目前控制參數值（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用主要區域中委派 Security Hub CSPM 管理員帳戶的憑證登入。

2. 在導覽窗格中，選擇設定和組態。
3. 在政策索引標籤上，選取組態政策，然後選擇檢視詳細資訊。政策詳細資訊隨即出現，包括目前的參數值。

Security Hub CSPM API

若要檢閱組態政策 (API) 中的目前控制參數值

1. 從主要區域中的委派管理員帳戶叫用 [GetConfigurationPolicy](#) API。
2. 提供您要查看其詳細資訊之組態政策的 ARN 或 ID。回應包含目前的參數值。

例如，下列 AWS CLI 命令會在指定的組態政策中擷取目前的控制參數值。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

控制調查結果也包含控制參數的目前值。在 [AWS 安全調查結果格式 \(ASFF\)](#) 中，這些值會出現在 Compliance 物件的 Parameters 欄位中。若要檢閱 Security Hub CSPM 主控台上的問題清單，請在導覽窗格中選擇問題清單。若要以程式設計方式檢閱問題清單，請使用 Security Hub CSPM API [GetFindings](#) 的操作。

自訂控制參數值

自訂控制參數的指示會根據您是否在 AWS Security Hub CSPM 中使用 [中央組態](#) 而有所不同。中央組態是一項功能，委派的 Security Hub CSPM 管理員可用來設定跨 AWS 區域帳戶和組織單位 (OUs) 的 Security Hub CSPM 功能。

如果您的組織使用中央組態，委派管理員可以建立包含自訂控制參數的組態政策。這些政策可以與集中管理的成員帳戶和 OUs 相關聯，它們在您的主要區域和所有連結區域中生效。委派管理員也可以將一或多個帳戶指定為自我管理，讓帳戶擁有者在每個區域中分別設定自己的參數。如果您的組織不使用中央組態，您必須在每個帳戶和區域中分別自訂控制參數。

我們建議您使用中央組態，因為它可讓您跨組織的不同部分調整控制參數值。例如，所有測試帳戶可能會使用特定參數值，而所有生產帳戶可能會使用不同的值。

在多個帳戶和區域中自訂控制參數

如果您是使用中央組態之組織的委派 Security Hub CSPM 管理員，請選擇您偏好的方法，然後依照步驟自訂跨多個帳戶和區域的控制參數。

Security Hub CSPM console

在多個帳戶和區域中自訂控制參數值（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

確保您已登入主區域。

2. 在導覽窗格中，選擇設定和組態。
3. 選擇 Policies (政策) 標籤。
4. 若要建立新的包含自訂參數的組態政策，請選擇建立政策。若要在現有組態政策中指定自訂參數，請選取政策，然後選擇編輯。

使用自訂控制參數值建立新的組態政策

1. 在自訂政策區段中，選擇您要啟用的安全標準和控制項。
2. 選取自訂控制參數。
3. 選取控制項，然後指定一或多個參數的自訂值。
4. 若要自訂更多控制項的參數，請選擇自訂其他控制項。
5. 在帳戶區段中，選取要套用政策的帳戶或 OUs。
6. 選擇下一步。
7. 選擇建立政策並套用。在您的主要區域和所有連結區域中，此動作會覆寫與此組態政策相關聯的帳戶和 OUs 的現有組態設定。帳戶和 OUs 可以透過直接應用程式或從父系繼承來與組態政策建立關聯。

在現有組態政策中自訂控制參數值

1. 在控制項區段的自訂政策下，指定您想要的新自訂參數值。
2. 如果這是您第一次在此政策中自訂控制參數，請選取自訂控制參數，然後選取要自訂的控制項。若要自訂更多控制項的參數，請選擇自訂其他控制項。
3. 在帳戶區段中，驗證您要套用政策的帳戶或 OUs。
4. 選擇下一步。
5. 檢閱您的變更，並確認其正確無誤。完成後，請選擇儲存政策並套用。在您的主要區域和所有連結區域中，此動作會覆寫與此組態政策相關聯的帳戶和 OUs 的現有組態設定。帳戶和 OUs 可以透過直接應用程式或從父系繼承來與組態政策建立關聯。

Security Hub CSPM API

在多個帳戶和區域中自訂控制參數值 (API)

使用自訂控制參數值建立新的組態政策

1. 從主要區域中的委派管理員帳戶叫用 [CreateConfigurationPolicy](#) API。
2. 針對 SecurityControlCustomParameters 物件，提供您要自訂之每個控制項的識別符。
3. 針對 Parameters 物件，提供您要自訂的每個參數的名稱。針對您自訂的每個參數，提供 CUSTOM 給 ValueType。對於 Value，請提供 參數的資料類型和自訂值。當 ValueType 為時，Value 欄位不可為空白CUSTOM。如果您的請求省略 控制項支援的參數，則該參數會保留其目前值。您可以透過叫用 [GetSecurityControlDefinition](#) API 來尋找控制項支援的參數、資料類型和有效值。

在現有組態政策中自訂控制參數值

1. 從主要區域中的委派管理員帳戶叫用 [UpdateConfigurationPolicy](#) API。
2. 針對 Identifier 欄位，提供您要更新的組態政策的 Amazon Resource Name (ARN) 或 ID。
3. 針對 SecurityControlCustomParameters 物件，提供您要自訂之每個控制項的識別符。
4. 針對 Parameters 物件，提供您要自訂的每個參數的名稱。針對您自訂的每個參數，提供 CUSTOM 給 ValueType。對於 Value，請提供 參數的資料類型和自訂值。如果您的請求省略 控制項支援的參數，則該參數會保留其目前值。您可以叫用 [GetSecurityControlDefinition](#) API 來尋找控制項支援的參數、資料類型和有效值。

例如，下列 AWS CLI 命令會為 daysToExpiration 參數建立具有自訂值的新組態政策 ACM.1。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
  "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0","arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
```



```
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters": [{"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}]}]}
```

在單一帳戶和區域中自訂控制參數

如果您不使用中央組態或擁有自我管理帳戶，您一次只能在一個區域中自訂帳戶的控制參數。

選擇您偏好的方法，然後依照步驟自訂控制參數。您的變更僅適用於目前區域中的帳戶。若要在其他區域中自訂控制參數，請在您要自訂參數的每個其他帳戶和區域中重複下列步驟。相同的控制項可以在不同的區域中使用不同的參數值。

Security Hub CSPM console

在一個帳戶和區域中自訂控制參數值（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇控制項。在表格中，選擇支援自訂參數且您想要變更參數的控制項。自訂參數欄指出哪些控制項支援自訂參數。
3. 在控制項的詳細資訊頁面上，選擇參數索引標籤，然後選擇編輯。
4. 指定您想要的參數值。
5. 或者，在變更原因區段中，選取自訂參數的原因。
6. 選擇儲存。

Security Hub CSPM API

在一個帳戶和區域中自訂控制參數值 (API)

1. 叫用 [UpdateSecurityControl](#) API。
2. 針對 SecurityControlId，提供您要自訂之控制項的 ID。
3. 針對 Parameters 物件，提供您要自訂的每個參數的名稱。針對您自訂的每個參數，提供 CUSTOM 給 ValueType。對於 Value，請提供參數的資料類型和自訂值。如果您的請求省略控制項支援的參數，則該參數會保留其目前值。您可以透過叫用 [GetSecurityControlDefinition](#) API 來尋找控制項支援的參數、資料類型和有效值。
4. 或者，對於 LastUpdateReason，提供自訂控制參數的原因。

例如，下列 AWS CLI 命令會定義 `daysToExpiration` 參數的自訂值 `ACM.1`。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub update-security-control \  
--region us-east-1 \  
--security-control-id ACM.1 \  
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":  
15}}}' \  
--last-update-reason "Internal compliance requirement"
```

還原至預設控制參數值

控制參數可以具有 AWS Security Hub CSPM 定義的預設值。有時，Security Hub CSPM 會更新參數的預設值，以反映不斷變化的安全最佳實務。如果您尚未指定控制項參數的自訂值，控制項會自動追蹤這些更新，並使用新的預設值。

您可以還原為使用控制項的預設參數值。還原的指示取決於您是否在 Security Hub CSPM 中使用 [中央組態](#)。中央組態是一項功能，委派的 Security Hub CSPM 管理員可用來設定跨 AWS 區域帳戶和組織單位 (OUs) 的 Security Hub CSPM 功能。

Note

並非所有控制參數都有預設的 Security Hub CSPM 值。在這種情況下，當 `ValueType` 設為 `DEFAULT`，Security Hub CSPM 不會使用特定的預設值。相反地，如果沒有自訂值，Security Hub CSPM 會忽略參數。

在多個帳戶和區域中還原為預設控制參數

如果您使用中央組態，則可以還原主區域和連結區域中多個集中受管帳戶和 OUs 的控制參數。

選擇您偏好的方法，然後依照步驟，使用中央組態在多個帳戶和區域中還原為預設參數值。

Security Hub CSPM console

在多個帳戶和區域中還原為預設控制參數值（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。

使用主要區域中委派 Security Hub CSPM 管理員帳戶的憑證登入。

2. 在導覽窗格中，選擇設定和組態。
3. 選擇 Policies (政策) 標籤。
4. 選取政策，然後選擇編輯。
5. 在自訂政策下，控制項區段會顯示您指定自訂參數的控制項清單。
6. 尋找具有一或多個參數值要還原的控制項。然後，選擇移除以還原為預設值。
7. 在帳戶區段中，驗證您要套用政策的帳戶或 OUs。
8. 選擇下一步。
9. 檢閱您的變更，並確認其正確無誤。完成後，請選擇儲存政策並套用。在您的主要區域和所有連結區域中，此動作會覆寫與此組態政策相關聯的帳戶和 OUs 的現有組態設定。帳戶和 OUs 可以透過直接應用程式或從父系繼承來與組態政策建立關聯。

Security Hub CSPM API

還原至多個帳戶和區域中的預設控制參數值 (API)

1. 從主要區域中的委派管理員帳戶叫用 [UpdateConfigurationPolicy](#) API。
2. 針對 Identifier 欄位，提供您要更新之政策的 Amazon Resource Name (ARN) 或 ID。
3. 針對 SecurityControlCustomParameters 物件，提供您要還原一或多個參數之每個控制項的識別符。
4. 在 Parameters 物件中，針對您要還原的每個參數，DEFAULT 為 ValueType 欄位提供。當 ValueType 設為 時 DEFAULT，您不需要為 Value 欄位提供值。如果您的請求中包含值，Security Hub CSPM 會忽略該值。如果您的請求省略 控制項支援的參數，則該參數會保留其目前值。

Warning

如果您省略 SecurityControlCustomParameters 欄位的控制項物件，Security Hub CSPM 會將控制項的所有自訂參數還原為其預設值。的完全空白清單會將所有控制項的自訂參數 SecurityControlCustomParameters 還原為其預設值。

例如，下列 AWS CLI 命令會將的 `daysToExpiration` 控制參數還原 ACM.1 為指定組態政策中的預設值。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
  "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0","arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
  "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "DEFAULT"}}]}}}'
```

還原至單一帳戶和區域中的預設控制參數

如果您不使用中央組態或擁有自我管理帳戶，您可以一次還原為在一個區域中使用帳戶的預設參數值。

選擇您偏好的方法，然後依照步驟還原為單一區域中您帳戶的預設參數值。若要在其他區域中還原為預設參數值，請在每個其他區域中重複這些步驟。

Note

如果您停用 Security Hub CSPM，則會重設您的自訂控制參數。如果您未來再次啟用 Security Hub CSPM，所有控制項都會使用預設參數值來啟動。

Security Hub CSPM console

還原至一個帳戶和區域中的預設控制參數值（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇控制項。選擇您要還原為預設參數值的控制項。

3. 在 Parameters 索引標籤上，選擇控制項參數旁的自訂。然後，選擇移除自訂。此參數現在使用預設 Security Hub CSPM 值，並追蹤預設值的未來更新。
4. 針對您要還原的每個參數值，重複上述步驟。

Security Hub CSPM API

還原至一個帳戶和區域中的預設控制參數值 (API)

1. 叫用 [UpdateSecurityControl](#) API。
2. 針對 SecurityControlId，提供您要還原其參數之控制項的 ARN 或 ID。
3. 在 Parameters 物件中，針對您要還原的每個參數，DEFAULT 為 ValueType 欄位提供。當 ValueType 設為 時 DEFAULT，您不需要為 Value 欄位提供值。如果您的請求中包含值，Security Hub CSPM 會忽略該值。
4. 或者，對於 LastUpdateReason，提供還原為預設參數值的原因。

例如，下列 AWS CLI 命令會將的 daysToExpiration 控制參數還原 ACM.1 為其預設值。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

檢查控制參數變更的狀態

當您嘗試自訂控制參數或還原為預設值時，您可以驗證所需的變更是否有效。這有助於確保控制項如您預期般運作，並提供預期的安全值。如果參數更新失敗，Security Hub CSPM 會保留 參數的目前值。

若要驗證參數更新是否成功，您可以在 Security Hub CSPM 主控台上檢閱控制項的詳細資訊。在 主控台上，選擇導覽窗格中的控制項。然後，選擇控制項以顯示其詳細資訊。參數索引標籤會顯示參數變更的狀態。

以程式設計方式，如果您更新參數的請求有效，UpdateStatus 欄位的值會 UPDATING 回應 [BatchGetSecurityControls](#) 操作。這表示更新有效，但所有調查結果可能尚未包含更新的參數值。當 的

值UpdateState變更為 時READY，Security Hub CSPM 會在執行控制項的安全檢查時使用更新的控制項參數值。調查結果包含更新的參數值。

UpdateSecurityControl 操作會傳回無效參數值的InvalidInputException回應。回應提供失敗原因的其他詳細資訊。例如，您可能已指定超出參數有效範圍的值。或者，您可能已指定未使用正確資料類型的值。使用有效的輸入再次提交您的請求。

如果您嘗試更新參數值時發生內部故障，則如果您 AWS Config 已啟用，Security Hub CSPM 會自動重試。如需詳細資訊，請參閱[啟用和設定 之前的考量事項 AWS Config](#)。

在 Security Hub CSPM 中檢閱和管理控制問題清單

控制項詳細資訊頁面會顯示控制項的作用中問題清單。清單不包含封存的問題清單。

控制項詳細資訊頁面支援跨區域彙總。如果您已設定彙總區域，控制詳細資訊頁面上的控制項狀態和安全檢查清單會包含所有連結的檢查 AWS 區域。

此清單提供工具來篩選和排序問題清單，讓您可以先專注於更緊急的問題清單。問題清單可能包含相關服務主控台中資源詳細資訊的連結。對於以 AWS Config 規則為基礎的控制項，您可以檢視規則的詳細資訊。

您也可以使用 AWS Security Hub CSPM API 來擷取問題清單和問題清單詳細資訊。

如需詳細資訊，請參閱[檢閱問題清單詳細資訊和歷史記錄](#)。

若要反映控制項調查結果調查的目前狀態，您可以設定工作流程狀態。如需詳細資訊，請參閱[the section called “設定問題清單的工作流程狀態”](#)。

您也可以將選取的 Security Hub CSPM 調查結果傳送至 Amazon EventBridge 中的自訂動作。如需詳細資訊，請參閱[the section called “將問題清單傳送至自訂動作”](#)。

主題

- [篩選和排序控制項問題清單](#)
- [控制問題清單的範例](#)

篩選和排序控制項問題清單

從 AWS Security Hub CSPM 主控台的控制項頁面或從標準的詳細資訊頁面選取控制項，將帶您前往控制項詳細資訊頁面。

控制項詳細資訊頁面會顯示控制項的標題和描述、整體控制項狀態，以及過去 24 小時內控制項的安全檢查明細。

使用控制項檢查清單旁的依選項篩選，快速專注於具有特定[工作流程狀態](#)或[合規狀態](#)的問題清單。

除了依選項篩選之外，您還可以使用新增篩選條件方塊，依其他欄位篩選檢查清單，例如 AWS 帳戶 ID 或資源 ID。

根據預設，合規狀態為 PASSED 的問題清單會先列出。您可以在資料欄標頭中選擇不同的選項，以變更預設排序。

從控制項詳細資訊頁面，您可以選擇下載，將目前的控制項問題清單頁面下載至 .csv 檔案。

如果您篩選調查結果清單，則下載只會包含符合篩選條件的控制項。如果您從清單中選取特定問題清單，則下載只會包含選取的問題清單。

如需篩選問題清單的詳細資訊，請參閱 [在 Security Hub CSPM 中篩選問題清單](#)。

控制問題清單的範例

下列範例提供 AWS 安全調查結果格式 (ASFF) 中 AWS Security Hub CSPM 控制調查結果的範例。控制調查結果的內容會因您是否啟用合併控制調查結果而有所不同。

如果您啟用合併的控制項調查結果，即使控制項適用於多個啟用的標準，Security Hub CSPM 也會為控制項產生單一調查結果。如果您未啟用此功能，Security Hub CSPM 會為每個控制項套用的已啟用標準產生單獨的控制項調查結果。例如，如果您啟用兩個標準，且控制項同時套用到這兩個標準，您會收到兩個單獨的控制項調查結果，每個標準各一個。如果您啟用合併的控制項問題清單，則只會收到一個控制項的問題清單。如需詳細資訊，請參閱[合併的控制問題清單](#)。

本頁面上的範例提供兩種案例的範例。這些範例包括：停用合併控制調查結果時控制個別 Security Hub CSPM 標準的調查結果，以及啟用合併控制調查結果時控制多個 Security Hub CSPM 標準的調查結果。

控制問題清單的範例

- [AWS 基礎安全最佳實務標準的範例調查結果](#)
- [CIS AWS Foundations Benchmark v5.0.0 的問題清單範例](#)
- [CIS AWS Foundations Benchmark v3.0.0 的問題清單範例](#)
- [CIS AWS Foundations Benchmark 1.4.0 版的範例調查結果](#)
- [CIS AWS Foundations Benchmark 1.2.0 版的範例調查結果](#)
- [NIST SP 800-53 修訂版 5 標準的範例調查結果](#)

- [NIST SP 800-171 修訂版 2 標準的範例調查結果](#)
- [支付卡產業資料安全標準 v3.2.1 的範例調查結果](#)
- [AWS 資源標記標準的範例問題清單](#)
- [AWS Control Tower 服務受管標準的範例調查結果](#)
- [多個標準的範例合併調查結果](#)

Note

控制調查結果參考中國區域和 AWS GovCloud (US) 區域中的不同欄位和值。如需詳細資訊，請參閱[整合對 ASFF 欄位和值的影響](#)。

AWS 基礎安全最佳實務標準的範例調查結果

下列範例提供適用於 AWS 基礎安全最佳實務 (FSBP) 標準之控制項的問題清單範例。在此範例中，會停用合併控制問題清單。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
```



```

    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],

```

```

"Compliance": {
  "Status": "FAILED",
  "SecurityControlId": "CloudTrail.2",
  "AssociatedStandards": [{
    "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
  }]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-Foundational-Security-Best-Practices"
  ]
}
}

```

CIS AWS Foundations Benchmark v5.0.0 的問題清單範例

下列範例提供適用於 CIS AWS Foundations Benchmark v5.0.0 之控制項的問題清單範例。在此範例中，會停用合併控制問題清單。

```

{
  "AwsAccountId": "123456789012",
  "CompanyName": "AWS",
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.7",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v5.0.0/5.1.1"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/5.0.0"
      }
    ]
  }
}

```

```

    },
    "CreatedAt": "2025-10-10T17:04:00.952Z",
    "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
at EBS volume creation is supported.",
    "FindingProviderFields": {
        "Types": [
            "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
        ],
        "Severity": {
            "Normalized": 40,
            "Label": "MEDIUM",
            "Product": 40,
            "Original": "MEDIUM"
        }
    },
    "FirstObservedAt": "2025-10-10T17:03:57.895Z",
    "GeneratorId": "cis-aws-foundations-benchmark/v/5.0.0/5.1.1",
    "Id": "arn:aws:securityhub:us-west-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/5.0.0/5.1.1/finding/443a9d3f-8a59-4fa0-8e2c-EXAMPLE111",
    "LastObservedAt": "2025-10-14T05:22:28.667Z",
    "ProcessedAt": "2025-10-14T05:22:50.099Z",
    "ProductArn": "arn:aws:securityhub:us-west-1::product/aws/securityhub",
    "ProductFields": {
        "StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/
v/5.0.0",
        "StandardsSubscriptionArn": "arn:aws:securityhub:us-
west-1:123456789012:subscription/cis-aws-foundations-benchmark/v/5.0.0",
        "ControlId": "5.1.1",
        "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
        "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2a99554f",
        "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
        "StandardsControlArn": "arn:aws:securityhub:us-west-1:123456789012:control/cis-aws-
foundations-benchmark/v/5.0.0/5.1.1",
        "aws/securityhub/ProductName": "Security Hub CSPM",
        "aws/securityhub/CompanyName": "AWS",
        "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
        "Resources:0/Id": "arn:aws:iam::123456789012:root",
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-1::product/aws/
securityhub/arn:aws:securityhub:us-west-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/5.0.0/5.1.1/finding/443a9d3f-8a59-4fa0-8e2c-EXAMPLE111",
        "PreviousComplianceStatus": "FAILED"
    }
}

```

```

},
"ProductName": "Security Hub CSPM",
"RecordState": "ACTIVE",
"Region": "us-west-1",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS Security
Hub controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
  }
},
"Resources": [
  {
    "Id": "AWS:::Account:123456789012",
    "Partition": "aws",
    "Region": "us-west-1",
    "Type": "AwsAccount"
  }
],
"SchemaVersion": "2018-10-08",
"Severity": {
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM",
  "Product": 40
},
"Title": "5.1.1 EBS default encryption should be enabled",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
],
"UpdatedAt": "2025-10-14T05:22:38.671Z",
"Workflow": {
  "Status": "NEW"
},
"WorkflowState": "NEW"
}

```

CIS AWS Foundations Benchmark v3.0.0 的問題清單範例

下列範例提供適用於 CIS AWS Foundations Benchmark v3.0.0 之控制項的問題清單範例。在此範例中，會停用合併控制問題清單。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
  }
}
```

```

    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS:::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    }
  },
  "Types": [

```

```

    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
    Foundations Benchmark"
  ],
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}

```

CIS AWS Foundations Benchmark 1.4.0 版的範例調查結果

下列範例提供適用於 CIS AWS Foundations Benchmark v1.4.0 之控制項的問題清單範例。在此範例中，會停用合併控制問題清單。

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
  benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
    Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrail is a web service that records AWS API calls for an
  account and makes those logs available to users and resources in accordance with IAM
  policies. AWS Key Management Service (KMS) is a managed service that helps create
  and control the encryption keys used to encrypt account data, and uses Hardware
  Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
  can be configured to leverage server side encryption (SSE) and AWS KMS customer

```

```

created master keys (CMK) to further protect CloudTrail logs. It is recommended that
CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.4.0/3.7"
    ]
  },

```



```

    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
    ]
  }
}

```

CIS AWS Foundations Benchmark 1.2.0 版的範例調查結果

下列範例提供適用於 CIS AWS Foundations Benchmark v1.2.0 之控制項的問題清單範例。在此範例中，會停用合併控制問題清單。

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",

```

```

    "LastObservedAt": "2021-09-28T16:10:05.350Z",
    "CreatedAt": "2020-08-29T04:10:06.337Z",
    "UpdatedAt": "2021-09-28T16:10:00.087Z",
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
      "Original": "MEDIUM"
    },
    "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
    "Description": "AWS Key Management Service (KMS) is a managed service that helps create and control the encryption keys used to encrypt account data, and uses Hardware Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs can be configured to leverage server side encryption (SSE) and KMS customer created master keys (CMK) to further protect CloudTrail logs. It is recommended that CloudTrail be configured to use SSE-KMS.",
    "Remediation": {
      "Recommendation": {
        "Text": "For directions on how to correct this issue, consult the AWS Security Hub CSPM controls documentation.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
      }
    },
    "ProductFields": {
      "StandardsGuideArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0",
      "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
      "RuleId": "2.7",
      "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
      "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-fe95bf3f",
      "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
      "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-foundations-benchmark/v/1.2.0/2.7",
      "aws/securityhub/ProductName": "Security Hub CSPM",
      "aws/securityhub/CompanyName": "AWS",
      "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-EDIT",
      "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
  },

```

```

"Resources": [
  {
    "Type": "AwsCloudTrailTrail",
    "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-D0-N0T-
EDIT",
    "Partition": "aws",
    "Region": "us-east-2"
  }
],
"Compliance": {
  "Status": "FAILED",
  "SecurityControlId": "CloudTrail.2",
  "AssociatedStandards": [{
    "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
  }]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
  ]
}
}

```

NIST SP 800-53 修訂版 5 標準的範例調查結果

下列範例提供適用於 NIST SP 800-53 修訂版 5 標準之控制項的問題清單範例。在此範例中，會停用合併控制問題清單。

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",

```

```

"ProductName": "Security Hub CSPM",
"CompanyName": "AWS",
"Region": "us-east-1",
"GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
"AwsAccountId": "123456789012",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards"
],
"FirstObservedAt": "2023-02-17T14:22:46.726Z",
"LastObservedAt": "2023-02-17T14:22:50.846Z",
"CreatedAt": "2023-02-17T14:22:46.726Z",
"UpdatedAt": "2023-02-17T14:22:46.726Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
"Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
"Remediation": {
  "Recommendation": {
    "Text": "For directions on how to fix this issue, consult the AWS Security Hub CSPM NIST 800-53 R5 documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/nist-800-53/v/5.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0",
  "ControlId": "CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-fe95bf3f",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub CSPM",
  "aws/securityhub/CompanyName": "AWS",

```

```

    "Resources/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "NIST.800-53.r5 AU-9",
      "NIST.800-53.r5 CA-9(1)",
      "NIST.800-53.r5 CM-3(6)",
      "NIST.800-53.r5 SC-13",
      "NIST.800-53.r5 SC-28",
      "NIST.800-53.r5 SC-28(1)",
      "NIST.800-53.r5 SC-7(10)",
      "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {

```

```

    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ]
},
"ProcessedAt": "2023-02-17T14:22:53.572Z"
}

```

NIST SP 800-171 修訂版 2 標準的範例調查結果

下列範例提供適用於 NIST SP 800-171 修訂版 2 標準之控制項的問題清單範例。在此範例中，會停用合併控制問題清單。

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-171/v/2.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "AwsAccountName": "TestAcct",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2025-05-29T05:23:58.690Z",
  "LastObservedAt": "2025-05-30T05:50:11.898Z",
  "CreatedAt": "2025-05-29T05:24:24.772Z",
  "UpdatedAt": "2025-05-30T05:50:34.292Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
}

```

```

"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS Security
Hub CSPM controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/nist-800-171/v/2.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-171/v/2.0.0",
  "ControlId": "CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-0ab1c2d4",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/
nist-800-171/v/2.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/
v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
  {
    "Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
    "Partition": "aws",
    "Region": "us-east-1",
    "Type": "AwsCloudTrailTrail"
  }
],
"Compliance": {
  "Status": "FAILED",
  "SecurityControlId": "CloudTrail.2",
  "RelatedRequirements": [
    "NIST.800-171.r2/3.3.8"
  ],
  "AssociatedStandards": [
    {

```

```

        "StandardsId": "standards/nist-800-171/v/2.0.0"
    }
]
},
"Workflow": {
    "Status": "NEW"
},
"WorkflowState": "NEW",
"RecordState": "ACTIVE",
"FindingProviderFields": {
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
        "Product": 40,
        "Label": "MEDIUM",
        "Normalized": 40,
        "Original": "MEDIUM"
    }
},
"ProcessedAt": "2025-05-30T05:50:40.297Z"
}

```

支付卡產業資料安全標準 v3.2.1 的範例調查結果

下列範例提供適用於支付卡產業資料安全標準 (PCI DSS) v3.2.1 的控制項調查結果範例。在此範例中，會停用合併控制問題清單。

```

{
    "SchemaVersion": "2018-10-08",
    "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
    "ProductName": "Security Hub CSPM",
    "CompanyName": "AWS",
    "Region": "us-east-2",
    "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
    "AwsAccountId": "123456789012",
    "Types": [
        "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ],
    "FirstObservedAt": "2020-08-06T02:18:23.089Z",
    "LastObservedAt": "2021-09-28T16:10:06.942Z",
}

```



```

"CreatedAt": "2020-08-06T02:18:23.089Z",
"UpdatedAt": "2021-09-28T16:10:00.090Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS
CMKs",
"Description": "This AWS control checks whether AWS CloudTrail is configured to use
the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
key (CMK) encryption by checking if the KmsKeyId is defined.",
"Remediation": {
  "Recommendation": {
    "Text": "For directions on how to correct this issue, consult the AWS Security
Hub CSPM controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/pci-dss/v/3.2.1",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
  "ControlId": "PCI.CloudTrail.1",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
  "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
  "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
  "aws/securityhub/ProductName": "Security Hub CSPM",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
  {
    "Type": "AwsCloudTrailTrail",

```

```

    "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-D0-NOT-
EDIT",
    "Partition": "aws",
    "Region": "us-east-2"
  }
],
"Compliance": {
  "Status": "FAILED",
  "RelatedRequirements": [
    "PCI DSS 3.4"
  ],
  "SecurityControlId": "CloudTrail.2",
  "AssociatedStandards": [{
    "StandardsId": "standards/pci-dss/v/3.2.1"
  }]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ]
}
}

```

AWS 資源標記標準的範例問題清單

下列範例提供適用於 AWS 資源標記標準之控制項的問題清單範例。在此範例中，會停用合併控制問題清單。

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",

```

```

"CompanyName": "AWS",
"Region": "eu-central-1",
"GeneratorId": "security-control/EC2.44",
"AwsAccountId": "123456789012",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards"
],
"FirstObservedAt": "2024-02-19T21:00:32.206Z",
"LastObservedAt": "2024-04-29T13:01:57.861Z",
"CreatedAt": "2024-02-19T21:00:32.206Z",
"UpdatedAt": "2024-04-29T13:01:41.242Z",
"Severity": {
  "Label": "LOW",
  "Normalized": 1,
  "Original": "LOW"
},
"Title": "EC2 subnets should be tagged",
"Description": "This control checks whether an Amazon EC2 subnet has tags with the
specific keys defined in the parameter requiredTagKeys. The control fails if the
subnet doesn't have any tag keys or if it doesn't have all the keys specified in
the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
control only checks for the existence of a tag key and fails if the subnet isn't
tagged with any key. System tags, which are automatically applied and begin with aws:,
are ignored.",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS Security
Hub CSPM controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
  }
},
"ProductFields": {
  "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "aws/securityhub/ProductName": "Security Hub CSPM",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/annotation": "No tags are present.",
  "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [

```

```

{
  "Type": "AwsEc2Subnet",
  "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
    "AwsEc2Subnet": {
      "AssignIpv6AddressOnCreation": false,
      "AvailabilityZone": "eu-central-1b",
      "AvailabilityZoneId": "euc1-az3",
      "AvailableIpAddressCount": 4091,
      "CidrBlock": "10.24.34.0/23",
      "DefaultForAz": true,
      "MapPublicIpOnLaunch": true,
      "OwnerId": "123456789012",
      "State": "available",
      "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
      "SubnetId": "subnet-1234567890abcdef0",
      "VpcId": "vpc-021345abcdef6789"
    }
  }
},
{
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ]
  },
  "SecurityControlParameters": [
    {
      "Name": "requiredTagKeys",
      "Value": [
        "peepoo"
      ]
    }
  ]
},
{
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  }
}

```

```

},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "LOW",
    "Original": "LOW"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ]
},
"ProcessedAt": "2024-04-29T13:02:03.259Z"
}

```

AWS Control Tower 服務受管標準的範例調查結果

下列範例提供適用於 AWS Control Tower 服務受管標準之控制項的問題清單範例。在此範例中，會停用合併控制問題清單。

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",

```

```

"Description": "This AWS control checks whether AWS CloudTrail is configured to use
the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS Security
Hub CSPM controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/service-managed-aws-control-tower/
v/1.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
  "ControlId": "CT.CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub CSPM",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
  {
    "Type": "AwsAccount",
    "Id": "AWS:::Account:123456789012",
    "Partition": "aws",
    "Region": "us-east-1"
  }
],
"Compliance": {
  "Status": "FAILED",
  "SecurityControlId": "CloudTrail.2",
  "AssociatedStandards": [{
    "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
  }
]

```

```

    ]]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}

```

多個標準的範例合併調查結果

下列範例提供適用於多個已啟用標準之控制項的調查結果範例。在此範例中，會啟用合併控制問題清單。

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-08-09T14:57:04.521Z",
  "LastObservedAt": "2025-05-30T03:30:17.407Z",
  "CreatedAt": "2024-08-09T14:57:04.521Z",
  "UpdatedAt": "2025-05-30T03:30:32.781Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,

```

```

    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security Hub CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-01a2b345",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-D0-NOT-DELETE",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-D0-NOT-DELETE",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "AwsCloudTrailTrail": {
          "HasCustomEventSelectors": false,
          "IncludeGlobalServiceEvents": true,
          "LogFileValidationEnabled": true,
          "HomeRegion": "us-east-1",
          "IsMultiRegionTrail": true,
          "S3BucketName": "cloudtrail-awslogs-do-not-delete",
          "IsOrganizationTrail": false,
          "Name": "TestTrail-D0-NOT-DELETE"
        }
      }
    }
  ]
}

```



```

],
"Compliance": {
  "Status": "FAILED",
  "SecurityControlId": "CloudTrail.2",
  "RelatedRequirements": [
    "CIS AWS Foundations Benchmark v1.2.0/2.7",
    "CIS AWS Foundations Benchmark v1.4.0/3.7",
    "CIS AWS Foundations Benchmark v3.0.0/3.5",
    "NIST.800-171.r2/3.3.8",
    "PCI DSS v3.2.1/3.4",
    "PCI DSS v4.0.1/10.3.2"
  ],
  "AssociatedStandards": [
    { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
    { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
    { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
    { "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"},
    { "StandardsId": "standards/nist-800-171/v/2.0.0"},
    { "StandardsId": "standards/pci-dss/v/3.2.1"},
    { "StandardsId": "standards/pci-dss/v/4.0.1"}
  ]
},
"Workflow": {
  "Status": "NEW"
},
"WorkflowState": "NEW",
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "Severity": {
    "Normalized": 40,
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  }
},
"ProcessedAt": "2025-05-30T03:31:00.831Z"
}

```

了解 Security Hub CSPM 中的整合

AWS Security Hub CSPM 可以從數個 AWS 服務 和支援的第三方安全解決方案中擷取 AWS Partner Network 安全調查結果。這些整合可協助您全面了解整個 AWS 環境的安全性和合規性。Security Hub CSPM 從整合的解決方案擷取問題清單，並將其轉換為 AWS 安全問題清單格式 (ASFF)。

Important

對於支援的 AWS 和第三方產品整合，Security Hub CSPM 會接收並合併僅在您為 啟用 Security Hub CSPM 之後產生的調查結果 AWS 帳戶。此服務不會追溯性地接收和合併在您啟用 Security Hub CSPM 之前產生的安全調查結果。

Security Hub CSPM 主控台的整合頁面可讓您存取可用的 AWS 和第三方產品整合。Security Hub CSPM API 也有管理整合的操作。

整合可能無法全部使用 AWS 區域。如果您目前在 Security Hub CSPM 主控台登入的區域中不支援整合，則不會出現在主控台的整合頁面上。如需中國區域可用的整合清單 AWS GovCloud (US) Regions，請參閱 [依區域的整合可用性](#)。

除了 AWS 服務 和內建的第三方整合之外，您還可以將自訂安全產品與 Security Hub CSPM 整合。然後，您可以使用 Security Hub CSPM API，將調查結果從這些產品傳送至 Security Hub CSPM。您也可以使用 API 來更新 Security Hub CSPM 從自訂安全產品收到的現有問題清單。

主題

- [檢閱 Security Hub CSPM 整合的清單](#)
- [啟用來自 Security Hub CSPM 整合的問題清單流程](#)
- [從 Security Hub CSPM 整合停用問題清單的流程](#)
- [從 Security Hub CSPM 整合檢視問題清單](#)
- [AWS 服務 與 Security Hub CSPM 整合](#)
- [與 Security Hub CSPM 的第三方產品整合](#)
- [將 Security Hub CSPM 與自訂產品整合](#)

檢閱 Security Hub CSPM 整合的清單

選擇您偏好的方法，並依照步驟檢閱 AWS Security Hub CSPM 中的整合清單或特定整合的詳細資訊。

Security Hub CSPM console

若要檢閱整合選項和詳細資訊（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在 Security Hub CSPM 導覽窗格中，選擇整合。

在整合頁面上，AWS 服務 會先列出與其他 的整合，然後列出與第三方產品的整合。

整合頁面會針對每個整合提供下列資訊：

- 公司名稱
- 產品名稱
- 整合描述
- 整合的適用類別
- 啟用整合的方式
- 整合目前的狀態

您可以從下列欄位輸入文字來篩選清單：

- 公司名稱
- 產品名稱
- 整合描述
- 類別

Security Hub CSPM API

檢閱整合選項和詳細資訊 (API)

若要取得整合清單，請使用 [DescribeProducts](#) 操作。如果您使用的是 AWS CLI，請執行 [describe-products](#) 命令。

若要擷取特定產品整合的詳細資訊，請使用 ProductArn 參數指定整合的 Amazon Resource Name (ARN)。

例如，下列 AWS CLI 命令會擷取 Security Hub CSPM 與 3CORESec 整合的詳細資訊。

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

啟用來自 Security Hub CSPM 整合的問題清單流程

在 AWS Security Hub CSPM 主控台的整合頁面上，您可以查看啟用每個整合所需的步驟。

對於大多數與其他整合 AWS 服務，啟用整合的唯一必要步驟是啟用其他服務。整合資訊包含其他服務首頁的連結。當您啟用其他服務時，會自動建立並套用允許 Security Hub CSPM 從服務接收問題清單的資源層級許可。

對於第三方產品整合，您可能需要從購買整合 AWS Marketplace，然後設定整合。整合資訊提供完成這些任務的連結。

如果有一個以上的產品版本可用 AWS Marketplace，請選取您要訂閱的版本，然後選擇繼續訂閱。例如，某些產品提供標準版本和 AWS GovCloud (US) 版本。

當您啟用產品整合時，資源政策會自動連接到該產品訂閱。此資源政策定義 Security Hub CSPM 從該產品接收問題清單所需的許可。

完成啟用整合的任何初步步驟後，您就可以停用並重新啟用該整合的問題清單流程。在整合頁面上，對於傳送問題清單的整合，狀態資訊會指出您目前是否接受問題清單。

Security Hub CSPM console

從整合啟用問題清單流程（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在 Security Hub CSPM 導覽窗格中，選擇整合。
3. 對於傳送問題清單的整合，狀態資訊會指出 Security Hub CSPM 目前是否接受來自該整合的問題清單。
4. 選擇接受問題清單。

Security Hub CSPM API

使用 [EnableImportFindingsForProduct](#) 操作。如果您使用的是 AWS CLI，請執行 [enable-import-findings-for-product](#) 命令。若要讓 Security Hub 從整合接收問題清單，您需要產品 ARN。若要取

得可用整合ARNs，請使用 [DescribeProducts](#) 操作。如果您使用的是 AWS CLI，請執行 [describe-products](#)。

例如，下列 AWS CLI 命令可讓 Security Hub CSPM 從 CrowdStrike Falcon 整合接收問題清單。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub enable-import-findings-for product --product-arn  
"arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

從 Security Hub CSPM 整合停用問題清單的流程

選擇您偏好的方法，並依照步驟停用來自 AWS Security Hub CSPM 整合的問題清單流程。

Security Hub CSPM console

從整合停用問題清單流程（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在 Security Hub CSPM 導覽窗格中，選擇整合。
3. 對於傳送問題清單的整合，狀態資訊會指出 Security Hub CSPM 目前是否接受來自該整合的問題清單。
4. 選擇停止接受問題清單。

Security Hub CSPM API

使用 [DisableImportFindingsForProduct](#) 操作。如果您使用的是 AWS CLI，請執行 [disable-import-findings-for-product](#) 命令。若要停用整合的問題清單流程，您需要訂閱 ARN 才能啟用整合。若要取得訂閱 ARN，請使用 [ListEnabledProductsForImport](#) 操作。如果您使用的是 AWS CLI，請執行 [list-enabled-products-for-import](#)。

例如，下列 AWS CLI 命令會停用從 CrowdStrike Falcon 整合到 Security Hub CSPM 的問題清單流程。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn  
"arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/  
crowdstrike-falcon"
```

從 Security Hub CSPM 整合檢視問題清單

當您開始接受來自 AWS Security Hub CSPM 整合的問題清單時，Security Hub CSPM 主控台的整合頁面會將整合的狀態顯示為接受問題清單。若要從整合檢閱問題清單，請選擇查看問題清單。

問題清單會顯示工作流程狀態為 NEW 或 NOTIFIED 選取整合的作用中問題清單。

如果您啟用跨區域彙總，則在彙總區域中，清單會包含來自彙總區域和啟用整合之連結區域的問題清單。Security Hub 不會根據跨區域彙總組態自動啟用整合。

在其他區域中，整合的調查結果清單僅包含目前區域的調查結果。

如需如何設定跨區域彙總的資訊，請參閱 [the section called “跨區域彙總資料”](#)。

從問題清單，您可以執行下列動作。

- [變更清單的篩選條件和群組](#)
- [檢視個別問題清單的詳細資訊](#)
- [更新問題清單的工作流程狀態](#)
- [將問題清單傳送到自訂動作](#)

AWS 服務 與 Security Hub CSPM 整合

AWS Security Hub CSPM 支援與其他數個整合 AWS 服務。這些整合可協助您全面了解整個 AWS 環境的安全性和合規性。

除非以下另有說明，否則在您啟用 Security Hub CSPM 和其他服務之後，會自動啟用將問題清單傳送到 Security Hub CSPM 的 AWS 服務整合。接收 Security Hub CSPM 調查結果的整合可能需要額外的啟用步驟。檢閱每個整合的相關資訊以進一步了解。

有些整合無法全部使用 AWS 區域。在 Security Hub CSPM 主控台上，如果目前區域中不支援整合，則整合不會出現在整合頁面上。如需中國區域可用的整合清單 AWS GovCloud (US) Regions，請參閱 [依區域的整合可用性](#)。

與 Security Hub CSPM AWS 的服務整合概觀

下表提供將問題清單傳送至 Security Hub CSPM 或從 Security Hub CSPM 接收問題清單的 AWS 服務概觀。

整合式 AWS 服務	Direction	
AWS Config	傳送問題清單	
AWS Firewall Manager	傳送問題清單	
Amazon GuardDuty	傳送問題清單	
AWS Health	傳送問題清單	
AWS Identity and Access Management Access Analyzer	傳送問題清單	
Amazon Inspector	傳送問題清單	
AWS IoT Device Defender	傳送問題清單	
Amazon Macie	傳送問題清單	
Amazon Route 53 Resolver DNS 防火牆	傳送問題清單	
AWS Systems Manager 修補程式管理員	傳送問題清單	
AWS Audit Manager	接收問題清單	
聊天應用程式中的 Amazon Q Developer	接收問題清單	
Amazon Detective	接收問題清單	
Amazon Security Lake	接收問題清單	
AWS Systems Manager Explorer 和 OpsCenter	接收和更新問題清單	
AWS Trusted Advisor	接收問題清單	

AWS 服務 將問題清單傳送至 Security Hub CSPM

下列 與 AWS 服務 整合，可將問題清單傳送至 Security Hub CSPM。Security Hub CSPM 會將問題清單轉換為[AWS 安全問題清單格式](#)。

AWS Config（傳送問題清單）

AWS Config 是一項服務，可讓您評估、稽核和評估 AWS 資源的組態。AWS Config 會持續監控和記錄您的 AWS 資源組態，並可讓您根據所需的組態自動評估記錄的組態。

透過使用 整合 AWS Config，您可以在 Security Hub CSPM 中將 AWS Config 受管和自訂規則評估的結果視為調查結果。這些調查結果可以與其他 Security Hub CSPM 調查結果一起檢視，提供安全狀態的完整概觀。

AWS Config 使用 Amazon EventBridge 將 AWS Config 規則評估傳送至 Security Hub CSPM。Security Hub CSPM 會將規則評估轉換為遵循 [AWS Security Finding 格式](#) 的調查結果。然後，Security Hub CSPM 會盡最大努力取得受影響資源的詳細資訊，例如 Amazon Resource Name (ARN)、資源標籤和建立日期。

如需此整合的詳細資訊，請參閱下列各節。

如何 AWS Config 將問題清單傳送至 Security Hub CSPM

Security Hub CSPM 中的所有調查結果都使用 ASFF 的標準 JSON 格式。ASFF 包含調查結果的來源、受影響的資源，以及調查結果目前狀態的詳細資訊。透過 EventBridge 將受管和自訂規則評估 AWS Config 傳送至 Security Hub CSPM。Security Hub CSPM 會將規則評估轉換為遵循 ASFF 的調查結果，並盡力充實調查結果。

AWS Config 傳送至 Security Hub CSPM 的問題清單類型

啟用整合後，會將所有 AWS Config 受管規則和自訂規則的評估 AWS Config 傳送至 Security Hub CSPM。只會傳送啟用 Security Hub CSPM 後執行的評估。例如，假設 AWS Config 規則評估顯示五個失敗的資源。如果您在評估之後啟用 Security Hub CSPM，然後規則顯示第六個失敗的資源，則只會 AWS Config 將第六個資源評估傳送到 Security Hub CSPM。

排除來自[服務連結 AWS Config 規則](#)的評估，例如用於執行 Security Hub CSPM 控制項檢查的規則。例外狀況是由在其中 AWS Control Tower 建立和管理的服務連結規則所產生的問題清單 AWS Config。包含這些規則的調查結果有助於確保您的調查結果資料包含由執行的主動檢查結果 AWS Control Tower。

將 AWS Config 問題清單傳送至 Security Hub CSPM

啟用整合時，Security Hub CSPM 將自動指派接收問題清單所需的許可 AWS Config。Security Hub CSPM 使用 service-to-service 層級許可，為您提供安全的方式來啟用此整合，並透過 AWS Config Amazon EventBridge 從 匯入問題清單。

傳送問題清單延遲

當 AWS Config 建立新的問題清單時，您通常可以在五分鐘內在 Security Hub CSPM 中檢視問題清單。

無法使用 Security Hub CSPM 時重試

AWS Config 會盡最大努力透過 EventBridge 將問題清單傳送至 Security Hub CSPM。當事件未成功交付至 Security Hub CSPM 時，EventBridge 會重試交付最多 24 小時或 185 次，以先到者為準。

更新 Security Hub CSPM 中的現有 AWS Config 問題清單

在 AWS Config 將問題清單傳送至 Security Hub CSPM 之後，可以將相同問題清單的更新傳送至 Security Hub CSPM，以反映問題清單活動的其他觀察。更新只會針對 ComplianceChangeNotification 事件傳送。如果沒有發生合規變更，則不會將更新傳送至 Security Hub CSPM。Security Hub CSPM 會在最近一次更新後 90 天刪除問題清單，如果沒有更新，則會在建立問題清單後 90 天刪除問題清單。

AWS Config 即使您刪除相關聯的資源，Security Hub CSPM 也不會封存從 傳送的問題清單。

問題 AWS Config 清單存在的區域

AWS Config 問題清單是以區域為基礎。會將問題清單 AWS Config 傳送至發生問題清單的相同區域或區域中的 Security Hub CSPM。

在 Security Hub CSPM 中檢視 AWS Config 問題清單

若要檢視問題 AWS Config 清單，請從 Security Hub CSPM 導覽窗格中選擇問題清單。若要篩選問題清單以僅顯示 AWS Config 問題清單，請在搜尋列下拉式清單中選擇產品名稱。輸入 Config，然後選擇套用。

解譯 Security Hub CSPM 中的 AWS Config 問題清單名稱

Security Hub CSPM 會將 AWS Config 規則評估轉換為遵循 [AWS 安全調查結果格式 \(ASFF\)](#)。AWS Config rule 評估的調查結果，使用與 ASFF 不同的事件模式。下表將 AWS Config 規則評估欄位與其 ASFF 對應，如 Security Hub CSPM 中所示。

Config 規則評估調查結果類型	ASFF 問題清單類型	硬式編碼值
detail.awsAccountId	AwsAccountId	
detail.newEvaluationResult. resultRecordedTime	CreatedAt	
detail.newEvaluationResult. resultRecordedTime	UpdatedAt	
	ProductArn	「arn : <partition> : securityhub : <region> : : product/aws/config」
	ProductName	「組態」
	CompanyName	"AWS"
	區域	"eu-central-1"
configRuleArn	GeneratorId、ProductFields	
detail.ConfigRuleARN/finding/ hash	Id	
detail.configRuleName	Title、ProductFields	
detail.configRuleName	說明	「針對組態規則的資源 合規變更建立此調查結果 : \${detail.ConfigRuleName} 」
組態項目「ARN」或 Security Hub CSPM 計算的 ARN	資源 【i】 .id	
detail.resourceType	資源 【i】 。類型	"AwsS3Bucket"
	資源 【i】 。分割區	"aws"
	資源 【i】 。區域	"eu-central-1"

Config 規則評估調查結果類型	ASFF 問題清單類型	硬式編碼值
組態項目「組態」	資源 【i】 。詳細資訊	
	SchemaVersion	"2018-10-08"
	Severity.Label	請參閱以下「解釋嚴重性標籤」
	類型	【「軟體和組態檢查」】
detail.newEvaluationResult.complianceType	Compliance.Status	「失敗」、「NOT_AVAILABLE」、「通過」或「警告」
	Workflow.Status	如果 AWS Config 問題清單是以「通過」的 Compliance.Status 產生，或 Compliance.Status 從「失敗」變更為「通過」，則為「已解決」。否則，Workflow.Status 將為「新」。您可以使用 BatchUpdateFindings API 操作變更此值。

解釋嚴重性標籤

AWS Config 規則評估中的所有調查結果在 ASFF 中都有預設的 MEDIUM 嚴重性標籤。您可以使用 [BatchUpdateFindings](#) API 操作更新問題清單的嚴重性標籤。

來自 的典型問題清單 AWS Config

Security Hub CSPM 會將 AWS Config 規則評估轉換為遵循 ASFF 的調查結果。以下是 ASFF AWS Config 中來自 的典型問題清單範例。

Note

如果描述超過 1,024 個字元，則會截斷為 1,024 個字元，並在結尾顯示「(截斷)」。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
  "ProductName": "Config",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks"
  ],
  "CreatedAt": "2022-04-15T05:00:37.181Z",
  "UpdatedAt": "2022-04-19T21:20:15.056Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
  "Description": "This finding is created for a resource compliance change for config rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
  "ProductFields": {
    "aws/securityhub/ProductName": "Config",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
    "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq",
    "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-integration-demo",
    "aws/config/ConfigComplianceType": "NON_COMPLIANT"
  },
  "Resources": [{
    "Type": "AwsS3Bucket",
    "Id": "arn:aws:s3:::amzn-s3-demo-bucket",
    "Partition": "aws",
    "Region": "eu-central-1",
    "Details": {
      "AwsS3Bucket": {
        "OwnerId": "4edbbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
```

```
    "CreatedAt": "2022-04-15T04:32:53.000Z"
  }
}
]],
"Compliance": {
  "Status": "FAILED"
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks"
  ]
}
}
```

啟用與設定整合

啟用 Security Hub CSPM 後，會自動啟用此整合。AWS Config 會立即開始將問題清單傳送至 Security Hub CSPM。

停止將問題清單發佈至 Security Hub CSPM

若要停止將問題清單傳送至 Security Hub CSPM，您可以使用 Security Hub CSPM 主控台或 Security Hub CSPM API。

如需停止問題清單流程的說明，請參閱 [啟用來自 Security Hub CSPM 整合的問題清單流程](#)。

AWS Firewall Manager (傳送問題清單)

當資源的 Web 應用程式防火牆 (WAF) 政策或 Web 存取控制清單 (Web ACL) 規則不合規時，防火牆管理員會將問題清單傳送至 Security Hub CSPM。當 AWS Shield Advanced 未保護資源，或發現攻擊時，防火牆管理員也會傳送問題清單。

啟用 Security Hub CSPM 後，會自動啟用此整合。Firewall Manager 會立即開始將問題清單傳送至 Security Hub CSPM。

若要進一步了解整合，請在 Security Hub CSPM 主控台中檢視整合頁面。

若要進一步了解 Firewall Manager，請參閱 [AWS WAF 開發人員指南](#)。

Amazon GuardDuty (傳送調查結果)

GuardDuty 會將其產生的所有調查結果類型傳送至 Security Hub CSPM。有些問題清單類型具有先決條件、啟用要求或區域限制。如需詳細資訊，請參閱《Amazon [GuardDuty 使用者指南](#)》中的 [GuardDuty 調查結果類型](#)。Amazon GuardDuty

GuardDuty 的新調查結果會在五分鐘內傳送至 Security Hub CSPM。問題清單的更新會根據 GuardDuty 設定中 Amazon EventBridge 的更新問題清單設定傳送。

當您使用 GuardDuty 設定頁面產生 GuardDuty 範例問題清單時，Security Hub CSPM 會收到範例問題清單，並省略[Sample]問題清單類型的字首。例如，GuardDuty 中的範例調查結果類型[SAMPLE] Recon:IAMUser/ResourcePermissions會顯示為 Security Hub CSPM Recon:IAMUser/ResourcePermissions中的。

啟用 Security Hub CSPM 後，會自動啟用此整合。GuardDuty 會立即開始將問題清單傳送至 Security Hub CSPM。

如需 GuardDuty 整合的詳細資訊，請參閱《Amazon GuardDuty 使用者指南》中的[與 AWS Security Hub CSPM 整合](#)。

AWS Health (傳送問題清單)

AWS Health 可讓您持續了解資源效能，以及 AWS 服務 和 的可用性 AWS 帳戶。您可以使用 AWS Health 事件來了解服務和資源變更如何影響執行 的應用程式 AWS。

與 的整合 AWS Health 不使用 BatchImportFindings。反之，AWS Health 會使用service-to-service事件傳訊，將問題清單傳送至 Security Hub CSPM。

如需整合的詳細資訊，請參閱下列各節。

如何 AWS Health 將問題清單傳送至 Security Hub CSPM

在 Security Hub CSPM 中，將安全問題做為調查結果進行追蹤。有些問題清單來自 AWS 其他服務或第三方合作夥伴偵測到的問題。Security Hub CSPM 也有一組規則，可用來偵測安全問題並產生問題清單。

Security Hub CSPM 提供用來跨所有這些來源管理調查結果的工具。您可以檢視並篩選問題清單列表，並檢視問題清單的詳細資訊。請參閱 [在 Security Hub CSPM 中檢閱問題清單詳細資訊和歷史記](#)

[錄](#)。您也可以追蹤問題清單的調查狀態。請參閱 [在 Security Hub CSPM 中設定問題清單的工作流程狀態](#)。

Security Hub CSPM 中的所有調查結果都使用稱為 的標準 JSON 格式[AWS 安全調查結果格式 \(ASFF\)](#)。ASFF 包含問題來源、受影響資源的詳細資訊，以及調查結果的目前狀態。

AWS Health 是將問題清單傳送至 Security Hub CSPM 的其中一個 AWS 服務。

AWS Health 傳送至 Security Hub CSPM 的問題清單類型

啟用整合之後，會將符合一或多個所列規格的問題清單 AWS Health 傳送至 Security Hub CSPM。Security Hub CSPM 會擷取 中的調查結果[AWS 安全調查結果格式 \(ASFF\)](#)。

• 包含下列任何 值的調查結果 AWS 服務：

- RISK
- ABUSE
- ACM
- CLOUDHSM
- CLOUDTRAIL
- CONFIG
- CONTROLTOWER
- DETECTIVE
- EVENTS
- GUARDDUTY
- IAM
- INSPECTOR
- KMS
- MACIE
- SES
- SECURITYHUB
- SHIELD
- SSO
- COGNITO

AWS 服務 整合

- IOTDEVICEDEFENDER

- NETWORKFIREWALL
- ROUTE53
- WAF
- FIREWALLMANAGER
- SECRETSMANAGER
- BACKUP
- AUDITMANAGER
- ARTIFACT
- CLOUDENDURE
- CODEGURU
- ORGANIZATIONS
- DIRECTORYSERVICE
- RESOURCEMANAGER
- CLOUDWATCH
- DRS
- INSPECTOR2
- RESILIENCEHUB
- 欄位中具有單字 security、abuse或 的調查結果 certificate AWS Health typeCode
- AWS Health 服務為 risk或 的調查結果 abuse

將 AWS Health 問題清單傳送至 Security Hub CSPM

當您選擇接受問題清單時 AWS Health，Security Hub CSPM 會自動指派接收問題清單所需的許可 AWS Health。Security Hub CSPM 使用service-to-service層級許可，為您提供安全、簡單的方法來代表您 AWS Health 透過 Amazon EventBridge 從 啟用此整合和匯入問題清單。選擇接受問題清單會授予 Security Hub CSPM 使用問題清單的許可 AWS Health。

傳送問題清單延遲

當 AWS Health 建立新的問題清單時，通常會在五分鐘內傳送至 Security Hub CSPM。

無法使用 Security Hub CSPM 時重試

AWS Health 會盡最大努力透過 EventBridge 將問題清單傳送至 Security Hub CSPM。當事件未成功交付至 Security Hub CSPM 時，EventBridge 會重試傳送事件 24 小時。

更新 Security Hub CSPM 中的現有調查結果

在 AWS Health 將問題清單傳送至 Security Hub CSPM 後，可以傳送更新至相同的問題清單，以反映對 Security Hub CSPM 的問題清單活動的其他觀察。

問題清單存在的區域

對於全域事件，AWS Health 會將問題清單傳送至 us-east-1 (AWS 分割區)、cn-northwest-1 (中國分割區) 和 gov-us-west-1 (GovCloud 分割區) 中的 Security Hub CSPM。會將區域特定事件 AWS Health 傳送至事件發生的相同區域或區域中的 Security Hub CSPM。

在 Security Hub CSPM 中檢視 AWS Health 問題清單

若要在 Security Hub CSPM 中檢視問題 AWS Health 清單，請從導覽面板中選擇問題清單。若要篩選問題清單以僅顯示問題 AWS Health 清單，請從產品名稱欄位中選擇運作狀態。

解譯 Security Hub CSPM 中的 AWS Health 問題清單名稱

AWS Health 使用 [AWS 安全調查結果格式 \(ASFF\)](#)。AWS Health finding 將調查結果傳送到 Security Hub CSPM，與 Security Hub CSPM ASFF 格式相比，會使用不同的事件模式。下表詳細說明所有 AWS Health 調查結果欄位及其 ASFF 對應欄位，如它們在 Security Hub CSPM 中所示。

運作狀態問題清單類型	ASFF 問題清單類型	硬式編碼值
帳戶	AwsAccountId	
detail.startTime	CreatedAt	
detail.eventDescription.lat estDescription	說明	
detail.eventTypeCode	GeneratorId	
detail.eventArn (包括帳戶) + detail.startTime 的雜湊	Id	
「arn : aws : securityhub : <region> : : product/aws/he alth」	ProductArn	
帳戶或 resourceId	資源 【i】 .id	

運作狀態問題清單類型	ASFF 問題清單類型	硬式編碼值
	資源 【i】 。類型	「其他」
	SchemaVersion	"2018-10-08"
	Severity.Label	請參閱以下「解譯嚴重性標籤」
"AWS Health -" detail.eventTypeCode	Title	
-	類型	【「軟體和組態檢查」】
event.time	UpdatedAt	
Health 主控台上的事件 URL	SourceUrl	

解譯嚴重性標籤

ASFF 調查結果中的嚴重性標籤使用以下邏輯決定：

- 如果符合下列條件，嚴重性至關重要：
 - 調查結果中的 service AWS Health 欄位具有 值 Risk
 - 調查結果中的 typeCode AWS Health 欄位具有 值 AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION
 - 調查結果中的 typeCode AWS Health 欄位具有 值 AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK
 - 調查結果中的 typeCode AWS Health 欄位具有 值 AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES

嚴重性高，如果：

- 調查結果中的 service AWS Health 欄位具有 值 Abuse
- 調查結果中的 typeCode AWS Health 欄位包含 值 SECURITY_NOTIFICATION
- 調查結果中的 typeCode AWS Health 欄位包含 值 ABUSE_DETECTION

嚴重性中，如果：

- 問題清單中的 service 欄位是下列任何項目：ACM、ARTIFACT、AUDITMANAGER、BACKUPCLOUDENDURECLOUDHSMCLOUDTRAIL、或 WAF
- AWS Health 調查結果中的 typeCode 欄位包含 值 CERTIFICATE
- AWS Health 調查結果中的 typeCode 欄位包含 值 END_OF_SUPPORT

來自的典型問題清單 AWS Health

AWS Health 使用 將問題清單傳送至 Security Hub CSPM [AWS 安全調查結果格式 \(ASFF\)](#)。以下是典型問題清單的範例 AWS Health。

Note

如果描述超過 1024 個字元，則會截斷為 1024 個字元，並在結尾說出（截斷）。

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
  "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks"
  ],
  "CreatedAt": "2022-01-07T16:34:04.000Z",
  "UpdatedAt": "2022-01-07T19:17:43.000Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
  "Description": "Congratulations! Amazon SES has successfully detected the
MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\n\nYou can now use this MAIL
FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity"
```

```

that is configured to use it. For information about how to configure a verified
identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
AWS Region US East (N. Virginia).",
    "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
    "ProductFields": {
        "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
        "aws/securityhub/ProductName": "Health",
        "aws/securityhub/CompanyName": "AWS"
    },
    "Resources": [
        {
            "Type": "Other",
            "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
        }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
        "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
        "Severity": {
            "Label": "MEDIUM"
        },
        "Types": [
            "Software and Configuration Checks"
        ]
    }
}
]
}

```

啟用與設定整合

啟用 Security Hub CSPM 後，會自動啟用此整合。AWS Health 立即開始將問題清單傳送至 Security Hub CSPM。

停止將問題清單發佈至 Security Hub CSPM

若要停止將問題清單傳送至 Security Hub CSPM，您可以使用 Security Hub CSPM 主控台或 Security Hub CSPM API。

如需停止問題清單流程的說明，請參閱 [啟用來自 Security Hub CSPM 整合的問題清單流程](#)。

AWS Identity and Access Management Access Analyzer（傳送問題清單）

使用 IAM Access Analyzer，所有調查結果都會傳送至 Security Hub CSPM。

IAM Access Analyzer 使用邏輯式推理來分析套用至帳戶中支援資源的資源型政策。當 IAM Access Analyzer 偵測到允許外部委託人存取您帳戶中資源的政策陳述式時，會產生調查結果。

在 IAM Access Analyzer 中，只有管理員帳戶可以看到適用於組織的分析器問題清單。對於組織分析器，`AwsAccountIdASFF` 欄位反映管理員帳戶 ID。在 `ProductFields`，`ResourceOwnerAccount` 欄位會指出發現問題清單的帳戶。如果您個別為每個帳戶啟用分析器，Security Hub CSPM 會產生多個調查結果，一個識別管理員帳戶 ID，另一個識別資源帳戶 ID。

如需詳細資訊，請參閱《IAM 使用者指南》中的 [與 AWS Security Hub CSPM 整合](#)。

Amazon Inspector（傳送問題清單）

Amazon Inspector 是一種漏洞管理服務，可持續掃描工作負載 AWS 是否有漏洞。Amazon Inspector 會自動探索和掃描位於 Amazon Elastic Container Registry 中的 Amazon EC2 執行個體和容器映像。掃描會尋找軟體漏洞和意外的網路暴露。

啟用 Security Hub CSPM 後，會自動啟用此整合。Amazon Inspector 會立即開始將所有產生的問題清單傳送至 Security Hub CSPM。

如需整合的詳細資訊，請參閱《Amazon Inspector 使用者指南》中的 [與 AWS Security Hub CSPM 整合](#)。

Security Hub CSPM 也可以從 Amazon Inspector Classic 接收問題清單。Amazon Inspector Classic 會將問題清單傳送至 Security Hub CSPM，這些問題清單是透過所有支援的規則套件的評估執行所產生的。

如需整合的詳細資訊，請參閱《Amazon Inspector Classic 使用者指南》中的 [與 AWS Security Hub CSPM 整合](#)。

Amazon Inspector 和 Amazon Inspector Classic 的調查結果使用相同的產品 ARN。Amazon Inspector 調查結果在 `ProductFields` 中具有下列項目：

```
"aws/inspector/ProductVersion": "2",
```

Note

[Amazon Inspector Code Security](#) 產生的安全調查結果不適用於此整合。不過，您可以在 Amazon Inspector 主控台和透過 [Amazon Inspector API](#) 存取這些特定問題清單。

AWS IoT Device Defender (傳送問題清單)

AWS IoT Device Defender 是一種安全服務，可稽核 IoT 裝置的組態、監控連線裝置以偵測異常行為，並協助降低安全風險。

啟用 AWS IoT Device Defender 和 Security Hub CSPM 後，請造訪 [Security Hub CSPM 主控台的整合頁面](#)，然後選擇接受稽核、偵測或兩者的調查結果。AWS IoT Device Defender Audit 和 Detect 開始將所有調查結果傳送至 Security Hub CSPM。

AWS IoT Device Defender 稽核會將檢查摘要傳送至 Security Hub CSPM，其中包含特定稽核檢查類型和稽核任務的一般資訊。AWS IoT Device Defender 偵測會將機器學習 (ML)、統計和靜態行為的違規調查結果傳送至 Security Hub CSPM。稽核也會將問題清單更新傳送至 Security Hub CSPM。

如需此整合的詳細資訊，請參閱《AWS IoT 開發人員指南》中的[與 AWS Security Hub CSPM 整合](#)。

Amazon Macie (傳送問題清單)

Amazon Macie 是一種資料安全服務，透過使用機器學習和模式比對來探索敏感資料、提供資料安全風險的可見性，以及啟用自動保護以防範這些風險。Macie 的調查結果可能表示您的 Amazon S3 資料資產中存在潛在的政策違規或敏感資料。

啟用 Security Hub CSPM 後，Macie 會自動開始將政策調查結果傳送至 Security Hub CSPM。您可以設定整合，以同時將敏感資料調查結果傳送至 Security Hub CSPM。

在 Security Hub CSPM 中，政策或敏感資料調查結果的調查結果類型會變更為與 ASFF 相容的值。例如，Macie 中的 Policy:IAMUser/S3BucketPublic 調查結果類型會顯示為 Security Hub CSPM Effects/Data Exposure/Policy:IAMUser-S3BucketPublic 中的。

Macie 也會將產生的範例調查結果傳送至 Security Hub CSPM。針對範例問題清單，受影響的資源名稱，macie-sample-finding-bucket 而 Sample 欄位的值為 true。

如需詳細資訊，請參閱《Amazon [Macie 使用者指南](#)》中的使用 [Security Hub 評估 Macie 問題](#) 清單。
Amazon Macie

Amazon Route 53 Resolver DNS 防火牆 (傳送問題清單)

使用 Amazon Route 53 Resolver DNS 防火牆，您可以篩選和調節虛擬私有雲端 (VPC) 的傳出 DNS 流量。您可以透過在 DNS 防火牆規則群組中建立可重複使用的篩選規則集合、將規則群組與 VPC 建立關聯，然後監控 DNS 防火牆日誌和指標中的活動來執行此操作。根據活動，您可以調整 DNS 防火牆行為。DNS 防火牆是 Route 53 Resolver 的一項功能。

Route 53 Resolver DNS Firewall 可以將多種問題清單類型傳送至 Security Hub CSPM：

- 與 AWS 受管網域清單相關聯的網域在 上封鎖或提醒的查詢相關的問題清單，這些網域清單是 管理的 AWS 網域清單。
- 對於與您定義的自訂網域清單相關聯的網域，與 上封鎖或提醒的查詢相關的調查結果。
- 與 DNS Firewall Advanced 封鎖或提醒的查詢相關的調查結果，這是一種 Route 53 Resolver 功能，可偵測與網域產生演算法 (DGAs) 和 DNS 通道等進階 DNS 威脅相關聯的查詢。

啟用 Security Hub CSPM 和 Route 53 Resolver DNS 防火牆之後，DNS 防火牆會自動開始將 AWS 受管網域清單和 DNS Firewall Advanced 的問題清單傳送至 Security Hub CSPM。若要將自訂網域清單的問題清單傳送至 Security Hub CSPM，請在 Security Hub CSPM 中手動啟用整合。

在 Security Hub CSPM 中，Route 53 Resolver DNS Firewall 的所有問題清單都具有下列類型：TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation。

如需詳細資訊，請參閱 [《Amazon Route 53 開發人員指南》中的將問題清單從 Route 53 Resolver DNS 防火牆傳送至 Security Hub](#)。

AWS Systems Manager 修補程式管理員 (傳送問題清單)

AWS Systems Manager 當客戶機群中的執行個體不符合其修補程式合規標準時，修補程式管理員會將問題清單傳送至 Security Hub CSPM。

Patch Manager 以安全相關和其他類型的更新自動化以修補受管執行個體。

啟用 Security Hub CSPM 後，會自動啟用此整合。Systems Manager 修補程式管理員會立即開始將問題清單傳送至 Security Hub CSPM。

如需使用修補程式管理員的詳細資訊，請參閱AWS Systems Manager 《使用者指南》中的[AWS Systems Manager 修補程式管理員](#)。

AWS 從 Security Hub CSPM 接收問題清單的服務

下列 AWS 服務已與 Security Hub CSPM 整合，並從 Security Hub CSPM 接收問題清單。如前所述，整合服務也可能更新問題清單。在這種情況下，您在整合服務中所做的更新也會反映在 Security Hub CSPM 中。

AWS Audit Manager（接收問題清單）

AWS Audit Manager 從 Security Hub CSPM 接收問題清單。這些調查結果可協助 Audit Manager 使用者準備稽核。

若要進一步了解 Audit Manager，請參閱 [AWS Audit Manager 使用者指南](#)。[AWS 支援的 Security Hub CSPM 檢查 AWS Audit Manager](#) 會列出 Security Hub CSPM 將調查結果傳送至 Audit Manager 的控制項。

聊天應用程式中的 Amazon Q Developer（接收問題清單）

聊天應用程式中的 Amazon Q Developer 是一種互動式代理程式，可協助您監控 Slack 頻道和 Amazon Chime 聊天室中的 AWS 資源並與之互動。

聊天應用程式中的 Amazon Q Developer 會收到 Security Hub CSPM 的問題清單。

若要進一步了解聊天應用程式與 Security Hub CSPM 整合中的 Amazon Q 開發人員，請參閱聊天應用程式管理員指南中的 Amazon Q 開發人員中的 [Security Hub CSPM 整合概觀](#)。

Amazon Detective（接收問題清單）

Detective 會自動從您的 AWS 資源收集日誌資料，並使用機器學習、統計分析和圖形理論，協助您視覺化和執行更快速且更有效率的安全調查。

Security Hub CSPM 與 Detective 整合可讓您從 Security Hub CSPM 中的 Amazon GuardDuty 調查結果轉向 Detective。然後，您可以使用 Detective 工具和視覺化來調查它們。整合不需要在 Security Hub CSPM 或 Detective 中進行任何額外的組態。

對於從其他收到的調查結果 AWS 服務，Security Hub CSPM 主控台上的調查結果詳細資訊面板包含 Detective 小節中的調查。該子區段包含 Detective 的連結，您可以在其中進一步調查調查結果標記的安全問題。您也可以根據 Security Hub CSPM 調查結果在 Detective 中建置行為圖表，以進行更有效的調查。如需詳細資訊，請參閱《Amazon Detective 管理指南》中的 [AWS 安全調查結果](#)。

如果啟用跨區域彙總，則當您從彙總區域樞紐時，Detective 會在問題清單來源的區域中開啟。

如果連結無效，則針對故障診斷建議，請參閱 [針對樞紐進行故障診斷](#)。

Amazon Security Lake (接收調查結果)

Security Lake 是全受管的安全資料湖服務。您可以使用 Security Lake 將來自雲端、內部部署和自訂來源的安全資料自動集中到存放在您帳戶中的資料湖中。訂閱者可以使用來自 Security Lake 的資料進行調查和分析使用案例。

若要啟用此整合，您必須啟用這兩個服務，並在 Security Lake 主控台、Security Lake API 或中新增 Security Hub CSPM 做為來源 AWS CLI。完成這些步驟後，Security Hub CSPM 會開始將所有調查結果傳送至 Security Lake。

Security Lake 會自動標準化 Security Hub CSPM 調查結果，並將其轉換為稱為開放網路安全結構描述架構 (OCSF) 的標準化開放原始碼結構描述。在 Security Lake 中，您可以新增一或多個訂閱者來取用 Security Hub CSPM 調查結果。

如需此整合的詳細資訊，包括新增 Security Hub CSPM 做為來源和建立訂閱者的指示，請參閱《Amazon Security Lake 使用者指南》中的[與 AWS Security Hub CSPM 整合](#)。

AWS Systems Manager Explorer 和 OpsCenter (接收和更新調查結果)

AWS Systems Manager Explorer 和 OpsCenter 會從 Security Hub CSPM 接收調查結果，並在 Security Hub CSPM 中更新這些調查結果。

Explorer 為您提供可自訂的儀表板，提供對您 AWS 環境運作狀態和效能的關鍵洞察和分析。

OpsCenter 為您提供一個集中位置來檢視、調查和解決操作工作項目。

如需 Explorer 和 OpsCenter 的詳細資訊，請參閱AWS Systems Manager 《使用者指南》中的[操作管理](#)。

AWS Trusted Advisor (接收問題清單)

Trusted Advisor 利用從為數十萬 AWS 客戶提供服務的最佳實務。會 Trusted Advisor 檢查您的 AWS 環境，然後在有機會節省成本、改善系統可用性和效能，或協助填補安全漏洞時提出建議。

當您同時啟用 Trusted Advisor 和 Security Hub CSPM 時，整合會自動更新。

Security Hub CSPM 會將 AWS 其基礎安全最佳實務檢查的結果傳送至 Trusted Advisor。

如需與 Security Hub CSPM 整合的詳細資訊 Trusted Advisor，請參閱 AWS 支援使用者指南中的[在中檢視 AWS Security Hub CSPM 控制項 AWS Trusted Advisor](#)。

與 Security Hub CSPM 的第三方產品整合

AWS Security Hub CSPM 與多個第三方合作夥伴產品整合。整合可以執行下列一或多個動作：

- 將產生的問題清單傳送至 Security Hub CSPM
- 從 Security Hub CSPM 接收問題清單
- 在 Security Hub CSPM 中更新問題清單

將問題清單傳送到 Security Hub CSPM 的整合具有 Amazon Resource Name (ARN)。

整合可能無法全部使用 AWS 區域。如果您目前在 Security Hub CSPM 主控台登入的區域中不支援整合，則不會出現在主控台的整合頁面上。如需中國區域可用的整合清單 AWS GovCloud (US) Regions，請參閱 [依區域的整合可用性](#)。

如果您有安全解決方案，並有興趣成為 Security Hub CSPM 合作夥伴，請傳送電子郵件至 <securityhub-partners@amazon.com>。如需詳細資訊，請參閱 [合作夥伴整合指南](#)。

與 Security Hub CSPM 的第三方整合概觀

下表提供第三方整合的概觀，可將問題清單傳送至 Security Hub CSPM 或從 Security Hub CSPM 接收問題清單。

整合	Direction	ARN (如適用)
3CORESec – 3CORESec NTA	傳送問題清單	arn:aws:securityhub:<REGION>::product/3coresec/3coresec
Alert Logic – SIEMless Threat Management	傳送問題清單	arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	傳送問題清單	arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity
Aqua Security – Kube-bench	傳送問題清單	arn:aws:securityhub:<REGION>::product/

整合	Direction	ARN (如適用)
		aqua-security/kube-bench
Armor – Armor Anywhere	傳送問題清單	arn:aws:securityhub:<REGION>:679703615338:product/armor-defense/armoranywhere
AttackIQ – AttackIQ	傳送問題清單	arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	傳送問題清單	arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurity-guardian
BigID – BigID Enterprise	傳送問題清單	arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	傳送問題清單	arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws
Check Point – CloudGuard IaaS	傳送問題清單	arn:aws:securityhub:<REGION>:758245563457:product/check-point/cloudguard-iaas

整合	Direction	ARN (如適用)
Check Point – CloudGuard Posture Management	傳送問題清單	arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc
Claroty – xDome	傳送問題清單	arn:aws:securityhub:<REGION>::product/claroty/xdome
Cloud Storage Security – Antivirus for Amazon S3	傳送問題清單	arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3
Contrast Security	傳送問題清單	arn:aws:securityhub:<REGION>::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	傳送問題清單	arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon
CyberArk – Privileged Threat Analytics	傳送問題清單	arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta
Data Theorem – Data Theorem	傳送問題清單	arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure

整合	Direction	ARN (如適用)
Drata	傳送問題清單	arn:aws:securityhub: <REGION>::product/drata/drata-integration
Forcepoint – Forcepoint CASB	傳送問題清單	arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb
Forcepoint – Forcepoint Cloud Security Gateway	傳送問題清單	arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway
Forcepoint – Forcepoint DLP	傳送問題清單	arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp
Forcepoint – Forcepoint NGFW	傳送問題清單	arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw
Fugue – Fugue	傳送問題清單	arn:aws:securityhub: <REGION>::product/fugue/fugue

整合	Direction	ARN (如適用)
Guardicore – Centra 4.0	傳送問題清單	arn:aws:securityhub:<REGION>::product/guardicore/guardicore
HackerOne – Vulnerability Intelligence	傳送問題清單	arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence
JFrog – Xray	傳送問題清單	arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray
Juniper Networks – vSRX Next Generation Firewall	傳送問題清單	arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	傳送問題清單	arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer
Lacework – Lacework	傳送問題清單	arn:aws:securityhub:<REGION>::product/lacework/lacework
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	傳送問題清單	arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws

整合	Direction	ARN (如適用)
NETSCOUT – NETSCOUT Cyber Investigator	傳送問題清單	arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator
Orca Cloud Security Platform	傳送問題清單	arn:aws:securityhub: <REGION>::product/orca-security/orca-security
Palo Alto Networks – Prisma Cloud Compute	傳送問題清單	arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise
Palo Alto Networks – Prisma Cloud Enterprise	傳送問題清單	arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock
Plerion – Cloud Security Platform	傳送問題清單	arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform
Prowler – Prowler	傳送問題清單	arn:aws:securityhub: <REGION>::product/prowler/prowler
Qualys – Vulnerability Management	傳送問題清單	arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm

整合	Direction	ARN (如適用)
Rapid7 – InsightVM	傳送問題清單	arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm
SentinelOne – SentinelOne	傳送問題清單	arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection
Snyk	傳送問題清單	arn:aws:securityhub: <region>::product/snyk/snyk
Sonrai Security – Sonrai Dig	傳送問題清單	arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig
Sophos – Server Protection	傳送問題清單	arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection
StackRox – StackRox Kubernetes Security	傳送問題清單	arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	傳送問題清單	arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda

整合	Direction	ARN (如適用)
Symantec – Cloud Workload Protection	傳送問題清單	arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp
Tenable – Tenable.io	傳送問題清單	arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io
Trend Micro – Cloud One	傳送問題清單	arn:aws:securityhub: <REGION>::product/trend-micro/cloud-one
Vectra – Cognito Detect	傳送問題清單	arn:aws:securityhub: <REGION>:978576646331:product/vectra-ai/cognito-detect
Wiz	傳送問題清單	arn:aws:securityhub: <REGION>::product/wiz-security/wiz-security
Atlassian - Jira Service Management	接收和更新問題清單	不適用
Atlassian - Jira Service Management Cloud	接收和更新問題清單	不適用
Atlassian – Opsgenie	接收問題清單	不適用
Dynatrace	接收問題清單	不適用
Elastic	接收問題清單	不適用

整合	Direction	ARN (如適用)
Fortinet – FortiCNP	接收問題清單	不適用
IBM – QRadar	接收問題清單	不適用
Logz.io Cloud SIEM	接收問題清單	不適用
MetricStream	接收問題清單	不適用
MicroFocus – MicroFocus Arcsight	接收問題清單	不適用
New Relic Vulnerability Management	接收問題清單	不適用
PagerDuty – PagerDuty	接收問題清單	不適用
Palo Alto Networks – Cortex XSOAR	接收問題清單	不適用
Palo Alto Networks – VM-Series	接收問題清單	不適用
Rackspace Technology – Cloud Native Security	接收問題清單	不適用
Rapid7 – InsightConnect	接收問題清單	不適用
RSA – RSA Archer	接收問題清單	不適用
ServiceNow – ITSM	接收和更新問題清單	不適用
Slack – Slack	接收問題清單	不適用
Splunk – Splunk Enterprise	接收問題清單	不適用
Splunk – Splunk Phantom	接收問題清單	不適用
ThreatModeler	接收問題清單	不適用

整合	Direction	ARN (如適用)
Trellix – Trellix Helix	接收問題清單	不適用
Caveonix – Caveonix Cloud	傳送和接收問題清單	arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud
Cloud Custodian – Cloud Custodian	傳送和接收問題清單	arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian
DisruptOps, Inc. – DisruptOPS	傳送和接收問題清單	arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops
Kion	傳送和接收問題清單	arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio
Turbot – Turbot	傳送和接收問題清單	arn:aws:securityhub:<REGION>:453761072151:product/turbot/turbot

將問題清單傳送至 Security Hub CSPM 的第三方整合

下列第三方合作夥伴產品整合可將問題清單傳送至 Security Hub CSPM。Security Hub CSPM 會將問題清單轉換為[AWS 安全問題清單格式](#)。

3CORESec – 3CORESec NTA

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/3coresec/3coresec

3CORESec 為內部部署和 AWS 系統提供受管偵測服務。它們與 Security Hub CSPM 的整合允許對惡意軟體、權限提升、橫向移動和不當網路分割等威脅的可見性。

[產品連結](#)

[合作夥伴文件](#)

Alert Logic – SIEMless Threat Management

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement

取得正確的涵蓋範圍：漏洞和資產可見性、威脅偵測和事件管理 AWS WAF，以及指派的 SOC 分析師選項。

[產品連結](#)

[合作夥伴文件](#)

Aqua Security – Aqua Cloud Native Security Platform

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity

Aqua Cloud Native Security Platform (CSP) 提供容器型和無伺服器應用程式的完整生命週期安全性，從 CI/CD 管道到執行期生產環境。

[產品連結](#)

[合作夥伴文件](#)

Aqua Security – Kube-bench

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench

Kube-bench 是一種開放原始碼工具，可針對您的環境執行網際網路安全中心 (CIS) Kubernetes Benchmark。

[產品連結](#)

[合作夥伴文件](#)

Armor – Armor Anywhere

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere

Armor Anywhere 為 提供受管安全性和合規性 AWS。

[產品連結](#)

[合作夥伴文件](#)

AttackIQ – AttackIQ

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:product/attackiq/attackiq-platform

AttackIQ Platform 模擬與 MITRE ATT&CK Framework 一致的真實對手行為，以協助驗證和改善您的整體安全狀態。

[產品連結](#)

[合作夥伴文件](#)

Barracuda Networks – Cloud Security Guardian

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian

Barracuda Cloud Security Sentry 協助組織在公有雲端中建置應用程式和移動工作負載時保持安全。

[AWS Marketplace 連結](#)

[產品連結](#)

BigID – BigID Enterprise

整合類型：傳送

產品 ARN : `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

BigID Enterprise Privacy Management Platform 可協助公司管理及保護所有系統的敏感資料 (PII)。

[產品連結](#)

[合作夥伴文件](#)

Blue Hexagon – Blue Hexagon 適用於 AWS

整合類型：傳送

產品 ARN : `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon 是即時威脅偵測平台。它使用深度學習原則來偵測已知和未知的威脅，包括惡意軟體和網路異常。

[AWS Marketplace 連結](#)

[合作夥伴文件](#)

Check Point – CloudGuard IaaS

整合類型：傳送

產品 ARN : `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard 輕鬆將全面的威脅預防安全性擴展到 ， AWS 同時保護雲端中的資產。

[產品連結](#)

[合作夥伴文件](#)

Check Point – CloudGuard Posture Management

整合類型：傳送

產品 ARN : `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

一種 SaaS 平台，可提供可驗證的雲端網路安全、進階 IAM 保護，以及全面的合規和管理。

[產品連結](#)

[合作夥伴文件](#)

Claroty – xDome

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/claroty/xdome

Claroty xDome 協助組織保護其在工業 (OT)、醫療保健 (IoMT) 和企業 (IoT) 環境中延伸物聯網 (XIoT) 的網路實體系統。

[產品連結](#)

[合作夥伴文件](#)

Cloud Storage Security – Antivirus for Amazon S3

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3

Cloud Storage Security 為 Amazon S3 物件提供雲端原生反惡意軟體和防毒掃描。

Antivirus for Amazon S3 提供 Amazon S3 中物件和檔案的即時和排程掃描，以找出惡意軟體和威脅。它可為問題和受感染的檔案提供可見性和修復。

[產品連結](#)

[合作夥伴文件](#)

Contrast Security – Contrast Assess

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/contrast-security/security-assess

Contrast Security Contrast Assess 是一種 IAST 工具，可在 Web 應用程式、APIs 和微服務中提供即時漏洞偵測。與 Security Hub CSPM Contrast Assess 整合，可協助為所有工作負載提供集中式可見性和回應。

[產品連結](#)[合作夥伴文件](#)

CrowdStrike – CrowdStrike Falcon

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon

CrowdStrike Falcon 單一輕量型感應器整合新一代防毒、端點偵測和回應，以及全年無休的雲端受管搜尋。

[AWS Marketplace 連結](#)[合作夥伴文件](#)

CyberArk – Privileged Threat Analytics

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta

Privileged Threat Analytics 收集、偵測、提醒和回應特殊權限帳戶的高風險活動和行為，以包含進行中攻擊。

[產品連結](#)[合作夥伴文件](#)

Data Theorem – Data Theorem

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure

Data Theorem 會持續掃描 Web 應用程式、APIs 和雲端資源，以搜尋安全漏洞和資料隱私權漏洞，以防止 AppSec 資料外洩。

[產品連結](#)

[合作夥伴文件](#)

Drata

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/drata/drata-integration

Drata 是一種合規自動化平台，可協助您實現和維護各種架構的合規性，例如 SOC2、ISO 和 GDPR。Drata 與 Security Hub CSPM 之間的整合可協助您將安全調查結果集中在一個位置。

[AWS Marketplace 連結](#)

[合作夥伴文件](#)

Forcepoint – Forcepoint CASB

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb

Forcepoint CASB 可讓您探索雲端應用程式的使用方式、分析風險，並針對 SaaS 和自訂應用程式強制執行適當的控制。

[產品連結](#)

[合作夥伴文件](#)

Forcepoint – Forcepoint Cloud Security Gateway

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway

Forcepoint Cloud Security Gateway 是一種融合式雲端安全服務，可隨時隨地為使用者和資料提供可見性、控制和威脅防護。

[產品連結](#)

[合作夥伴文件](#)

Forcepoint – Forcepoint DLP

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp

Forcepoint DLP 解決以人為本的風險，在您的人員工作和資料所在的任何地方都具有可見性和控制性。

[產品連結](#)

[合作夥伴文件](#)

Forcepoint – Forcepoint NGFW

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw

Forcepoint NGFW 可讓您使用管理網路和回應威脅所需的可擴展性、保護和洞見，將 AWS 環境連接到企業網路。

[產品連結](#)

[合作夥伴文件](#)

Fugue – Fugue

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/fugue/fugue

Fugue 是一種無代理程式、可擴展的雲端原生平台，可使用相同的政策自動驗證infrastructure-as-code和雲端執行期環境。

[產品連結](#)

[合作夥伴文件](#)

Guardicore – Centra 4.0

整合類型：傳送

產品 ARN : `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra 為現代資料中心和雲端中的工作負載提供流程視覺化、微分段和違規偵測。

[產品連結](#)

[合作夥伴文件](#)

HackerOne – Vulnerability Intelligence

整合類型：傳送

產品 ARN : `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

HackerOne 平台與全球駭客社群合作，發現最相關的安全問題。Vulnerability Intelligence 可讓您的組織超越自動化掃描。它會分享HackerOne道德駭客已驗證並提供重現步驟的漏洞。

[AWS 市集連結](#)

[合作夥伴文件](#)

JFrog – Xray

整合類型：傳送

產品 ARN : `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray 是一種通用應用程式安全軟體合成分析 (SCA) 工具，可持續掃描二進位檔是否有授權合規和安全漏洞，以便您可以執行安全的軟體供應鏈。

[AWS Marketplace 連結](#)

[合作夥伴文件](#)

Juniper Networks – vSRX Next Generation Firewall

整合類型：傳送

產品 ARN : `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks' vSRX Virtual Next Generation Firewall 提供完整的雲端型虛擬防火牆，具有進階安全性、安全的 SD-WAN、強大的聯網和內建自動化。

[AWS Marketplace 連結](#)

[合作夥伴文件](#)

[產品連結](#)

k9 Security – Access Analyzer

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer

k9 Security 當 AWS Identity and Access Management 您的帳戶發生重要的存取變更時，會通知您。使用 k9 Security，您可以了解使用者和 IAM 角色對關鍵 AWS 服務和資料的存取。

k9 Security 專為持續交付而建置，可讓您使用可行的存取稽核和 Terraform 的 AWS CDK 簡單政策自動化來操作 IAM。

[產品連結](#)

[合作夥伴文件](#)

Lacework – Lacework

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/lacework/lacework

Lacework 是雲端的資料驅動型安全平台。Restorework Cloud Security Platform 可大規模自動化雲端安全性，讓您可以快速且安全地進行創新。

[產品連結](#)

[合作夥伴文件](#)

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws

McAfee MVISION Cloud Native Application Protection Platform (CNAPP) 為您的 AWS 環境提供雲端安全狀態管理 (CSPM) 和雲端工作負載保護平台 (CWPP)。

[產品連結](#)

[合作夥伴文件](#)

NETSCOUT – NETSCOUT Cyber Investigator

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator

NETSCOUT Cyber Investigator 是全企業的網路威脅、風險調查和鑑識分析平台，有助於降低網路威脅對企業的影響。

[產品連結](#)

[合作夥伴文件](#)

Orca Cloud Security Platform

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/orca-security/orca-security

Orca Cloud Security Platform 可識別、排定優先順序，並修復整個雲端資產的風險和合規問題。無 Orca's 代理程式、AI 驅動的平台提供全面涵蓋範圍，可偵測漏洞、設定錯誤、橫向移動、API 風險、敏感資料、異常事件和行為，以及過度寬鬆的身分。

Orca 與 Security Hub CSPM 整合，將深度雲端安全遙測帶入 Security Hub CSPM。Orca 使用其 SideScanning 技術，優先考慮跨雲端基礎設施、工作負載、應用程式、資料、APIs、身分等的風險。

[產品連結](#)

[合作夥伴文件](#)

Palo Alto Networks – Prisma Cloud Compute

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise

Prisma Cloud Compute 是一種雲端原生網路安全平台，可保護 VMs、容器和無伺服器平台。

[產品連結](#)[合作夥伴文件](#)

Palo Alto Networks – Prisma Cloud Enterprise

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock

透過雲端安全分析、進階威脅偵測和合規監控來保護您的 AWS 部署。

[產品連結](#)[合作夥伴文件](#)

Plerion – Cloud Security Platform

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform

Plerion 是一種雲端安全平台，具有獨特的威脅導向、風險驅動的方法，可在您的工作負載中提供預防性、偵測性和修正性動作。Plerion 與 Security Hub CSPM 之間的整合，可讓客戶集中並針對其安全調查結果採取行動。

[AWS Marketplace 連結](#)[合作夥伴文件](#)

Prowler – Prowler

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/prowler/prowler

Prowler 是一種開放原始碼安全工具，可執行與安全最佳實務、強化和持續監控相關的 AWS 檢查。

[產品連結](#)[合作夥伴文件](#)

Qualys – Vulnerability Management

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm

Qualys Vulnerability Management (VM) 會持續掃描並識別漏洞，保護您的資產。

[產品連結](#)

[合作夥伴文件](#)

Rapid7 – InsightVM

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm

Rapid7 InsightVM 為現代環境提供漏洞管理，讓您有效率地尋找、排定優先順序並修復漏洞。

[產品連結](#)

[合作夥伴文件](#)

SentinelOne – SentinelOne

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection

SentinelOne 是一種自動延伸偵測和回應 (XDR) 平台，包含跨端點、容器、雲端工作負載和 IoT 裝置進行 AI 支援的預防、偵測、回應和狩獵。

[AWS Marketplace 連結](#)

[產品連結](#)

Snyk

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/snyk/snyk

Snyk 提供安全平台，可掃描應用程式元件在 上執行的工作負載中是否有安全風險 AWS。這些風險會以調查結果的形式傳送到 Security Hub CSPM，協助開發人員和安全團隊將它們及其其餘 AWS 安全性調查結果視覺化並排定優先順序。

[AWS Marketplace 連結](#)

[合作夥伴文件](#)

Sonrai Security – Sonrai Dig

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig

Sonrai Dig 會監控和修復雲端設定錯誤和政策違規，因此您可以改善安全性和合規狀態。

[產品連結](#)

[合作夥伴文件](#)

Sophos – Server Protection

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection

Sophos Server Protection 使用全面的defense-in-depth技術，保護組織核心的關鍵應用程式和資料。

[產品連結](#)

StackRox – StackRox Kubernetes Security

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security

StackRox 在整個容器生命週期中強制執行合規和安全政策，協助企業大規模保護其容器和 Kubernetes 部署：建置、部署和執行。

[產品連結](#)

[合作夥伴文件](#)

Sumo Logic – Machine Data Analytics

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda

Sumo Logic 是一種安全的機器資料分析平台，可讓開發和安全營運團隊建置、執行和保護其 AWS 應用程式。

[產品連結](#)

[合作夥伴文件](#)

Symantec – Cloud Workload Protection

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp

Cloud Workload Protection 透過反惡意軟體、入侵預防和檔案完整性監控，為您的 Amazon EC2 執行個體提供完整的保護。

[產品連結](#)

[合作夥伴文件](#)

Tenable – Tenable.io

整合類型：傳送

產品 ARN：arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io

準確識別、調查和排定漏洞的優先順序。在雲端中受管。

[產品連結](#)

[合作夥伴文件](#)

Trend Micro – Cloud One

整合類型：傳送

產品 ARN : `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One 會在正確的時間和位置提供正確的安全性資訊給團隊。此整合會即時將安全性調查結果傳送至 Security Hub CSPM，以增強 Security Hub CSPM 中 AWS 資源和Trend Micro Cloud One事件詳細資訊的可見性。

[AWS Marketplace 連結](#)

[合作夥伴文件](#)

Vectra – Cognito Detect

整合類型：傳送

產品 ARN : `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra 正在透過應用進階 AI 來偵測和回應隱藏的網路攻擊者，在它們可以竊取或造成損害之前，轉換網路安全。

[AWS Marketplace 連結](#)

[合作夥伴文件](#)

Wiz – Wiz Security

整合類型：傳送

產品 ARN : `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz 會持續分析您、使用者和工作負載的組態、漏洞、網路 AWS 帳戶、IAM 設定、秘密等，以探索代表實際風險的關鍵問題。整合 Wiz 與 Security Hub CSPM，以視覺化方式呈現和回應 Wiz 從 Security Hub CSPM 主控台偵測到的問題。

[AWS Marketplace 連結](#)

[合作夥伴文件](#)

從 Security Hub CSPM 接收問題清單的第三方整合

下列第三方合作夥伴產品整合可以從 Security Hub CSPM 接收問題清單。如前所述，產品也可能更新問題清單。在這種情況下，您對合作夥伴產品的問題清單所做的更新也會反映在 Security Hub CSPM 中。

Atlassian - Jira Service Management

整合類型：接收和更新

AWS Service Management Connector 的 會將問題清單從 Security Hub CSPM Jira傳送至 Jira。問題會根據Jira問題清單建立。當Jira問題更新時，對應的調查結果會在 Security Hub CSPM 中更新。

整合僅支援 Jira Server 和 Jira Data Center。

如需整合及其運作方式的概觀，請觀看影片 [AWS Security Hub CSPM – 與 的雙向整合Atlassian Jira Service Management](#)。

[產品連結](#)

[合作夥伴文件](#)

Atlassian - Jira Service Management Cloud

整合類型：接收和更新

Jira Service Management Cloud 是 Jira Service Management 的雲端元件。

AWS Service Management Connector 的 Jira會將問題清單從 Security Hub CSPM 傳送至 Jira。問題清單會觸發在 中建立問題Jira Service Management Cloud。當您更新 中的這些問題時Jira Service Management Cloud，對應的調查結果也會在 Security Hub CSPM 中更新。

[產品連結](#)

[合作夥伴文件](#)

Atlassian – Opsgenie

整合類型：接收

Opsgenie 是一種現代化的事件管理解決方案，用於操作全年無休的服務，讓開發和營運團隊能夠規劃服務中斷，並在事件期間保持控制。

與 Security Hub CSPM 整合可確保關鍵任務安全相關事件路由至適當的團隊，以立即解決。

[產品連結](#)

[合作夥伴文件](#)

Dynatrace

整合類型：接收

與 Security Hub CSPM 的 Dynatrace 整合有助於統一、視覺化和自動化跨工具和環境的安全調查結果。將 Dynatrace 執行時間內容新增至安全調查結果可讓您更智慧地排定優先順序、協助減少警示的雜訊，並讓您的 DevSecOps 團隊專注於有效解決影響生產環境和應用程式的關鍵問題。

[產品連結](#)

[合作夥伴文件](#)

Elastic

整合類型：接收

Elastic 為安全性、可觀測性和搜尋建置以搜尋為基礎的解決方案。使用 Security Hub CSPM 整合，以程式設計方式從 Security Hub CSPM Elastic 擷取問題清單和洞見，標準化它們以進行相互關聯和分析，並在 中提供統一的儀表板和偵測 Elastic Security，從而加快分類和調查速度，而無需部署代理程式。

[產品連結](#)

[合作夥伴文件](#)

Fortinet – FortiCNP

整合類型：接收

FortiCNP 是一種雲端原生保護產品，可將安全調查結果彙總為可行的洞見，並根據風險分數排定安全洞見的優先順序，以減少警示疲勞並加速修復。

[AWS Marketplace 連結](#)

[合作夥伴文件](#)

IBM – QRadar

整合類型：接收

IBM QRadar SIEM 讓安全團隊能夠快速準確地偵測、排定優先順序、調查和回應威脅。

[產品連結](#)

[合作夥伴文件](#)

Logz.io Cloud SIEM

整合類型：接收

Logz.io 是 的提供者Cloud SIEM，可提供日誌和事件資料的進階相互關聯，以協助安全團隊即時偵測、分析和回應安全威脅。

[產品連結](#)

[合作夥伴文件](#)

MetricStream – CyberGRC

整合類型：接收

MetricStream CyberGRC 可協助您管理、衡量和降低網路安全風險。透過接收 Security Hub CSPM 調查結果，CyberGRC 提供這些風險的更多可見性，因此您可以優先考慮網路安全投資並遵循 IT 政策。

[AWS Marketplace 連結](#)

[產品連結](#)

MicroFocus – MicroFocus Arcsight

整合類型：接收

ArcSight 即時加速有效的威脅偵測和回應，整合事件相互關聯，以及受監督和非監督的分析與回應自動化和協同運作。

[產品連結](#)

[合作夥伴文件](#)

New Relic Vulnerability Management

整合類型：接收

New Relic Vulnerability Management 會從 Security Hub CSPM 接收安全調查結果，因此您可以在堆疊的內容中取得安全性與效能遙測的集中檢視。

[AWS Marketplace 連結](#)

[合作夥伴文件](#)

PagerDuty – PagerDuty

整合類型：接收

PagerDuty 數位操作管理平台可讓團隊透過自動將任何訊號轉換為正確的洞見和動作，主動緩解影響客戶的問題。

AWS 使用者可以使用PagerDuty一組 AWS 整合，放心地擴展其 AWS 和混合環境。

與 Security Hub CSPM 彙總和組織的安全提醒結合時， PagerDuty可讓團隊自動化其威脅回應程序，並快速設定自訂動作以防止潛在問題。

PagerDuty 正在進行雲端遷移專案的使用者可以快速移動，同時減少整個遷移生命週期中發生的問題的影響。

[產品連結](#)

[合作夥伴文件](#)

Palo Alto Networks – Cortex XSOAR

整合類型：接收

Cortex XSOAR 是一種安全協調、自動化和回應 (SOAR) 平台，可與您的整個安全產品堆疊整合，以加速事件回應和安全操作。

[產品連結](#)

[合作夥伴文件](#)

Palo Alto Networks – VM-Series

整合類型：接收

Palo Alto VM-Series 與 Security Hub CSPM 整合會收集威脅情報，並將其傳送至VM-Series新一代防火牆，做為封鎖惡意 IP 地址活動的自動安全政策更新。

[產品連結](#)

[合作夥伴文件](#)

Rackspace Technology – Cloud Native Security

整合類型：接收

Rackspace Technology 除了原生安全產品之外，還提供受管 AWS 安全服務，以透過 Rackspace SOC、進階分析和威脅修復進行全年無休的監控。

[產品連結](#)

Rapid7 – InsightConnect

整合類型：接收

Rapid7 InsightConnect 是一種安全協同運作和自動化解決方案，可讓您的團隊最佳化 SOC 操作，幾乎不需要程式碼。

[產品連結](#)

[合作夥伴文件](#)

RSA – RSA Archer

整合類型：接收

RSA Archer IT 和安全風險管理可讓您判斷哪些資產對您的業務至關重要、建立和傳達安全政策和標準、偵測和回應攻擊、識別和修復安全缺陷，以及建立明確的 IT 風險管理最佳實務。

[產品連結](#)

[合作夥伴文件](#)

ServiceNow – ITSM

整合類型：接收和更新

與 Security Hub CSPM 的 ServiceNow 整合允許在 中檢視來自 Security Hub CSPM 的安全調查結果 ServiceNow ITSM。您也可以設定 ServiceNow 在收到 Security Hub CSPM 的問題清單時，自動建立事件或問題。

這些事件和問題的任何更新都會對 Security Hub CSPM 中的調查結果進行更新。

如需整合及其運作方式的概觀，請觀看視訊 [AWS Security Hub CSPM - 雙向整合。ServiceNow ITSM](#)

[產品連結](#)[合作夥伴文件](#)

Slack – Slack

整合類型：接收

Slack 是商業技術堆疊的一層，將人員、資料和應用程式集合在一起。大家可在一個位置有效率地一起工作、尋找重要資訊，以及存取數十萬種關鍵應用程式和服務，將工作做到最好。

[產品連結](#)[合作夥伴文件](#)

Splunk – Splunk Enterprise

整合類型：接收

Splunk 使用 Amazon CloudWatch Events 做為 Security Hub CSPM 調查結果的取用者。將您的資料傳送至 Splunk 以進行進階安全分析和 SIEM。

[產品連結](#)[合作夥伴文件](#)

Splunk – Splunk Phantom

整合類型：接收

使用適用於 AWS Security Hub CSPM Splunk Phantom 的應用程式，問題清單會傳送至 Phantom，以便透過其他威脅情報資訊自動擴充內容，或執行自動回應動作。

[產品連結](#)[合作夥伴文件](#)

ThreatModeler

整合類型：接收

ThreatModeler 是一種自動化威脅建模解決方案，可保護和擴展企業軟體和雲端開發生命週期。

[產品連結](#)

[合作夥伴文件](#)

Trellix – Trellix Helix

整合類型：接收

Trellix Helix 是一種雲端託管的安全操作平台，可讓組織控制從提醒到修正的任何事件。

[產品連結](#)

[合作夥伴文件](#)

將問題清單傳送至 Security Hub CSPM 並從中接收問題清單的第三方整合

下列第三方合作夥伴產品整合可以將問題清單傳送至 Security Hub CSPM 並從中接收問題清單。

Caveonix – Caveonix Cloud

整合類型：傳送和接收

產品 ARN：arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud

採用 Caveonix AI 技術的平台可自動化混合雲端中的可見性、評估和緩解措施，涵蓋雲端原生服務、VMs 和容器。與 AWS Security Hub CSPM 整合，Caveonix 會合併 AWS 資料和進階分析，以深入了解安全提醒和合規。

[AWS Marketplace 連結](#)

[合作夥伴文件](#)

Cloud Custodian – Cloud Custodian

整合類型：傳送和接收

產品 ARN：arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian

Cloud Custodian 讓使用者能夠在雲端中妥善管理。簡單 YAML DSL 允許輕鬆定義的規則，以啟用安全且成本最佳化且受管良好的雲端基礎設施。

[產品連結](#)

[合作夥伴文件](#)

DisruptOps, Inc. – DisruptOPS

整合類型：傳送和接收

產品 ARN：arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops

DisruptOps 安全操作平台透過使用自動化護欄，協助組織在您的雲端中維護最佳安全實務。

[產品連結](#)

[合作夥伴文件](#)

Kion

整合類型：傳送和接收

產品 ARN：arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio

Kion (先前為 cloudtamer.io) 是 的完整雲端控管解決方案 AWS。Kion 可讓利益相關者了解雲端操作，並協助雲端使用者管理帳戶、控制預算和成本，並確保持續合規。

[產品連結](#)

[合作夥伴文件](#)

Turbot – Turbot

整合類型：傳送和接收

產品 ARN：arn:aws:securityhub:<REGION>::product/turbot/turbot

Turbot 確保您的雲端基礎設施安全、合規、可擴展且成本最佳化。

[產品連結](#)

[合作夥伴文件](#)

將 Security Hub CSPM 與自訂產品整合

除了整合 AWS 服務和第三方產品所產生的問題清單之外，AWS Security Hub CSPM 還可以使用其他自訂安全產品所產生的問題清單。

您可以使用 Security Hub CSPM API [BatchImportFindings](#) 的操作，將這些調查結果傳送至 Security Hub CSPM。您可以使用相同的操作來更新您已傳送至 Security Hub CSPM 的自訂產品的問題清單。

設定自訂整合時，請使用 Security Hub CSPM 合作夥伴整合指南中提供[的指引和檢查清單](#)。

自訂產品整合的需求和建議

您必須先啟用 Security Hub CSPM，才能成功叫用 [BatchImportFindings](#) API 操作。

您還必須使用 提供自訂產品的調查結果詳細資訊[the section called “問題清單格式：ASFF”](#)。檢閱自訂產品整合的下列需求和建議：

設定產品 ARN

當您啟用 Security Hub CSPM 時，您目前的帳戶中會產生 Security Hub CSPM 的預設產品 Amazon Resource Name (ARN)。

此產品 ARN 的格式如下：arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default。例如 arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default。

叫用 BatchImportFindings API 操作時，請使用此產品 ARN 做為 [ProductArn](#) 屬性的值。

設定公司和產品名稱

您可以使用 BatchImportFindings 為將問題清單傳送到 Security Hub CSPM 的自訂整合設定偏好的公司名稱和產品名稱。

您指定的名稱會取代預先設定的公司名稱和產品名稱，分別稱為個人名稱和預設名稱，並會出現在 Security Hub CSPM 主控台和每個調查結果的 JSON 中。請參閱 [用於尋找供應商的 BatchImportFindings](#)。

設定問題清單 ID

您必須使用 [Id](#) 屬性提供、管理和增加您自己的問題清單 ID。

每個新問題清單都應具有唯一的問題清單 ID。如果自訂產品使用相同的問題清單 ID 傳送多個問題清單，Security Hub CSPM 只會處理第一個問題清單。

設定帳戶 ID

您必須使用 [AwsAccountId](#) 屬性指定自己的帳戶 ID。

設定建立日期和更新日期

您必須針對 [CreatedAt](#) 和 [UpdatedAt](#) 屬性提供自己的時間戳記。

從自訂產品更新問題清單

除了從自訂產品傳送新的問題清單之外，您也可以使用 [BatchImportFindings](#) API 操作更新自訂產品的現有問題清單。

如要更新現有問題清單，請使用現有的問題清單 ID (透過 [Id](#) 屬性)。在請求中適當更新資訊來重新傳送完整的問題清單，包括修改後的 [UpdatedAt](#) 時間戳記。

自訂整合範例

您可以使用下列範例自訂產品整合做為建立自訂解決方案的指南：

從Chef InSpec掃描將問題清單傳送至 Security Hub CSPM

您可以建立執行[Chef InSpec](#)合規掃描的 CloudFormation 範本，然後將問題清單傳送至 Security Hub CSPM。

如需詳細資訊，請參閱[使用 Chef InSpec和 AWS Security Hub CSPM 進行持續合規監控](#)。

將偵測到的容器漏洞Trivy傳送至 Security Hub CSPM

您可以建立 CloudFormation 範本，使用 [AquaSecurity Trivy](#) 掃描容器是否有漏洞，然後將這些漏洞調查結果傳送至 Security Hub CSPM。

如需詳細資訊，請參閱[如何使用 Trivy和AWS Security Hub CSPM 建置容器漏洞掃描的 CI/CD 管道](#)。

在 Security Hub CSPM 中建立和更新問題清單

在 AWS Security Hub CSPM 中，問題清單是安全檢查或安全相關偵測的可觀察記錄。問題清單可能來自下列其中一個來源：

- Security Hub CSPM 中控制項的安全檢查。
- 與另一個的整合 AWS 服務。
- 與第三方產品的整合。
- 自訂整合。

Security Hub CSPM 會將所有來源的問題清單標準化為稱為AWS 安全問題清單格式 (ASFF) 的標準語法和格式。如需此格式的詳細資訊，包括個別 ASFF 欄位的說明，請參閱 [AWS 安全調查結果格式](#)

(ASFF)。如果您啟用跨區域彙總，Security Hub CSPM 也會自動將新的和更新的調查結果從所有連結的區域彙總到您指定的彙總區域。如需詳細資訊，請參閱[了解 Security Hub CSPM 中的跨區域彙總](#)。

建立問題清單之後，可以更新，如下所示：

- 問題清單提供者可以使用 Security Hub CSPM API [BatchImportFindings](#) 的操作來更新問題清單的一般資訊。問題清單提供者只能更新其建立的問題清單。
- 客戶可以使用 Security Hub CSPM 主控台或 Security Hub CSPM API [BatchUpdateFindings](#) 的操作來更新調查結果調查的狀態。SIEM、票證、事件管理、SOAR 或其他類型的工具也可以代表客戶使用 [BatchUpdateFindings](#) 此操作。

為了減少問題清單雜訊並簡化個別問題清單的追蹤和分析，Security Hub CSPM 會自動刪除最近尚未更新的問題清單。Security Hub CSPM 執行此作業的時間取決於問題清單是作用中還是封存：

- 作用中問題清單是記錄狀態 (RecordState) 為 的問題清單 ACTIVE。Security Hub CSPM 會儲存作用中的問題清單 90 天。如果作用中的問題清單已有 90 天未更新，則會過期，且 Security Hub CSPM 會將其永久刪除。
- 封存的問題清單是記錄狀態 (RecordState) 為 的問題清單 ARCHIVED。Security Hub CSPM 會將封存的問題清單存放 30 天。如果封存的問題清單已有 30 天未更新，則會過期，且 Security Hub CSPM 會將其永久刪除。

對於控制項問題清單，這是 Security Hub CSPM 從控制項安全檢查產生的問題清單，Security Hub CSPM 會根據問題清單 UpdatedAt 欄位的值來判斷問題清單是否已過期。如果作用中問題清單的這個值超過 90 天，Security Hub CSPM 會永久刪除問題清單。如果封存的問題清單超過 30 天，Security Hub CSPM 會永久刪除問題清單。

對於所有其他類型的问题清單，Security Hub CSPM 會根據問題清單的 ProcessedAt 和 UpdatedAt 欄位的值來判斷問題清單是否已過期。Security Hub CSPM 會比較這些欄位的值，並判斷哪個欄位較新。如果作用中問題清單的最近值超過 90 天，Security Hub CSPM 會永久刪除問題清單。如果封存問題清單的最近值超過 30 天，Security Hub CSPM 會永久刪除問題清單。問題清單提供者可以使用 Security Hub CSPM API [BatchImportFindings](#) 的操作來變更一或多個問題清單 UpdatedAt 欄位的值。

如需長期保留問題清單，您可以將問題清單匯出至 S3 儲存貯體。您可以搭配 Amazon EventBridge 規則使用自訂動作來執行此操作。如需詳細資訊，請參閱[使用 EventBridge 進行自動回應和修復](#)。

主題

- [用於尋找供應商的 BatchImportFindings](#)

- [客戶的 BatchUpdateFindings](#)
- [在 Security Hub CSPM 中檢閱問題清單詳細資訊和歷史記錄](#)
- [在 Security Hub CSPM 中篩選問題清單](#)
- [在 Security Hub CSPM 中分組問題清單](#)
- [在 Security Hub CSPM 中設定問題清單的工作流程狀態](#)
- [將問題清單傳送至自訂 Security Hub CSPM 動作](#)
- [AWS 安全調查結果格式 \(ASFF\)](#)

用於尋找供應商的 BatchImportFindings

尋找提供者可以使用 [BatchImportFindings](#) 操作在 AWS Security Hub CSPM 中建立新的問題清單。他們也可以使用此操作來更新他們建立的問題清單。尋找供應商無法更新他們未建立的問題清單。

客戶、SIEMs、票證、SOAR 和其他類型的工具必須使用 [BatchUpdateFindings](#) 操作，進行與調查結果提供者調查相關的更新。如需詳細資訊，請參閱 [the section called “客戶的 BatchUpdateFindings”](#)。

當 Security Hub CSPM 收到建立或更新問題清單的 BatchImportFindings 請求時，它會自動在 Amazon EventBridge 中產生 Security Hub Findings - Imported 事件。您可以對該事件採取自動動作。如需詳細資訊，請參閱 [the section called “自動化回應和修復”](#)。

使用 BatchImportFindings 的先決條件

BatchImportFindings 必須由下列其中一項呼叫：

- 與調查結果相關聯的帳戶。關聯帳戶的識別符必須符合調查結果的 `AwsAccountId` 屬性值。
- 允許列為官方 Security Hub CSPM 合作夥伴整合的帳戶。

Security Hub CSPM 只能接受已啟用 Security Hub CSPM 的帳戶的問題清單更新。同時也必須啟用問題清單提供者。如果 Security Hub CSPM 已停用，或未啟用調查結果提供者整合，則會在 FailedFindings 清單中傳回調查結果，並顯示 InvalidAccess 錯誤。

決定是要建立或更新問題清單

若要判斷是否要建立或更新問題清單，Security Hub CSPM 會檢查 ID 欄位。如果 ID 不符合現有的調查結果，Security Hub CSPM 會建立新的調查結果。

如果 ID 符合現有的調查結果，Security Hub CSPM 會檢查 UpdatedAt 欄位是否有更新，然後繼續執行如下操作：

- 如果在更新UpdatedAt時符合或發生在現有調查結果UpdatedAt的 之前，Security Hub CSPM 會忽略更新請求。
- 如果更新UpdatedAt發生在現有調查結果UpdatedAt的 之後，Security Hub CSPM 會更新現有調查結果。

使用 尋找更新的限制 **BatchImportFindings**

問題清單提供者無法使用 `BatchImportFindings` 更新現有問題清單的下列屬性：

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Security Hub CSPM 會忽略這些屬性`BatchImportFindings`請求中提供的任何內容。客戶或代表他們的實體（例如票證工具）可以使用 `BatchUpdateFindings` 更新這些屬性。

使用 更新問題清單 `FindingProviderFields`

調查結果提供者也不應該使用 `BatchImportFindings` 來更新 AWS 安全性調查結果格式 (ASFF) 中的下列頂層屬性：

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

反之，問題清單提供者應該使用 [FindingProviderFields](#) 物件來提供這些屬性的值。

範例

```
"FindingProviderFields": {
  "Confidence": 42,
  "Criticality": 99,
  "RelatedFindings": [
```

```
{
  "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
  "Id": "123e4567-e89b-12d3-a456-426655440000"
},
"Severity": {
  "Label": "MEDIUM",
  "Original": "MEDIUM"
},
"Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

對於BatchImportFindings請求，Security Hub CSPM 會處理最上層屬性和 中的值[FindingProviderFields](#)，如下所示。

(偏好) **BatchImportFindings**提供 中屬性的值[FindingProviderFields](#)，但不提供對應頂層屬性的值。

例如，BatchImportFindings提供 FindingProviderFields.Confidence，但不提供 Confidence。這是 BatchImportFindings請求的偏好選項。

Security Hub CSPM 會更新 中屬性的值FindingProviderFields。

只有在 屬性尚未由 更新時，才會將值複寫至頂層屬性BatchUpdateFindings。

BatchImportFindings 提供最上層屬性的值，但不提供 中對應屬性的值[FindingProviderFields](#)。

例如，BatchImportFindings提供 Confidence，但不提供 FindingProviderFields.Confidence。

Security Hub CSPM 使用 值來更新 中的屬性FindingProviderFields。它會覆寫任何現有的值。

只有在 屬性尚未由 更新時，Security Hub CSPM 才會更新最上層屬性BatchUpdateFindings。

BatchImportFindings 在 中提供最上層屬性和對應屬性的值[FindingProviderFields](#)。

例如，同時BatchImportFindings提供 Confidence和 FindingProviderFields.Confidence。

對於新調查結果，Security Hub CSPM 會使用 中的值FindingProviderFields來填入 中最上層屬性和對應的屬性FindingProviderFields。它不使用提供的頂層屬性值。

對於現有的調查結果，Security Hub CSPM 會使用這兩個值。不過，只有在 屬性尚未由 更新時，才會更新頂層屬性值BatchUpdateFindings。

客戶的 BatchUpdateFindings

AWS Security Hub CSPM 客戶和代其行事的實體可以使用 [BatchUpdateFindings](#) 操作，更新從調查結果提供者處理 Security Hub CSPM 調查結果的相關資訊。身為客戶，您可以直接使用此操作。SIEM、票證、事件管理和 SOAR 工具也可以代表客戶使用此操作。

您無法使用 BatchUpdateFindings操作建立新的問題清單。不過，您可以使用它一次更新最多 100 個現有問題清單。在BatchUpdateFindings請求中，您可以指定要更新的調查結果、要更新調查結果 AWS 的安全調查結果格式 (ASFF) 欄位，以及欄位的新值。然後，Security Hub CSPM 會更新請求中指定的問題清單。此程序需要幾分鐘的時間。如果您使用 BatchUpdateFindings操作更新問題清單，您的更新不會影響問題清單UpdatedAt欄位的現有值。

當 Security Hub CSPM 收到更新問題清單的BatchUpdateFindings請求時，它會自動在 Amazon EventBridge 中產生Security Hub Findings – Imported事件。您可以選擇性地使用此事件，對指定的調查結果採取自動動作。如需詳細資訊，請參閱[the section called “自動化回應和修復”](#)。

的可用欄位 BatchUpdateFindings

如果您登入 Security Hub CSPM 管理員帳戶，您可以使用 BatchUpdateFindings 更新管理員帳戶或成員帳戶所產生的問題清單。成員帳戶只能BatchUpdateFindings用來更新其帳戶的調查結果。

客戶可以使用 BatchUpdateFindings更新下列欄位和物件：

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

設定 的存取權 BatchUpdateFindings

您可以設定 AWS Identity and Access Management (IAM) 政策來限制對 的存取BatchUpdateFindings，使用 來更新問題清單欄位和欄位值。

在 陳述式中，BatchUpdateFindings使用下列值來限制對 的存取：

- Action 是 securityhub:BatchUpdateFindings
- Effect 是 Deny
- 對於 Condition，您可以根據下列項目拒絕BatchUpdateFindings請求：
 - 調查結果包含特定欄位。
 - 問題清單包含特定的欄位值。

條件索引鍵

這些是限制存取 的條件金鑰BatchUpdateFindings。

ASFF 欄位

ASFF 欄位的條件索引鍵如下所示：

```
securityhub:ASFFSyntaxPath/<fieldName>
```

<fieldName> 將 取代為 ASFF 欄位。設定對 的存取時BatchUpdateFindings，請在 IAM 政策中包含一或多個特定 ASFF 欄位，而非父層級欄位。例如，若要限制對 Workflow.Status 欄位的存取，您必須在政策 securityhub:ASFFSyntaxPath/Workflow.Status中包含，而不是Workflow父層級欄位。

不允許對欄位進行所有更新

若要防止使用者對特定欄位進行任何更新，請使用下列條件：

```
"Condition": {
    "Null": {
        "securityhub:ASFFSyntaxPath/<fieldName>": "false"
    }
}
```

例如，下列陳述式指出 BatchUpdateFindings 無法用來更新問題清單 Workflow.Status 的欄位。

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "Null": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
    }
  }
}
```

不允許特定欄位值

若要防止使用者將欄位設定為特定值，請使用如下所示的條件：

```
"Condition": {
  "StringEquals": {
    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
  }
}
```

例如，下列陳述式表示 BatchUpdateFindings 無法用於將 Workflow.Status 設定為 SUPPRESSED。

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
  }
}
```

您也可以提供不允許的值清單。

```
"Condition": {
```

```

    "StringEquals": {
      "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
"<fieldValue2>", "<fieldValue3>" ]
    }
  }
}

```

例如，下列陳述式表示 BatchUpdateFindings 無法用於 Workflow.Status 將設定為 RESOLVED 或 SUPPRESSED。

```

{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": [
        "RESOLVED",
        "NOTIFIED"
      ]
    }
  }
}

```

在 Security Hub CSPM 中檢閱問題清單詳細資訊和歷史記錄

在 AWS Security Hub CSPM 中，問題清單是安全檢查或安全相關偵測的可觀察記錄。Security Hub CSPM 會在完成控制項的安全性檢查，以及從整合 AWS 服務 或 第三方產品擷取問題清單時產生問題清單。每個調查結果都包含變更和其他詳細資訊的歷史記錄，例如嚴重性評分和受影響資源的相關資訊。

您可以在 Security Hub CSPM 主控台或使用 Security Hub CSPM API 或 以程式設計方式檢閱個別問題清單的歷史記錄和其他詳細資訊 AWS CLI。

為了協助您簡化分析，當您選擇特定問題清單時，Security Hub CSPM 主控台會顯示問題清單面板。面板包含不同的功能表和索引標籤，用於檢閱問題清單的特定詳細資訊。

動作功能表

在此功能表中，您可以檢閱問題清單的完整 JSON 或新增備註。問題清單一次只能連接一個備註。此功能表也提供 [設定問題清單工作流程狀態](#) 的選項，[或將問題清單傳送至 Amazon EventBridge 中的自訂動作](#)。EventBridge

調查選單

在此功能表中，您可以在 Amazon Detective 中調查問題清單。Detective 從調查結果中擷取實體，例如 IP 地址和 AWS 使用者，並視覺化其活動。您可以使用實體活動做為起點，以調查調查結果的原因和影響。

概觀標籤

此標籤提供調查結果的摘要。例如，您可以判斷問題清單的建立和上次更新時間、其存在的帳戶，以及問題清單的來源。對於控制項調查結果，此索引標籤也會在 Security Hub CSPM 文件中顯示相關 AWS Config 規則的名稱，以及修補指引的連結。

在概觀索引標籤的資源快照中，您可以取得調查結果所涉及資源的簡短概觀。對於某些資源，這包含開啟資源選項，可直接連結到相關 AWS 服務 主控台上受影響的資源。歷史記錄快照最多可顯示追蹤歷史記錄最近日期對調查結果所做的兩個變更。例如，如果您昨天進行了一項變更，今天進行了另一項變更，快照會顯示今天的變更。若要檢閱先前的項目，請切換到歷史記錄索引標籤。

合規資料列會展開以顯示更多詳細資訊。例如，如果控制項包含參數，您可以檢閱 Security Hub CSPM 在執行控制項安全檢查時目前使用的參數值。

資源索引標籤

此標籤提供有關問題清單所涉及資源的詳細資訊。如果您已登入擁有資源的帳戶，您可以在適用的 AWS 服務 主控台中檢閱資源。如果您不是資源的擁有者，此標籤會顯示擁有者的 AWS 帳戶 ID。

詳細資訊列會顯示調查結果中的資源特定詳細資訊。它以 JSON 格式顯示調查結果的 [ResourceDetails](#) 區段。

標籤列會顯示指派給問題清單所涉及資源的標籤索引鍵和值。AWS Resource Groups 標記 API [GetResources](#) [操作支援](#) 的資源可以加上標籤。Security Hub CSPM 會在處理新的或更新的調查結果時使用 [服務連結角色](#) 來呼叫此操作，並在 AWS Security Finding Format (ASFF) `Resource.Id` 欄位填入資源的 ARN 時擷取資源標籤。Security Hub CSPM 會忽略無效的資源 IDs。如需在調查結果中包含資源標籤的詳細資訊，請參閱 [Tags \(標籤\)](#)。

歷史記錄索引標籤

此標籤會追蹤問題清單的歷史記錄。問題清單歷史記錄可供作用中和封存的問題清單使用。它提供隨時間對調查結果進行變更的不可變線索，包括 ASFF 欄位變更的內容、變更發生的時間，以及使用者。標籤上的每個頁面最多可顯示 20 個變更。首先顯示更多最近的變更。

對於作用中的問題清單，問題清單歷史記錄最多可使用 90 天。對於封存的問題清單，問題清單歷史記錄最多可使用 30 天。調查結果歷史記錄包含由 [Security Hub CSPM 自動化規則](#) 手動或自動所做的變更。它不包含對頂層時間戳記欄位的變更，例如 `CreatedAt` 和 `UpdatedAt` 欄位。

如果您已登入 Security Hub CSPM 管理員帳戶，則調查結果歷史記錄適用於管理員帳戶和所有成員帳戶。

威脅索引標籤

此索引標籤包含來自 ASFF 的 [Action](#)、[Malware](#) 和 [ProcessDetails](#) 物件的資料，包括威脅類型，以及資源是目標還是演員。這些詳細資訊通常適用於源自 Amazon GuardDuty 的調查結果。

漏洞索引標籤

此標籤會顯示 ASFF [Vulnerability](#) 物件中的資料，包括是否有與調查結果相關聯的入侵或可用修正。這些詳細資訊通常適用於源自 Amazon Inspector 的調查結果。

每個索引標籤上的資料列都包含複製或篩選選項。例如，如果您針對工作流程狀態為已通知的問題清單開啟面板，您可以選擇工作流程狀態列旁的篩選條件選項。如果您選擇顯示具有此值的所有問題清單，Security Hub CSPM 會篩選問題清單表格，並僅顯示工作流程狀態相同的問題清單。

檢閱問題清單詳細資訊和歷史記錄

選擇您偏好的方法，並依照步驟檢閱 Security Hub CSPM 中的調查結果詳細資訊。

如果您啟用跨區域彙總並登入彙總區域，調查結果資料會包含來自彙總區域和連結區域的資料。在其他區域中，問題清單資料僅適用於該區域。如需跨區域彙總的詳細資訊，請參閱 [the section called “跨區域彙總資料”](#)。

Security Hub CSPM console

檢閱問題清單詳細資訊和歷史記錄

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 若要顯示問題清單，請執行下列其中一項操作：
 - 在導覽窗格中，選擇調查結果。視需要新增搜尋篩選條件，以縮小問題清單範圍。
 - 在導覽窗格中，選擇 Insights。選擇洞見。然後，在結果清單中，選擇洞見結果。
 - 在導覽窗格中選擇整合。選擇查看整合的問題清單。
 - 在導覽窗格中，選擇控制項。
3. 選擇問題清單。問題清單面板會顯示問題清單的詳細資訊。
4. 在問題清單面板中，執行下列任一動作：

- 若要檢閱問題清單的特定詳細資訊，請選擇索引標籤。
- 若要對調查結果採取動作，請從動作功能表中選擇一個選項。
- 若要在 Amazon Detective 中調查調查結果，請選擇調查選項。

Note

如果您與整合，AWS Organizations 且已登入成員帳戶，則調查結果面板會包含帳戶名稱。對於手動邀請的成員帳戶，而不是透過 Organizations，問題清單面板只會包含帳戶 ID。

Security Hub CSPM API

使用 Security Hub CSPM API [GetFindings](#) 的操作，或者如果您使用的是 AWS CLI，請執行 [get-findings](#) 命令。您可以為 Filters 參數提供一或多個值，以縮小要擷取的問題清單範圍。

如果結果量太大，您可以使用 MaxResults 參數將問題清單限制為指定的數字，並使用 NextToken 參數將問題清單分頁。使用 SortCriteria 參數依特定欄位排序問題清單。

例如，下列 AWS CLI 命令會擷取符合指定篩選條件的問題清單，並依 LastObservedAt 欄位以遞減順序排序結果。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-  
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":  
"NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria  
'{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

若要檢閱問題清單歷史記錄，請使用 [GetFindingHistory](#) 操作。如果您使用的是 AWS CLI，請執行 [get-finding-history](#) 命令。使用 ProductArn 和 Id 欄位識別您要取得歷史記錄的問題清單。如需這些欄位的相關資訊，請參閱「[AwsSecurityFindingIdentifier](#)」。每個請求只能擷取一個問題清單的歷史記錄。

例如，下列 AWS CLI 命令會擷取指定調查結果的歷史記錄。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub get-finding-history \
```

```
--region us-west-2 \  
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default" \  
--max-results 2 \  
--start-time "2021-09-30T15:53:35.573Z" \  
--end-time "2021-09-31T15:53:35.573Z"
```

PowerShell

使用 Get-SHUBFinding cmdlet。選擇性地填入 Filter 參數，以縮小要擷取的問題清單範圍。

例如，以下 cmdlet 會擷取符合指定篩選條件的問題清單。

```
Get-SHUBFinding -Filter @{AwsAccountId =  
[Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =  
"XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =  
"EQUALS"; Value = 'FAILED'}}
```

Note

如果您依 CompanyName 或 篩選問題清單 ProductName，Security Hub CSPM 會使用 ProductFields ASFF 物件一部分的值。Security Hub CSPM 不使用頂層 CompanyName 和 ProductName 欄位。

在 Security Hub CSPM 中篩選問題清單

AWS Security Hub CSPM 會從安全檢查產生自己的調查結果，並從整合產品接收調查結果。您可以在 Security Hub CSPM 主控台的調查結果、整合和洞見頁面上顯示調查結果清單。您可以新增篩選條件來縮小調查結果清單，讓清單與您的組織或使用案例相關。

如需篩選特定安全控制項問題清單的資訊，請參閱 [the section called “篩選和排序控制項問題清單”](#)。本頁面上的資訊適用於問題清單、洞見和整合頁面。

問題清單上的預設篩選條件

根據預設，Security Hub CSPM 主控台上的調查結果清單會根據 AWS 安全調查結果格式 (ASFF) 的 RecordState 和 Workflow.Status 欄位進行篩選。這是除了特定洞見或整合的篩選條件之外。

記錄狀態指出問題清單是作用中還是封存。根據預設，問題清單只會顯示作用中的問題清單。如果問題清單提供者不再處於作用中或重要狀態，則可以封存問題清單。如果刪除相關聯的資源，Security Hub CSPM 也會自動封存控制項調查結果。

工作流程狀態指出調查結果調查的狀態。根據預設，問題清單只會顯示工作流程狀態為 NEW 或 NOTIFIED 的問題清單。您可以更新問題清單的工作流程狀態。

新增篩選條件的說明

您可以依最多十個屬性篩選問題清單。對於每個屬性，您最多可以提供 20 個篩選值。

篩選問題清單時，Security Hub CSPM AND 會將邏輯套用至一組篩選條件。只有當問題清單符合所有提供的篩選條件時，問題清單才會相符。例如，如果您新增 GuardDuty 做為產品名稱的篩選條件，以及 AwsS3Bucket 做為資源類型的篩選條件，Security Hub CSPM 會顯示符合這兩個條件的問題清單。

Security Hub CSPM OR 會將邏輯套用至使用相同屬性但不同值的篩選條件。例如，如果您將 GuardDuty 和 Amazon Inspector 新增為產品名稱的篩選條件值，Security Hub CSPM 會顯示由 GuardDuty 或 Amazon Inspector 產生的調查結果。

將篩選條件新增至問題清單（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 若要顯示問題清單，請從導覽窗格中執行下列其中一個動作：
 - 選擇問題清單。
 - 選擇 Insights。選擇洞見。然後，在結果清單中，選擇洞見結果。
 - 選擇 Integrations (整合)。選擇查看整合的問題清單。
3. 在新增篩選條件方塊中，選取要篩選的一或多個檔案。

當您依公司名稱或產品名稱篩選時，主控台會使用 AWS 安全調查結果格式 (ASFF) 的最上層 CompanyName 和 ProductName 欄位。API 使用下巢狀化的值 ProductFields。

4. 選擇篩選條件比對類型。

對於字串篩選條件，您可以從下列選項中選擇：

- is – 尋找完全符合篩選條件值的值。
- 開頭為 – 尋找開頭為篩選條件值的值。
- 不是 – 尋找不符合篩選條件值的值。

- 開頭不是 - 尋找開頭不是篩選條件值的值。

對於資源標籤欄位，您可以根據特定索引鍵或值進行篩選。

對於數值篩選條件，您可以選擇提供單一數字 (簡單) 或數字範圍 (範圍)。

對於日期或時間篩選條件，您可以選擇提供目前日期和時間 (滾動視窗) 或特定日期範圍 (固定範圍) 的長度。

新增多個篩選條件有下列互動：

- 為，並以 OR 聯結篩選條件開頭。如果包含任何篩選條件值，則值會相符。例如，如果您指定嚴重性標籤為 CRITICAL，嚴重性標籤為 HIGH，則結果會同時包含關鍵和高嚴重性問題清單。
- 不是 且開頭不是篩選條件，由 AND 聯結。值只有在不包含任何這些篩選條件值時才相符。例如，如果您指定嚴重性標籤不是 LOW，嚴重性標籤不是 MEDIUM，則結果不包含低或中嚴重性問題清單。

如果您的欄位上有 篩選條件，則不能有 不是，或 不是以相同欄位上的篩選條件開頭。

5. 指定篩選條件值。對於字串篩選條件，篩選條件值區分大小寫。
6. 選擇套用。

對於現有的篩選條件，您可以變更篩選條件比對類型或值。在篩選的問題清單上，選擇篩選條件。在編輯篩選條件方塊中，選擇新的比對類型或值，然後選擇套用。

若要移除篩選條件，請選擇 x 圖示。系統會自動更新清單以反映變更。

在 Security Hub CSPM 中分組問題清單

您可以根據所選屬性的值，將 AWS Security Hub CSPM 中的問題清單分組。

當您將調查結果分組時，調查結果清單會取代為相符調查結果中所選屬性的值清單。對於每個值，清單會顯示相符問題清單的數量。

例如，如果您依 AWS 帳戶 ID 將問題清單分組，您會看到帳戶識別符清單，其中包含每個帳戶的相符問題清單數量。

Security Hub CSPM 最多可顯示所選屬性的 100 個值。如果超過 100 個值，您只會看到前 100 個。

當您選擇屬性值時，Security Hub CSPM 會顯示該值的相符問題清單。

將問題清單清單中的問題清單分組（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 若要顯示問題清單，請從導覽窗格中執行下列其中一個動作：
 - 選擇問題清單。
 - 選擇 Insights。選擇洞見。然後，在結果清單中，選擇洞見結果。
 - 選擇 Integrations (整合)。選擇查看整合的問題清單。
3. 在分組依據下拉式清單中，選擇要用於分組的屬性。

若要移除分組屬性，請選擇 x 圖示。當您移除分組屬性時，清單會從屬性值清單變更為調查結果清單。

在 Security Hub CSPM 中設定問題清單的工作流程狀態

工作流程狀態會追蹤調查問題清單的進度。工作流程狀態專屬於個別問題清單，不會影響新問題清單的產生。例如，如果您將問題清單的工作流程狀態變更為 SUPPRESSED 或 RESOLVED，您的變更不會阻止 Security Hub CSPM 為相同問題產生新的問題清單。

問題清單的工作流程狀態可以是下列其中一個值。

新

檢閱問題清單之前的初始狀態。

從整合擷取的問題清單 AWS 服務，例如 AWS Config，其初始狀態 NEW 為。

NEW 在下列情況下，Security Hub CSPM 也會將工作流程狀態從 NOTIFIED 或 重設 RESOLVED 為：

- RecordState 從 ARCHIVED 變更為 ACTIVE。
- Compliance.Status 從 PASSED 變更為 FAILED、WARNING 或 NOT_AVAILABLE。

這些變更表示需要額外調查。

已通知

指出您已向資源擁有者告知嚴重性問題。當您不是資源擁有者，且需要資源擁有者介入以解決安全問題時，可以使用此狀態。

如果發生下列其中一種情況，工作流程狀態會自動從 變更為 NOTIFIED NEW：

- RecordState 從 ARCHIVED變更為 ACTIVE。
- Compliance.Status 從 PASSED變更為 FAILED、WARNING或 NOT_AVAILABLE。

已隱藏

表示您已檢閱調查結果，但不認為需要任何動作。

如果SUPPRESSED問題清單的工作流程狀態從 變更為 ARCHIVED，則不會RecordState變更ACTIVE。

已解析

問題清單已檢閱並進行修補，目前視為已解決。

除非發生下列其中一種情況，RESOLVED否則問題清單仍會保留：

- RecordState 從 ARCHIVED變更為 ACTIVE。
- Compliance.Status 從 PASSED變更為 FAILED、WARNING或 NOT_AVAILABLE。

在這些情況下，工作流程狀態會自動重設為 NEW。

對於控制項的問題清單，如果 Compliance.Status是 PASSED，Security Hub CSPM 會自動將工作流程狀態設定為 RESOLVED。

設定問題清單的工作流程狀態

若要變更一或多個問題清單的工作流程狀態，您可以使用 Security Hub CSPM 主控台或 Security Hub CSPM API。如果您變更調查結果的工作流程狀態，請注意，Security Hub CSPM 可能需要幾分鐘的時間來處理請求並更新調查結果。

Tip

您也可以使用自動化規則自動變更問題清單的工作流程狀態。使用自動化規則，您可以設定 Security Hub CSPM，根據您指定的條件自動更新調查結果的工作流程狀態。如需詳細資訊，請參閱[了解 Security Hub CSPM 中的自動化規則](#)。

若要變更一或多個問題清單的工作流程狀態，請選擇您偏好的方法，然後依照步驟進行。

Security Hub CSPM console

變更問題清單的工作流程狀態

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，執行下列其中一項操作，以顯示問題清單的資料表：
 - 選擇問題清單。
 - 選擇 Insights。然後選擇洞見。在洞見結果中，選擇結果。
 - 選擇 Integrations (整合)。然後，在整合的 區段中，選擇查看問題清單。
 - 選擇安全標準。然後，在標準的 區段中，選擇檢視結果。在控制項表格中，選擇控制項以顯示控制項的問題清單。
3. 在問題清單表格中，選取您要變更工作流程狀態的每個問題清單的核取方塊。
4. 在頁面頂端，選擇工作流程狀態，然後為選取的調查結果選擇新的工作流程狀態。
5. 在設定工作流程狀態對話方塊中，選擇性地輸入備註，詳細說明變更工作流程狀態的原因。然後選擇設定狀態。

Security Hub CSPM API

使用 [BatchUpdateFindings](#) 操作。同時提供產生調查結果之產品的調查結果 ID 和 ARN。您可以使用 [GetFindings](#) 操作來取得這些詳細資訊。

AWS CLI

執行 [batch-update-findings](#) 命令。同時提供產生調查結果之產品的調查結果 ID 和 ARN。您可以執行 [get-findings](#) 命令來取得這些詳細資訊。

```
batch-update-findings --finding-identifiers  
Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

範例

```
aws securityhub batch-update-findings --finding-identifiers  
Id="arn:aws:securityhub:us-west-1:123456789012:subscription/  
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
```

```
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --  
workflow Status="RESOLVED"
```

將問題清單傳送至自訂 Security Hub CSPM 動作

您可以建立 AWS Security Hub CSPM 自訂動作，以使用 Amazon EventBridge 自動化 Security Hub CSPM。針對自訂動作，事件類型為 Security Hub Findings - Custom Action。設定自訂動作之後，您可以將問題清單傳送至該動作。如需建立自訂動作的詳細資訊和詳細步驟，請參閱 [the section called “自動化回應和修復”](#)。

將問題清單傳送至自訂動作（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 若要顯示問題清單，請執行下列其中一項操作：
 - 在 Security Hub CSPM 導覽窗格中，選擇調查結果。
 - 在 Security Hub CSPM 導覽窗格中，選擇 Insights。選擇洞見。然後在結果清單中，選擇洞見結果。
 - 在 Security Hub CSPM 導覽窗格中，選擇整合。選擇查看整合的問題清單。
 - 在 Security Hub CSPM 導覽窗格中，選擇安全標準。選擇檢視結果以顯示控制項清單。然後選擇控制項名稱。
3. 在調查結果清單中，選取要傳送至自訂動作的每個調查結果的核取方塊。

您一次最多可以傳送 20 個問題清單。

4. 針對動作，選擇自訂動作。

AWS 安全調查結果格式 (ASFF)

AWS Security Hub CSPM 會取用和彙總整合 AWS 服務 和第三方產品的問題清單。Security Hub CSPM 使用稱為 AWS Security Finding Format (ASFF) 的標準調查結果格式來處理這些調查結果，無需耗費時間進行資料轉換。

此頁面提供 AWS 安全性調查結果格式 (ASFF) 中調查結果的 JSON 完整大綱。格式衍生自 [JSON 結構描述](#)。選擇連結物件的名稱，以檢閱該物件的問題清單範例。將您的 Security Hub CSPM 問題清單與此處顯示的資源和範例進行比較，可協助您解譯問題清單。

如需個別 ASFF 屬性的說明，請參閱 [the section called “必要的頂層 ASFF 屬性”](#)和 [the section called “選用最上層 ASFF 屬性”](#)。

```
"Findings": [  
  {  
    "Action": {  
      "ActionType": "string",  
      "AwsApiCallAction": {  
        "AffectedResources": {  
          "string": "string"  
        },  
        "Api": "string",  
        "CallerType": "string",  
        "DomainDetails": {  
          "Domain": "string"  
        },  
        "FirstSeen": "string",  
        "LastSeen": "string",  
        "RemoteIpDetails": {  
          "City": {  
            "CityName": "string"  
          },  
          "Country": {  
            "CountryCode": "string",  
            "CountryName": "string"  
          },  
          "IpAddressV4": "string",  
          "Geolocation": {  
            "Lat": number,  
            "Lon": number  
          },  
          "Organization": {  
            "Asn": number,  
            "AsnOrg": "string",  
            "Isp": "string",  
            "Org": "string"  
          }  
        },  
        "ServiceName": "string"  
      },  
      "DnsRequestAction": {  
        "Blocked": boolean,  
        "Domain": "string",
```

```
"Protocol": "string",
},
"NetworkConnectionAction": {
  "Blocked": boolean,
  "ConnectionDirection": "string",
  "LocalPortDetails": {
    "Port": number,
    "PortName": "string"
  },
  "Protocol": "string",
  "RemoteIpDetails": {
    "City": {
      "CityName": "string"
    },
    "Country": {
      "CountryCode": "string",
      "CountryName": "string"
    },
    "IpAddressV4": "string",
    "Geolocation": {
      "Lat": number,
      "Lon": number
    },
    "Organization": {
      "Asn": number,
      "AsnOrg": "string",
      "Isp": "string",
      "Org": "string"
    }
  },
  "RemotePortDetails": {
    "Port": number,
    "PortName": "string"
  }
},
"PortProbeAction": {
  "Blocked": boolean,
  "PortProbeDetails": [{
    "LocalIpDetails": {
      "IpAddressV4": "string"
    },
    "LocalPortDetails": {
      "Port": number,
      "PortName": "string"
    }
  }
}
```



```

    },
    "RemoteIpDetails": {
      "City": {
        "CityName": "string"
      },
      "Country": {
        "CountryCode": "string",
        "CountryName": "string"
      },
      "GeoLocation": {
        "Lat": number,
        "Lon": number
      },
      "IpAddressV4": "string",
      "Organization": {
        "Asn": number,
        "AsnOrg": "string",
        "Isp": "string",
        "Org": "string"
      }
    }
  ]
},
"AwsAccountId": "string",
"AwsAccountName": "string",
"CompanyName": "string",
"Compliance": {
  "AssociatedStandards": [{
    "StandardsId": "string"
  }],
  "RelatedRequirements": ["string"],
  "SecurityControlId": "string",
  "SecurityControlParameters": [
    {
      "Name": "string",
      "Value": ["string"]
    }
  ],
  "Status": "string",
  "StatusReasons": [
    {
      "Description": "string",
      "ReasonCode": "string"
    }
  ]
}

```

```
    }
  ]
},
"Confidence": number,
"CreatedAt": "string",
"Criticality": number,
"Description": "string",
"Detection": {
  "Sequence": {
    "Uid": "string",
    "Actors": [{
      "Id": "string",
      "Session": {
        "Uid": "string",
        "MfaStatus": "string",
        "CreatedTime": "string",
        "Issuer": "string"
      },
      "User": {
        "CredentialUid": "string",
        "Name": "string",
        "Type": "string",
        "Uid": "string",
        "Account": {
          "Uid": "string",
          "Name": "string"
        }
      }
    ]
  },
  "Endpoints": [{
    "Id": "string",
    "Ip": "string",
    "Domain": "string",
    "Port": number,
    "Location": {
      "City": "string",
      "Country": "string",
      "Lat": number,
      "Lon": number
    },
    "AutonomousSystem": {
      "Name": "string",
      "Number": number
    }
  },
```

```
    "Connection": {
      "Direction": "string"
    }
  ]],
  "Signals": [{
    "Id": "string",
    "Title": "string",
    "ActorIds": ["string"],
    "Count": number,
    "FirstSeenAt": number,
    "SignalIndicators": [
      {
        "Key": "string",
        "Title": "string",
        "Values": ["string"]
      },
      {
        "Key": "string",
        "Title": "string",
        "Values": ["string"]
      }
    ],
    "LastSeenAt": number,
    "Name": "string",
    "ResourceIds": ["string"],
    "Type": "string"
  ]],
  "SequenceIndicators": [
    {
      "Key": "string",
      "Title": "string",
      "Values": ["string"]
    },
    {
      "Key": "string",
      "Title": "string",
      "Values": ["string"]
    }
  ]
}
},
"FindingProviderFields": {
  "Confidence": number,
  "Criticality": number,
```

```

    "RelatedFindings": [{
      "ProductArn": "string",
      "Id": "string"
    }],
    "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
    },
    "Types": ["string"]
  },
  "FirstObservedAt": "string",
  "GeneratorId": "string",
  "Id": "string",
  "LastObservedAt": "string",
  "Malware": [{
    "Name": "string",
    "Path": "string",
    "State": "string",
    "Type": "string"
  }],
  "Network": {
    "DestinationDomain": "string",
    "DestinationIPv4": "string",
    "DestinationIPv6": "string",
    "DestinationPort": number,
    "Direction": "string",
    "OpenPortRange": {
      "Begin": integer,
      "End": integer
    },
    "Protocol": "string",
    "SourceDomain": "string",
    "SourceIPv4": "string",
    "SourceIPv6": "string",
    "SourceMac": "string",
    "SourcePort": number
  },
  "NetworkPath": [{
    "ComponentId": "string",
    "ComponentType": "string",
    "Egress": {
      "Destination": {
        "Address": ["string"],

```

```

    "PortRanges": [{
      "Begin": integer,
      "End": integer
    }]
  },
  "Protocol": "string",
  "Source": {
    "Address": ["string"],
    "PortRanges": [{
      "Begin": integer,
      "End": integer
    }]
  }
},
"Ingress": {
  "Destination": {
    "Address": ["string"],
    "PortRanges": [{
      "Begin": integer,
      "End": integer
    }]
  },
  "Protocol": "string",
  "Source": {
    "Address": ["string"],
    "PortRanges": [{
      "Begin": integer,
      "End": integer
    }]
  }
},
}],
"Note": {
  "Text": "string",
  "UpdatedAt": "string",
  "UpdatedBy": "string"
},
"PatchSummary": {
  "FailedCount": number,
  "Id": "string",
  "InstalledCount": number,
  "InstalledOtherCount": number,
  "InstalledPendingReboot": number,
  "InstalledRejectedCount": number,

```

```

    "MissingCount": number,
    "Operation": "string",
    "OperationEndTime": "string",
    "OperationStartTime": "string",
    "RebootOption": "string"
  },
  "Process": {
    "LaunchedAt": "string",
    "Name": "string",
    "ParentPid": number,
    "Path": "string",
    "Pid": number,
    "TerminatedAt": "string"
  },
  "ProductArn": "string",
  "ProductFields": {
    "string": "string"
  },
  "ProductName": "string",
  "RecordState": "string",
  "Region": "string",
  "RelatedFindings": [{
    "Id": "string",
    "ProductArn": "string"
  }],
  "Remediation": {
    "Recommendation": {
      "Text": "string",
      "Url": "string"
    }
  },
  "Resources": [{
    "ApplicationArn": "string",
    "ApplicationName": "string",
    "DataClassification": {
      "DetailedResultsLocation": "string",
      "Result": {
        "AdditionalOccurrences": boolean,
        "CustomDataIdentifiers": {
          "Detections": [{
            "Arn": "string",
            "Count": integer,
            "Name": "string",
            "Occurrences": {

```

```
    "Cells": [{
      "CellReference": "string",
      "Column": integer,
      "ColumnName": "string",
      "Row": integer
    }],
    "LineRanges": [{
      "End": integer,
      "Start": integer,
      "StartColumn": integer
    }],
    "OffsetRanges": [{
      "End": integer,
      "Start": integer,
      "StartColumn": integer
    }],
    "Pages": [{
      "LineRange": {
        "End": integer,
        "Start": integer,
        "StartColumn": integer
      },
      "OffsetRange": {
        "End": integer,
        "Start": integer,
        "StartColumn": integer
      },
      "PageNumber": integer
    }],
    "Records": [{
      "JsonPath": "string",
      "RecordIndex": integer
    }]
  }
}],
"TotalCount": integer
},
"MimeType": "string",
"SensitiveData": [{
  "Category": "string",
  "Detections": [{
    "Count": integer,
    "Occurrences": {
      "Cells": [{
```

```
    "CellReference": "string",
    "Column": integer,
    "ColumnName": "string",
    "Row": integer
  ]],
  "LineRanges": [{
    "End": integer,
    "Start": integer,
    "StartColumn": integer
  }],
  "OffsetRanges": [{
    "End": integer,
    "Start": integer,
    "StartColumn": integer
  }],
  "Pages": [{
    "LineRange": {
      "End": integer,
      "Start": integer,
      "StartColumn": integer
    },
    "OffsetRange": {
      "End": integer,
      "Start": integer,
      "StartColumn": integer
    },
    "PageNumber": integer
  }],
  "Records": [{
    "JsonPath": "string",
    "RecordIndex": integer
  }]
},
"Type": "string"
}],
"TotalCount": integer
}],
"SizeClassified": integer,
"Status": {
  "Code": "string",
  "Reason": "string"
}
}
},
```



```
"Details": {
  "AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": boolean,
    "BrokerArn": "string",
    "BrokerId": "string",
    "BrokerName": "string",
    "Configuration": {
      "Id": "string",
      "Revision": integer
    },
    "DeploymentMode": "string",
    "EncryptionOptions": {
      "UseAwsOwnedKey": boolean
    },
    "EngineType": "string",
    "EngineVersion": "string",
    "HostInstanceType": "string",
    "Logs": {
      "Audit": boolean,
      "AuditLogGroup": "string",
      "General": boolean,
      "GeneralLogGroup": "string"
    },
    "MaintenanceWindowStartTime": {
      "DayOfWeek": "string",
      "TimeOfDay": "string",
      "TimeZone": "string"
    },
    "PubliclyAccessible": boolean,
    "SecurityGroups": [
      "string"
    ],
    "StorageType": "string",
    "SubnetIds": [
      "string",
      "string"
    ],
    "Users": [{
      "Username": "string"
    }]
  },
  "AwsApiGatewayRestApi": {
    "ApiKeySource": "string",
    "BinaryMediaTypes": [" string"],
```

```

    "CreatedDate": "string",
    "Description": "string",
    "EndpointConfiguration": {
      "Types": ["string"]
    },
    "Id": "string",
    "MinimumCompressionSize": number,
    "Name": "string",
    "Version": "string"
  },
  "AwsApiGatewayStage": {
    "AccessLogSettings": {
      "DestinationArn": "string",
      "Format": "string"
    },
    "CacheClusterEnabled": boolean,
    "CacheClusterSize": "string",
    "CacheClusterStatus": "string",
    "CanarySettings": {
      "DeploymentId": "string",
      "PercentTraffic": number,
      "StageVariableOverrides": [{
        "string": "string"
      }],
      "UseStageCache": boolean
    },
    "ClientCertificateId": "string",
    "CreatedDate": "string",
    "DeploymentId": "string",
    "Description": "string",
    "DocumentationVersion": "string",
    "LastUpdatedDate": "string",
    "MethodSettings": [{
      "CacheDataEncrypted": boolean,
      "CachingEnabled": boolean,
      "CacheTtlInSeconds": number,
      "DataTraceEnabled": boolean,
      "HttpMethod": "string",
      "LoggingLevel": "string",
      "MetricsEnabled": boolean,
      "RequireAuthorizationForCacheControl": boolean,
      "ResourcePath": "string",
      "ThrottlingBurstLimit": number,
      "ThrottlingRateLimit": number,

```

```

    "UnauthorizedCacheControlHeaderStrategy": "string"
  }],
  "StageName": "string",
  "TracingEnabled": boolean,
  "Variables": {
    "string": "string"
  },
  "WebAclArn": "string"
},
"AwsApiGatewayV2Api": {
  "ApiEndpoint": "string",
  "ApiId": "string",
  "ApiKeySelectionExpression": "string",
  "CorsConfiguration": {
    "AllowCredentials": boolean,
    "AllowHeaders": ["string"],
    "AllowMethods": ["string"],
    "AllowOrigins": ["string"],
    "ExposeHeaders": ["string"],
    "MaxAge": number
  },
  "CreatedDate": "string",
  "Description": "string",
  "Name": "string",
  "ProtocolType": "string",
  "RouteSelectionExpression": "string",
  "Version": "string"
},
"AwsApiGatewayV2Stage": {
  "AccessLogSettings": {
    "DestinationArn": "string",
    "Format": "string"
  },
  "ApiGatewayManaged": boolean,
  "AutoDeploy": boolean,
  "ClientCertificateId": "string",
  "CreatedDate": "string",
  "DefaultRouteSettings": {
    "DataTraceEnabled": boolean,
    "DetailedMetricsEnabled": boolean,
    "LoggingLevel": "string",
    "ThrottlingBurstLimit": number,
    "ThrottlingRateLimit": number
  }
},

```

```

    "DeploymentId": "string",
    "Description": "string",
    "LastDeploymentStatusMessage": "string",
    "LastUpdatedDate": "string",
    "RouteSettings": {
      "DetailedMetricsEnabled": boolean,
      "LoggingLevel": "string",
      "DataTraceEnabled": boolean,
      "ThrottlingBurstLimit": number,
      "ThrottlingRateLimit": number
    },
    "StageName": "string",
    "StageVariables": [{
      "string": "string"
    }]
  },
  "AwsAppSyncGraphQLApi": {
    "AwsAppSyncGraphQLApi": {
      "AdditionalAuthenticationProviders": [
        {
          "AuthenticationType": "string",
          "LambdaAuthorizerConfig": {
            "AuthorizerResultTtlInSeconds": integer,
            "AuthorizerUri": "string"
          }
        }
      ],
      "AuthenticationType": "string"
    },
    "ApiId": "string",
    "Arn": "string",
    "AuthenticationType": "string",
    "Id": "string",
    "LogConfig": {
      "CloudWatchLogsRoleArn": "string",
      "ExcludeVerboseContent": boolean,
      "FieldLogLevel": "string"
    },
    "Name": "string",
    "XrayEnabled": boolean
  },
  "AwsAthenaWorkGroup": {

```

```

    "Description": "string",
    "Name": "string",
    "WorkgroupConfiguration": {
      "ResultConfiguration": {
        "EncryptionConfiguration": {
          "EncryptionOption": "string",
          "KmsKey": "string"
        }
      }
    },
    "State": "string"
  },
  "AwsAutoScalingAutoScalingGroup": {
    "AvailabilityZones": [{
      "Value": "string"
    }],
    "CreatedTime": "string",
    "HealthCheckGracePeriod": integer,
    "HealthCheckType": "string",
    "LaunchConfigurationName": "string",
    "LoadBalancerNames": ["string"],
    "LaunchTemplate": {
      "LaunchTemplateId": "string",
      "LaunchTemplateName": "string",
      "Version": "string"
    },
    "MixedInstancesPolicy": {
      "InstancesDistribution": {
        "OnDemandAllocationStrategy": "string",
        "OnDemandBaseCapacity": number,
        "OnDemandPercentageAboveBaseCapacity": number,
        "SpotAllocationStrategy": "string",
        "SpotInstancePools": number,
        "SpotMaxPrice": "string"
      }
    },
    "LaunchTemplate": {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "string",
        "LaunchTemplateName": "string",
        "Version": "string"
      }
    },
    "CapacityRebalance": boolean,
    "Overrides": [{
      "InstanceType": "string",

```

```

        "WeightedCapacity": "string"
    }
}
},
"AwsAutoScalingLaunchConfiguration": {
    "AssociatePublicIpAddress": boolean,
    "BlockDeviceMappings": [{
        "DeviceName": "string",
        "Ebs": {
            "DeleteOnTermination": boolean,
            "Encrypted": boolean,
            "Iops": number,
            "SnapshotId": "string",
            "VolumeSize": number,
            "VolumeType": "string"
        },
        "NoDevice": boolean,
        "VirtualName": "string"
    }],
    "ClassicLinkVpcId": "string",
    "ClassicLinkVpcSecurityGroups": ["string"],
    "CreatedTime": "string",
    "EbsOptimized": boolean,
    "IamInstanceProfile": "string"
},
    "ImageId": "string",
    "InstanceMonitoring": {
        "Enabled": boolean
    },
    "InstanceType": "string",
    "KernelId": "string",
    "KeyName": "string",
    "LaunchConfigurationName": "string",
    "MetadataOptions": {
        "HttpEndPoint": "string",
        "HttpPutReponseHopLimit": number,
        "HttpTokens": "string"
    },
    "PlacementTenancy": "string",
    "RamdiskId": "string",
    "SecurityGroups": ["string"],
    "SpotPrice": "string",
    "UserData": "string"
}

```

```

},
"AwsBackupBackupPlan": {
  "BackupPlan": {
    "AdvancedBackupSettings": [{
      "BackupOptions": {
        "WindowsVSS": "string"
      },
      "ResourceType": "string"
    }],
    "BackupPlanName": "string",
    "BackupPlanRule": [{
      "CompletionWindowMinutes": integer,
      "CopyActions": [{
        "DestinationBackupVaultArn": "string",
        "Lifecycle": {
          "DeleteAfterDays": integer,
          "MoveToColdStorageAfterDays": integer
        }
      }],
      "Lifecycle": {
        "DeleteAfterDays": integer
      },
      "RuleName": "string",
      "ScheduleExpression": "string",
      "StartWindowMinutes": integer,
      "TargetBackupVault": "string"
    }]
  },
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "VersionId": "string"
},
"AwsBackupBackupVault": {
  "AccessPolicy": {
    "Statement": [{
      "Action": ["string"],
      "Effect": "string",
      "Principal": {
        "AWS": "string"
      },
      "Resource": "string"
    }],
    "Version": "string"
  },

```

```

    "BackupVaultArn": "string",
    "BackupVaultName": "string",
    "EncryptionKeyArn": "string",
    "Notifications": {
      "BackupVaultEvents": ["string"],
      "SNSTopicArn": "string"
    }
  },
  "AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": integer,
    "BackupVaultName": "string",
    "BackupVaultArn": "string",
    "CalculatedLifecycle": {
      "DeleteAt": "string",
      "MoveToColdStorageAt": "string"
    },
    "CompletionDate": "string",
    "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
    },
    "CreationDate": "string",
    "EncryptionKeyArn": "string",
    "IamRoleArn": "string",
    "IsEncrypted": boolean,
    "LastRestoreTime": "string",
    "Lifecycle": {
      "DeleteAfterDays": integer,
      "MoveToColdStorageAfterDays": integer
    },
    "RecoveryPointArn": "string",
    "ResourceArn": "string",
    "ResourceType": "string",
    "SourceBackupVaultArn": "string",
    "Status": "string",
    "StatusMessage": "string",
    "StorageClass": "string"
  },
  "AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "string",
    "CreatedAt": "string",
    "DomainName": "string",

```



```

"DomainValidationOptions": [{
  "DomainName": "string",
  "ResourceRecord": {
    "Name": "string",
    "Type": "string",
    "Value": "string"
  },
  "ValidationDomain": "string",
  "ValidationEmails": ["string"],
  "ValidationMethod": "string",
  "ValidationStatus": "string"
}],
"ExtendedKeyUsages": [{
  "Name": "string",
  "OId": "string"
}],
"FailureReason": "string",
"ImportedAt": "string",
"InUseBy": ["string"],
"IssuedAt": "string",
"Issuer": "string",
"KeyAlgorithm": "string",
"KeyUsages": [{
  "Name": "string"
}],
"NotAfter": "string",
"NotBefore": "string",
"Options": {
  "CertificateTransparencyLoggingPreference": "string"
},
"RenewalEligibility": "string",
"RenewalSummary": {
  "DomainValidationOptions": [{
    "DomainName": "string",
    "ResourceRecord": {
      "Name": "string",
      "Type": "string",
      "Value": "string"
    },
    "ValidationDomain": "string",
    "ValidationEmails": ["string"],
    "ValidationMethod": "string",
    "ValidationStatus": "string"
  }],

```

```

    "RenewalStatus": "string",
    "RenewalStatusReason": "string",
    "UpdatedAt": "string"
  },
  "Serial": "string",
  "SignatureAlgorithm": "string",
  "Status": "string",
  "Subject": "string",
  "SubjectAlternativeNames": ["string"],
  "Type": "string"
},
"AwsCloudFormationStack": {
  "Capabilities": ["string"],
  "CreationTime": "string",
  "Description": "string",
  "DisableRollback": boolean,
  "DriftInformation": {
    "StackDriftStatus": "string"
  },
  "EnableTerminationProtection": boolean,
  "LastUpdatedTime": "string",
  "NotificationArns": ["string"],
  "Outputs": [{
    "Description": "string",
    "OutputKey": "string",
    "OutputValue": "string"
  }],
  "RoleArn": "string",
  "StackId": "string",
  "StackName": "string",
  "StackStatus": "string",
  "StackStatusReason": "string",
  "TimeoutInMinutes": number
},
"AwsCloudFrontDistribution": {
  "CacheBehaviors": {
    "Items": [{
      "ViewerProtocolPolicy": "string"
    }]
  },
  "DefaultCacheBehavior": {
    "ViewerProtocolPolicy": "string"
  },
  "DefaultRootObject": "string",

```

```
"DomainName": "string",
"Etag": "string",
"LastModifiedTime": "string",
"Logging": {
  "Bucket": "string",
  "Enabled": boolean,
  "IncludeCookies": boolean,
  "Prefix": "string"
},
"OriginGroups": {
  "Items": [{
    "FailoverCriteria": {
      "StatusCodes": {
        "Items": [number],
        "Quantity": number
      }
    }
  }]
},
"Origins": {
  "Items": [{
    "CustomOriginConfig": {
      "HttpPort": number,
      "HttpsPort": number,
      "OriginKeepaliveTimeout": number,
      "OriginProtocolPolicy": "string",
      "OriginReadTimeout": number,
      "OriginSslProtocols": {
        "Items": ["string"],
        "Quantity": number
      }
    }
  }],
  "DomainName": "string",
  "Id": "string",
  "OriginPath": "string",
  "S3OriginConfig": {
    "OriginAccessIdentity": "string"
  }
},
"Status": "string",
"ViewerCertificate": {
  "AcmCertificateArn": "string",
  "Certificate": "string",
```

```
    "CertificateSource": "string",
    "CloudFrontDefaultCertificate": boolean,
    "IamCertificateId": "string",
    "MinimumProtocolVersion": "string",
    "SslSupportMethod": "string"
  },
  "WebAclId": "string"
},
"AwsCloudTrailTrail": {
  "CloudWatchLogsLogGroupArn": "string",
  "CloudWatchLogsRoleArn": "string",
  "HasCustomEventSelectors": boolean,
  "HomeRegion": "string",
  "IncludeGlobalServiceEvents": boolean,
  "IsMultiRegionTrail": boolean,
  "IsOrganizationTrail": boolean,
  "KmsKeyId": "string",
  "LogFileValidationEnabled": boolean,
  "Name": "string",
  "S3BucketName": "string",
  "S3KeyPrefix": "string",
  "SnsTopicArn": "string",
  "SnsTopicName": "string",
  "TrailArn": "string"
},
"AwsCloudWatchAlarm": {
  "ActionsEnabled": boolean,
  "AlarmActions": ["string"],
  "AlarmArn": "string",
  "AlarmConfigurationUpdatedTimestamp": "string",
  "AlarmDescription": "string",
  "AlarmName": "string",
  "ComparisonOperator": "string",
  "DatapointsToAlarm": number,
  "Dimensions": [{
    "Name": "string",
    "Value": "string"
  }],
  "EvaluateLowSampleCountPercentile": "string",
  "EvaluationPeriods": number,
  "ExtendedStatistic": "string",
  "InsufficientDataActions": ["string"],
  "MetricName": "string",
  "Namespace": "string",
```

```

    "OkActions": ["string"],
    "Period": number,
    "Statistic": "string",
    "Threshold": number,
    "ThresholdMetricId": "string",
    "TreatMissingData": "string",
    "Unit": "string"
  },
  "AwsCodeBuildProject": {
    "Artifacts": [{
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "OverrideArtifactName": boolean,
      "Packaging": "string",
      "Path": "string",
      "Type": "string"
    }],
    "SecondaryArtifacts": [{
      "ArtifactIdentifier": "string",
      "Type": "string",
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "Packaging": "string",
      "Path": "string",
      "EncryptionDisabled": boolean,
      "OverrideArtifactName": boolean
    }],
    "EncryptionKey": "string",
    "Certificate": "string",
    "Environment": {
      "Certificate": "string",
      "EnvironmentVariables": [{
        "Name": "string",
        "Type": "string",
        "Value": "string"
      }],
    },
    "ImagePullCredentialsType": "string",
    "PrivilegedMode": boolean,
    "RegistryCredential": {
      "Credential": "string",

```

```

    "CredentialProvider": "string"
  },
  "Type": "string"
},
"LogsConfig": {
  "CloudWatchLogs": {
    "GroupName": "string",
    "Status": "string",
    "StreamName": "string"
  },
  "S3Logs": {
    "EncryptionDisabled": boolean,
    "Location": "string",
    "Status": "string"
  }
},
"Name": "string",
"ServiceRole": "string",
"Source": {
  "Type": "string",
  "Location": "string",
  "GitCloneDepth": integer
},
"VpcConfig": {
  "VpcId": "string",
  "Subnets": ["string"],
  "SecurityGroupIds": ["string"]
}
},
"AwsDmsEndpoint": {
  "CertificateArn": "string",
  "DatabaseName": "string",
  "EndpointArn": "string",
  "EndpointIdentifier": "string",
  "EndpointType": "string",
  "EngineName": "string",
  "KmsKeyId": "string",
  "Port": integer,
  "ServerName": "string",
  "SslMode": "string",
  "Username": "string"
},
"AwsDmsReplicationInstance": {
  "AllocatedStorage": integer,

```

```

    "AutoMinorVersionUpgrade": boolean,
    "AvailabilityZone": "string",
    "EngineVersion": "string",
    "KmsKeyId": "string",
    "MultiAZ": boolean,
    "PreferredMaintenanceWindow": "string",
    "PubliclyAccessible": boolean,
    "ReplicationInstanceClass": "string",
    "ReplicationInstanceIdentifier": "string",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "string"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "string"
        }
    ],
},
"AwsDmsReplicationTask": {
    "CdcStartPosition": "string",
    "Id": "string",
    "MigrationType": "string",
    "ReplicationInstanceArn": "string",
    "ReplicationTaskIdentifier": "string",
    "ReplicationTaskSettings": {
        "string": "string"
    },
    "SourceEndpointArn": "string",
    "TableMappings": {
        "string": "string"
    },
    "TargetEndpointArn": "string"
},
"AwsDynamoDbTable": {
    "AttributeDefinitions": [{
        "AttributeName": "string",
        "AttributeType": "string"
    }],
    "BillingModeSummary": {
        "BillingMode": "string",
        "LastUpdateToPayPerRequestDateTime": "string"
    },
    "CreationDateTime": "string",
    "DeletionProtectionEnabled": boolean,

```

```
"GlobalSecondaryIndexes": [{
  "Backfilling": boolean,
  "IndexArn": "string",
  "IndexName": "string",
  "IndexSizeBytes": number,
  "IndexStatus": "string",
  "ItemCount": number,
  "KeySchema": [{
    "AttributeName": "string",
    "KeyType": "string"
  }],
  "Projection": {
    "NonKeyAttributes": ["string"],
    "ProjectionType": "string"
  },
  "ProvisionedThroughput": {
    "LastDecreaseDateTime": "string",
    "LastIncreaseDateTime": "string",
    "NumberOfDecreasesToday": number,
    "ReadCapacityUnits": number,
    "WriteCapacityUnits": number
  }
}],
"GlobalTableVersion": "string",
"ItemCount": number,
"KeySchema": [{
  "AttributeName": "string",
  "KeyType": "string"
}],
"LatestStreamArn": "string",
"LatestStreamLabel": "string",
"LocalSecondaryIndexes": [{
  "IndexArn": "string",
  "IndexName": "string",
  "KeySchema": [{
    "AttributeName": "string",
    "KeyType": "string"
  }],
  "Projection": {
    "NonKeyAttributes": ["string"],
    "ProjectionType": "string"
  }
}],
"ProvisionedThroughput": {
```



```

    "LastDecreaseDateTime": "string",
    "LastIncreaseDateTime": "string",
    "NumberOfDecreasesToday": number,
    "ReadCapacityUnits": number,
    "WriteCapacityUnits": number
  },
  "Replicas": [{
    "GlobalSecondaryIndexes": [{
      "IndexName": "string",
      "ProvisionedThroughputOverride": {
        "ReadCapacityUnits": number
      }
    }],
    "KmsMasterKeyId": "string",
    "ProvisionedThroughputOverride": {
      "ReadCapacityUnits": number
    },
    "RegionName": "string",
    "ReplicaStatus": "string",
    "ReplicaStatusDescription": "string"
  }],
  "RestoreSummary": {
    "RestoreDateTime": "string",
    "RestoreInProgress": boolean,
    "SourceBackupArn": "string",
    "SourceTableArn": "string"
  },
  "SseDescription": {
    "InaccessibleEncryptionDateTime": "string",
    "KmsMasterKeyArn": "string",
    "SseType": "string",
    "Status": "string"
  },
  "StreamSpecification": {
    "StreamEnabled": boolean,
    "StreamViewType": "string"
  },
  "TableId": "string",
  "TableName": "string",
  "TableSizeBytes": number,
  "TableStatus": "string"
},
"AwsEc2ClientVpnEndpoint": {
  "AuthenticationOptions": [

```

```

{
  "MutualAuthentication": {
    "ClientRootCertificateChainArn": "string"
  },
  "Type": "string"
},
],
"ClientCidrBlock": "string",
"ClientConnectOptions": {
  "Enabled": boolean
},
"ClientLoginBannerOptions": {
  "Enabled": boolean
},
"ClientVpnEndpointId": "string",
"ConnectionLogOptions": {
  "Enabled": boolean
},
"Description": "string",
"DnsServer": ["string"],
"ServerCertificateArn": "string",
"SecurityGroupIdSet": [
  "string"
],
"SelfServicePortalUrl": "string",
"SessionTimeoutHours": "integer",
"SplitTunnel": boolean,
"TransportProtocol": "string",
"VpcId": "string",
"VpnPort": integer
},
"AwsEc2Eip": {
  "AllocationId": "string",
  "AssociationId": "string",
  "Domain": "string",
  "InstanceId": "string",
  "NetworkBorderGroup": "string",
  "NetworkInterfaceId": "string",
  "NetworkInterfaceOwnerId": "string",
  "PrivateIpAddress": "string",
  "PublicIp": "string",
  "PublicIpv4Pool": "string"
},
"AwsEc2Instance": {

```

```

    "IamInstanceProfileArn": "string",
    "ImageId": "string",
    "IPv4Addresses": ["string"],
    "IPv6Addresses": ["string"],
    "KeyName": "string",
    "LaunchedAt": "string",
    "MetadataOptions": {
      "HttpEndpoint": "string",
      "HttpProtocolIpv6": "string",
      "HttpPutResponseHopLimit": number,
      "HttpTokens": "string",
      "InstanceMetadataTags": "string"
    },
    "Monitoring": {
      "State": "string"
    },
    "NetworkInterfaces": [{
      "NetworkInterfaceId": "string"
    }],
    "SubnetId": "string",
    "Type": "string",
    "VirtualizationType": "string",
    "VpcId": "string"
  },
  "AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "string",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "string",
    "ImageId": "string",
    "LatestVersionNumber": "string",
    "LaunchTemplateData": {
      "BlockDeviceMappings": [{
        "DeviceName": "string",
        "Ebs": {
          "DeleteonTermination": boolean,
          "Encrypted": boolean,
          "SnapshotId": "string",
          "VolumeSize": number,
          "VolumeType": "string"
        }
      }],
      "MetadataOptions": {
        "HttpTokens": "string",

```

```

    "HttpPutResponseHopLimit" : number
  },
  "Monitoring": {
    "Enabled": boolean
  },
  "NetworkInterfaces": [{
    "AssociatePublicIpAddress" : boolean
  }]
},
"LaunchTemplateName": "string",
"LicenseSpecifications": ["string"],
"SecurityGroupIds": ["string"],
"SecurityGroups": ["string"],
"TagSpecifications": ["string"]
},
"AwsEc2NetworkAcl": {
  "Associations": [{
    "NetworkAclAssociationId": "string",
    "NetworkAclId": "string",
    "SubnetId": "string"
  }],
  "Entries": [{
    "CidrBlock": "string",
    "Egress": boolean,
    "IcmpTypeCode": {
      "Code": number,
      "Type": number
    },
    "Ipv6CidrBlock": "string",
    "PortRange": {
      "From": number,
      "To": number
    },
    "Protocol": "string",
    "RuleAction": "string",
    "RuleNumber": number
  }],
  "IsDefault": boolean,
  "NetworkAclId": "string",
  "OwnerId": "string",
  "VpcId": "string"
},
"AwsEc2NetworkInterface": {
  "Attachment": {

```

```

    "AttachmentId": "string",
    "AttachTime": "string",
    "DeleteOnTermination": boolean,
    "DeviceIndex": number,
    "InstanceId": "string",
    "InstanceOwnerId": "string",
    "Status": "string"
  },
  "Ipv6Addresses": [{
    "Ipv6Address": "string"
  }],
  "NetworkInterfaceId": "string",
  "PrivateIpAddresses": [{
    "PrivateDnsName": "string",
    "PrivateIpAddress": "string"
  }],
  "PublicDnsName": "string",
  "PublicIp": "string",
  "SecurityGroups": [{
    "GroupId": "string",
    "GroupName": "string"
  }],
  "SourceDestCheck": boolean
},
"AwsEc2RouteTable": {
  "AssociationSet": [{
    "AssociationState": {
      "State": "string"
    },
    "Main": boolean,
    "RouteTableAssociationId": "string",
    "RouteTableId": "string"
  }],
  "PropogatingVgwSet": [],
  "RouteTableId": "string",
  "RouteSet": [
    {
      "DestinationCidrBlock": "string",
      "GatewayId": "string",
      "Origin": "string",
      "State": "string"
    },
    {
      "DestinationCidrBlock": "string",

```

```
        "GatewayId": "string",
        "Origin": "string",
        "State": "string"
    }
],
"VpcId": "string"
},
"AwsEc2SecurityGroup": {
    "GroupId": "string",
    "GroupName": "string",
    "IpPermissions": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
            "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
            "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
            "PrefixListId": "string"
        }],
        "ToPort": number,
        "UserIdGroupPairs": [{
            "GroupId": "string",
            "GroupName": "string",
            "PeeringStatus": "string",
            "UserId": "string",
            "VpcId": "string",
            "VpcPeeringConnectionId": "string"
        }]
    }],
    "IpPermissionsEgress": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
            "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
            "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
            "PrefixListId": "string"
        }],
    }],
```

```

    "ToPort": number,
    "UserIdGroupPairs": [{
      "GroupId": "string",
      "GroupName": "string",
      "PeeringStatus": "string",
      "UserId": "string",
      "VpcId": "string",
      "VpcPeeringConnectionId": "string"
    }]
  }],
  "OwnerId": "string",
  "VpcId": "string"
},
"AwsEc2Subnet": {
  "AssignIpv6AddressOnCreation": boolean,
  "AvailabilityZone": "string",
  "AvailabilityZoneId": "string",
  "AvailableIpAddressCount": number,
  "CidrBlock": "string",
  "DefaultForAz": boolean,
  "Ipv6CidrBlockAssociationSet": [{
    "AssociationId": "string",
    "Ipv6CidrBlock": "string",
    "CidrBlockState": "string"
  }],
  "MapPublicIpOnLaunch": boolean,
  "OwnerId": "string",
  "State": "string",
  "SubnetArn": "string",
  "SubnetId": "string",
  "VpcId": "string"
},
"AwsEc2TransitGateway": {
  "AmazonSideAsn": number,
  "AssociationDefaultRouteTableId": "string",
  "AutoAcceptSharedAttachments": "string",
  "DefaultRouteTableAssociation": "string",
  "DefaultRouteTablePropagation": "string",
  "Description": "string",
  "DnsSupport": "string",
  "Id": "string",
  "MulticastSupport": "string",
  "PropagationDefaultRouteTableId": "string",
  "TransitGatewayCidrBlocks": ["string"],

```

```

    "VpnEcmpSupport": "string"
  },
  "AwsEc2Volume": {
    "Attachments": [{
      "AttachTime": "string",
      "DeleteOnTermination": boolean,
      "InstanceId": "string",
      "Status": "string"
    }],
    "CreateTime": "string",
    "DeviceName": "string",
    "Encrypted": boolean,
    "KmsKeyId": "string",
    "Size": number,
    "SnapshotId": "string",
    "Status": "string",
    "VolumeId": "string",
    "VolumeScanStatus": "string",
    "VolumeType": "string"
  },
  "AwsEc2Vpc": {
    "CidrBlockAssociationSet": [{
      "AssociationId": "string",
      "CidrBlock": "string",
      "CidrBlockState": "string"
    }],
    "DhcpOptionsId": "string",
    "Ipv6CidrBlockAssociationSet": [{
      "AssociationId": "string",
      "CidrBlockState": "string",
      "Ipv6CidrBlock": "string"
    }],
    "State": "string"
  },
  "AwsEc2VpcEndpointService": {
    "AcceptanceRequired": boolean,
    "AvailabilityZones": ["string"],
    "BaseEndpointDnsNames": ["string"],
    "ManagesVpcEndpoints": boolean,
    "GatewayLoadBalancerArns": ["string"],
    "NetworkLoadBalancerArns": ["string"],
    "PrivateDnsName": "string",
    "ServiceId": "string",
    "ServiceName": "string",

```



```
"ServiceState": "string",
"ServiceType": [{
  "ServiceType": "string"
}],
},
"AwsEc2VpcPeeringConnection": {
  "AcceptorVpcInfo": {
    "CidrBlock": "string",
    "CidrBlockSet": [{
      "CidrBlock": "string"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "string"
    }],
    "OwnerId": "string",
    "PeeringOptions": {
      "AllowDnsResolutionFromRemoteVpc": boolean,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
      "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
    },
    "Region": "string",
    "VpcId": "string"
  },
  "ExpirationTime": "string",
  "RequesterVpcInfo": {
    "CidrBlock": "string",
    "CidrBlockSet": [{
      "CidrBlock": "string"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "string"
    }],
    "OwnerId": "string",
    "PeeringOptions": {
      "AllowDnsResolutionFromRemoteVpc": boolean,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
      "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
    },
    "Region": "string",
    "VpcId": "string"
  },
  "Status": {
    "Code": "string",
    "Message": "string"
```

```
    },
    "VpcPeeringConnectionId": "string"
  },
  "AwsEcrContainerImage": {
    "Architecture": "string",
    "ImageDigest": "string",
    "ImagePublishedAt": "string",
    "ImageTags": ["string"],
    "RegistryId": "string",
    "RepositoryName": "string"
  },
  "AwsEcrRepository": {
    "Arn": "string",
    "ImageScanningConfiguration": {
      "ScanOnPush": boolean
    },
    "ImageTagMutability": "string",
    "LifecyclePolicy": {
      "LifecyclePolicyText": "string",
      "RegistryId": "string"
    },
    "RepositoryName": "string",
    "RepositoryPolicyText": "string"
  },
  "AwsEcsCluster": {
    "ActiveServicesCount": number,
    "CapacityProviders": ["string"],
    "ClusterArn": "string",
    "ClusterName": "string",
    "ClusterSettings": [{
      "Name": "string",
      "Value": "string"
    }],
    "Configuration": {
      "ExecuteCommandConfiguration": {
        "KmsKeyId": "string",
        "LogConfiguration": {
          "CloudWatchEncryptionEnabled": boolean,
          "CloudWatchLogGroupName": "string",
          "S3BucketName": "string",
          "S3EncryptionEnabled": boolean,
          "S3KeyPrefix": "string"
        },
        "Logging": "string"
      }
    }
  }
}
```

```

    }
  },
  "DefaultCapacityProviderStrategy": [{
    "Base": number,
    "CapacityProvider": "string",
    "Weight": number
  }],
  "RegisteredContainerInstancesCount": number,
  "RunningTasksCount": number,
  "Status": "string"
},
"AwsEcsContainer": {
  "Image": "string",
  "MountPoints": [{
    "ContainerPath": "string",
    "SourceVolume": "string"
  }],
  "Name": "string",
  "Privileged": boolean
},
"AwsEcsService": {
  "CapacityProviderStrategy": [{
    "Base": number,
    "CapacityProvider": "string",
    "Weight": number
  }],
  "Cluster": "string",
  "DeploymentConfiguration": {
    "DeploymentCircuitBreaker": {
      "Enable": boolean,
      "Rollback": boolean
    },
    "MaximumPercent": number,
    "MinimumHealthyPercent": number
  },
  "DeploymentController": {
    "Type": "string"
  },
  "DesiredCount": number,
  "EnableEcsManagedTags": boolean,
  "EnableExecuteCommand": boolean,
  "HealthCheckGracePeriodSeconds": number,
  "LaunchType": "string",
  "LoadBalancers": [{

```

```

    "ContainerName": "string",
    "ContainerPort": number,
    "LoadBalancerName": "string",
    "TargetGroupArn": "string"
  ]],
  "Name": "string",
  "NetworkConfiguration": {
    "AwsVpcConfiguration": {
      "AssignPublicIp": "string",
      "SecurityGroups": ["string"],
      "Subnets": ["string"]
    }
  },
  "PlacementConstraints": [{
    "Expression": "string",
    "Type": "string"
  }],
  "PlacementStrategies": [{
    "Field": "string",
    "Type": "string"
  }],
  "PlatformVersion": "string",
  "PropagateTags": "string",
  "Role": "string",
  "SchedulingStrategy": "string",
  "ServiceArn": "string",
  "ServiceName": "string",
  "ServiceRegistries": [{
    "ContainerName": "string",
    "ContainerPort": number,
    "Port": number,
    "RegistryArn": "string"
  }],
  "TaskDefinition": "string"
},
"AwsEcsTask": {
  "CreatedAt": "string",
  "ClusterArn": "string",
  "Group": "string",
  "StartedAt": "string",
  "StartedBy": "string",
  "TaskDefinitionArn": "string",
  "Version": number,
  "Volumes": [{

```

```
"Name": "string",
"Host": {
  "SourcePath": "string"
},
}],
"Containers": [{
  "Image": "string",
  "MountPoints": [{
    "ContainerPath": "string",
    "SourceVolume": "string"
  }],
  "Name": "string",
  "Privileged": boolean
}]
},
"AwsEcsTaskDefinition": {
  "ContainerDefinitions": [{
    "Command": ["string"],
    "Cpu": number,
    "DependsOn": [{
      "Condition": "string",
      "ContainerName": "string"
    }],
    "DisableNetworking": boolean,
    "DnsSearchDomains": ["string"],
    "DnsServers": ["string"],
    "DockerLabels": {
      "string": "string"
    },
    "DockerSecurityOptions": ["string"],
    "EntryPoint": ["string"],
    "Environment": [{
      "Name": "string",
      "Value": "string"
    }],
    "EnvironmentFiles": [{
      "Type": "string",
      "Value": "string"
    }],
    "Essential": boolean,
    "ExtraHosts": [{
      "Hostname": "string",
      "IpAddress": "string"
    }],
  }],
}
```

```
"FirelensConfiguration": {
  "Options": {
    "string": "string"
  },
  "Type": "string"
},
"HealthCheck": {
  "Command": ["string"],
  "Interval": number,
  "Retries": number,
  "StartPeriod": number,
  "Timeout": number
},
"Hostname": "string",
"Image": "string",
"Interactive": boolean,
"Links": ["string"],
"LinuxParameters": {
  "Capabilities": {
    "Add": ["string"],
    "Drop": ["string"]
  },
  "Devices": [{
    "ContainerPath": "string",
    "HostPath": "string",
    "Permissions": ["string"]
  }],
  "InitProcessEnabled": boolean,
  "MaxSwap": number,
  "SharedMemorySize": number,
  "Swappiness": number,
  "Tmpfs": [{
    "ContainerPath": "string",
    "MountOptions": ["string"],
    "Size": number
  }]
},
"LogConfiguration": {
  "LogDriver": "string",
  "Options": {
    "string": "string"
  },
  "SecretOptions": [{
    "Name": "string",
```

```
    "ValueFrom": "string"
  }],
},
"Memory": number,
"MemoryReservation": number,
"MountPoints": [{
  "ContainerPath": "string",
  "ReadOnly": boolean,
  "SourceVolume": "string"
}],
"Name": "string",
"PortMappings": [{
  "ContainerPort": number,
  "HostPort": number,
  "Protocol": "string"
}],
"Privileged": boolean,
"PseudoTerminal": boolean,
"ReadonlyRootFilesystem": boolean,
"RepositoryCredentials": {
  "CredentialsParameter": "string"
},
"ResourceRequirements": [{
  "Type": "string",
  "Value": "string"
}],
"Secrets": [{
  "Name": "string",
  "ValueFrom": "string"
}],
"StartTimeout": number,
"StopTimeout": number,
"SystemControls": [{
  "Namespace": "string",
  "Value": "string"
}],
"Ulimits": [{
  "HardLimit": number,
  "Name": "string",
  "SoftLimit": number
}],
"User": "string",
"VolumesFrom": [{
  "ReadOnly": boolean,
```

```
    "SourceContainer": "string"
  }],
  "WorkingDirectory": "string"
}],
"Cpu": "string",
"ExecutionRoleArn": "string",
"Family": "string",
"InferenceAccelerators": [{
  "DeviceName": "string",
  "DeviceType": "string"
}],
"IpcMode": "string",
"Memory": "string",
"NetworkMode": "string",
"PidMode": "string",
"PlacementConstraints": [{
  "Expression": "string",
  "Type": "string"
}],
"ProxyConfiguration": {
  "ContainerName": "string",
  "ProxyConfigurationProperties": [{
    "Name": "string",
    "Value": "string"
  }],
  "Type": "string"
},
"RequiresCompatibilities": ["string"],
"Status": "string",
"TaskRoleArn": "string",
"Volumes": [{
  "DockerVolumeConfiguration": {
    "Autoprovision": boolean,
    "Driver": "string",
    "DriverOpts": {
      "string": "string"
    },
    "Labels": {
      "string": "string"
    },
    "Scope": "string"
  },
  "EfsVolumeConfiguration": {
    "AuthorizationConfig": {
```



```

    "AccessPointId": "string",
    "Iam": "string"
  },
  "FilesystemId": "string",
  "RootDirectory": "string",
  "TransitEncryption": "string",
  "TransitEncryptionPort": number
},
"Host": {
  "SourcePath": "string"
},
"Name": "string"
}]
},
"AwsEfsAccessPoint": {
  "AccessPointId": "string",
  "Arn": "string",
  "ClientToken": "string",
  "FileSystemId": "string",
  "PosixUser": {
    "Gid": "string",
    "SecondaryGids": ["string"],
    "Uid": "string"
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": "string",
      "OwnerUid": "string",
      "Permissions": "string"
    },
    "Path": "string"
  }
},
"AwsEksCluster": {
  "Arn": "string",
  "CertificateAuthorityData": "string",
  "ClusterStatus": "string",
  "Endpoint": "string",
  "Logging": {
    "ClusterLogging": [{
      "Enabled": boolean,
      "Types": ["string"]
    }]
  }
},

```

```

    "Name": "string",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": boolean,
      "SecurityGroupIds": ["string"],
      "SubnetIds": ["string"]
    },
    "RoleArn": "string",
    "Version": "string"
  },
  "AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "string",
    "Cname": "string",
    "DateCreated": "string",
    "DateUpdated": "string",
    "Description": "string",
    "EndpointUrl": "string",
    "EnvironmentArn": "string",
    "EnvironmentId": "string",
    "EnvironmentLinks": [{
      "EnvironmentName": "string",
      "LinkName": "string"
    }],
    "EnvironmentName": "string",
    "OptionSettings": [{
      "Namespace": "string",
      "OptionName": "string",
      "ResourceName": "string",
      "Value": "string"
    }],
    "PlatformArn": "string",
    "SolutionStackName": "string",
    "Status": "string",
    "Tier": {
      "Name": "string",
      "Type": "string",
      "Version": "string"
    },
    "VersionLabel": "string"
  },
  "AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
      "DomainId": "string",
      "DomainName": "string",

```

```
"Endpoint": "string",
"Endpoints": {
  "string": "string"
},
"DomainEndpointOptions": {
  "EnforceHTTPS": boolean,
  "TLSSecurityPolicy": "string"
},
"ElasticsearchClusterConfig": {
  "DedicatedMasterCount": number,
  "DedicatedMasterEnabled": boolean,
  "DedicatedMasterType": "string",
  "InstanceCount": number,
  "InstanceType": "string",
  "ZoneAwarenessConfig": {
    "AvailabilityZoneCount": number
  },
  "ZoneAwarenessEnabled": boolean
},
"ElasticsearchVersion": "string",
"EncryptionAtRestOptions": {
  "Enabled": boolean,
  "KmsKeyId": "string"
},
"LogPublishingOptions": {
  "AuditLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  },
  "IndexSlowLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  },
  "SearchSlowLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  }
},
"NodeToNodeEncryptionOptions": {
  "Enabled": boolean
},
"ServiceSoftwareOptions": {
  "AutomatedUpdateDate": "string",
```

```

    "Cancellable": boolean,
    "CurrentVersion": "string",
    "Description": "string",
    "NewVersion": "string",
    "UpdateAvailable": boolean,
    "UpdateStatus": "string"
  },
  "VPCOptions": {
    "AvailabilityZones": [
      "string"
    ],
    "SecurityGroupIds": [
      "string"
    ],
    "SubnetIds": [
      "string"
    ],
    "VPCId": "string"
  }
},
"AwsElbLoadBalancer": {
  "AvailabilityZones": ["string"],
  "BackendServerDescriptions": [{
    "InstancePort": number,
    "PolicyNames": ["string"]
  }],
  "CanonicalHostedZoneName": "string",
  "CanonicalHostedZoneNameID": "string",
  "CreatedTime": "string",
  "DnsName": "string",
  "HealthCheck": {
    "HealthyThreshold": number,
    "Interval": number,
    "Target": "string",
    "Timeout": number,
    "UnhealthyThreshold": number
  },
  "Instances": [{
    "InstanceId": "string"
  }],
  "ListenerDescriptions": [{
    "Listener": {
      "InstancePort": number,
      "InstanceProtocol": "string",

```

```
    "LoadBalancerPort": number,
    "Protocol": "string",
    "SslCertificateId": "string"
  },
  "PolicyNames": ["string"]
}],
"LoadBalancerAttributes": {
  "AccessLog": {
    "EmitInterval": number,
    "Enabled": boolean,
    "S3BucketName": "string",
    "S3BucketPrefix": "string"
  },
  "ConnectionDraining": {
    "Enabled": boolean,
    "Timeout": number
  },
  "ConnectionSettings": {
    "IdleTimeout": number
  },
  "CrossZoneLoadBalancing": {
    "Enabled": boolean
  },
  "AdditionalAttributes": [{
    "Key": "string",
    "Value": "string"
  }]
},
"LoadBalancerName": "string",
"Policies": {
  "AppCookieStickinessPolicies": [{
    "CookieName": "string",
    "PolicyName": "string"
  }],
  "LbCookieStickinessPolicies": [{
    "CookieExpirationPeriod": number,
    "PolicyName": "string"
  }],
  "OtherPolicies": ["string"]
},
"Scheme": "string",
"SecurityGroups": ["string"],
"SourceSecurityGroup": {
  "GroupName": "string",
```

```

    "OwnerAlias": "string"
  },
  "Subnets": ["string"],
  "VpcId": "string"
},
"aws:elasticloadbalancing:LoadBalancer": {
  "AvailabilityZones": {
    "SubnetId": "string",
    "ZoneName": "string"
  },
  "CanonicalHostedZoneId": "string",
  "CreatedTime": "string",
  "DNSName": "string",
  "IpAddressType": "string",
  "LoadBalancerAttributes": [{
    "Key": "string",
    "Value": "string"
  }],
  "Scheme": "string",
  "SecurityGroups": ["string"],
  "State": {
    "Code": "string",
    "Reason": "string"
  },
  "Type": "string",
  "VpcId": "string"
},
"aws:elasticloadbalancing:LoadBalancerAttributes": {
  "Description": "string",
  "RegistryArn": "string",
  "RegistryName": "string"
},
"aws:elasticloadbalancing:LoadBalancerAttributes": {
  "Arn": "string",
  "Description": "string",
  "EndpointId": "string",
  "EndpointUrl": "string",
  "EventBuses": [
    {
      "EventBusArn": "string"
    },
    {
      "EventBusArn": "string"
    }
  ]
}

```

```
],
  "Name": "string",
  "ReplicationConfig": {
    "State": "string"
  },
  "RoleArn": "string",
  "RoutingConfig": {
    "FailoverConfig": {
      "Primary": {
        "HealthCheck": "string"
      },
      "Secondary": {
        "Route": "string"
      }
    }
  },
  "State": "string"
},
"AwsEventsEventBus": {
  "Arn": "string",
  "Name": "string",
  "Policy": "string"
},
"AwsGuardDutyDetector": {
  "FindingPublishingFrequency": "string",
  "ServiceRole": "string",
  "Status": "string",
  "DataSources": {
    "CloudTrail": {
      "Status": "string"
    },
    "DnsLogs": {
      "Status": "string"
    },
    "FlowLogs": {
      "Status": "string"
    },
    "S3Logs": {
      "Status": "string"
    },
    "Kubernetes": {
      "AuditLogs": {
        "Status": "string"
      }
    }
  }
}
```

```

    },
    "MalwareProtection": {
      "ScanEc2InstanceWithFindings": {
        "EbsVolumes": {
          "Status": "string"
        }
      },
      "ServiceRole": "string"
    }
  },
  "AwsIamAccessKey": {
    "AccessKeyId": "string",
    "AccountId": "string",
    "CreatedAt": "string",
    "PrincipalId": "string",
    "PrincipalName": "string",
    "PrincipalType": "string",
    "SessionContext": {
      "Attributes": {
        "CreationDate": "string",
        "MfaAuthenticated": boolean
      },
      "SessionIssuer": {
        "AccountId": "string",
        "Arn": "string",
        "PrincipalId": "string",
        "Type": "string",
        "UserName": "string"
      }
    },
    "Status": "string"
  },
  "AwsIamGroup": {
    "AttachedManagedPolicies": [{
      "PolicyArn": "string",
      "PolicyName": "string"
    }],
    "CreateDate": "string",
    "GroupId": "string",
    "GroupName": "string",
    "GroupPolicyList": [{
      "PolicyName": "string"
    }],

```



```
    "Path": "string"
  },
  "AwsIamPolicy": {
    "AttachmentCount": number,
    "CreateDate": "string",
    "DefaultVersionId": "string",
    "Description": "string",
    "IsAttachable": boolean,
    "Path": "string",
    "PermissionsBoundaryUsageCount": number,
    "PolicyId": "string",
    "PolicyName": "string",
    "PolicyVersionList": [{
      "CreateDate": "string",
      "IsDefaultVersion": boolean,
      "VersionId": "string"
    }],
    "UpdateDate": "string"
  },
  "AwsIamRole": {
    "AssumeRolePolicyDocument": "string",
    "AttachedManagedPolicies": [{
      "PolicyArn": "string",
      "PolicyName": "string"
    }],
    "CreateDate": "string",
    "InstanceProfileList": [{
      "Arn": "string",
      "CreateDate": "string",
      "InstanceProfileId": "string",
      "InstanceProfileName": "string",
      "Path": "string",
      "Roles": [{
        "Arn": "string",
        "AssumeRolePolicyDocument": "string",
        "CreateDate": "string",
        "Path": "string",
        "RoleId": "string",
        "RoleName": "string"
      }]
    }],
    "MaxSessionDuration": number,
    "Path": "string",
    "PermissionsBoundary": {
```

```

    "PermissionsBoundaryArn": "string",
    "PermissionsBoundaryType": "string"
  },
  "RoleId": "string",
  "RoleName": "string",
  "RolePolicyList": [{
    "PolicyName": "string"
  }]
},
"AwsIamUser": {
  "AttachedManagedPolicies": [{
    "PolicyArn": "string",
    "PolicyName": "string"
  }],
  "CreateDate": "string",
  "GroupList": ["string"],
  "Path": "string",
  "PermissionsBoundary": {
    "PermissionsBoundaryArn": "string",
    "PermissionsBoundaryType": "string"
  },
  "UserId": "string",
  "UserName": "string",
  "UserPolicyList": [{
    "PolicyName": "string"
  }]
},
"AwsKinesisStream": {
  "Arn": "string",
  "Name": "string",
  "RetentionPeriodHours": number,
  "ShardCount": number,
  "StreamEncryption": {
    "EncryptionType": "string",
    "KeyId": "string"
  }
},
"AwsKmsKey": {
  "AWSAccountId": "string",
  "CreationDate": "string",
  "Description": "string",
  "KeyId": "string",
  "KeyManager": "string",
  "KeyRotationStatus": boolean,

```

```
"KeyState": "string",
"Origin": "string"
},
"AwsLambdaFunction": {
  "Architectures": [
    "string"
  ],
  "Code": {
    "S3Bucket": "string",
    "S3Key": "string",
    "S3ObjectVersion": "string",
    "ZipFile": "string"
  },
  "CodeSha256": "string",
  "DeadLetterConfig": {
    "TargetArn": "string"
  },
  "Environment": {
    "Variables": {
      "Stage": "string"
    }
  },
  "Error": {
    "ErrorCode": "string",
    "Message": "string"
  }
},
"FunctionName": "string",
"Handler": "string",
"KmsKeyArn": "string",
"LastModified": "string",
"Layers": {
  "Arn": "string",
  "CodeSize": number
},
"PackageType": "string",
"RevisionId": "string",
"Role": "string",
"Runtime": "string",
"Timeout": integer,
"TracingConfig": {
  "Mode": "string"
},
"Version": "string",
"VpcConfig": {
```

```

    "SecurityGroupIds": ["string"],
    "SubnetIds": ["string"]
  },
  "MasterArn": "string",
  "MemorySize": number
},
"AwsLambdaLayerVersion": {
  "CompatibleRuntimes": [
    "string"
  ],
  "CreateDate": "string",
  "Version": number
},
"AwsMskCluster": {
  "ClusterInfo": {
    "ClientAuthentication": {
      "Sasl": {
        "Scram": {
          "Enabled": boolean
        },
        "Iam": {
          "Enabled": boolean
        }
      },
      "Tls": {
        "CertificateAuthorityArnList": [],
        "Enabled": boolean
      },
      "Unauthenticated": {
        "Enabled": boolean
      }
    },
    "ClusterName": "string",
    "CurrentVersion": "string",
    "EncryptionInfo": {
      "EncryptionAtRest": {
        "DataVolumeKMSKeyId": "string"
      },
      "EncryptionInTransit": {
        "ClientBroker": "string",
        "InCluster": boolean
      }
    }
  },
  "EnhancedMonitoring": "string",

```

```

    "NumberOfBrokerNodes": integer
  }
},
"AwsNetworkFirewallFirewall": {
  "DeleteProtection": boolean,
  "Description": "string",
  "FirewallArn": "string",
  "FirewallId": "string",
  "FirewallName": "string",
  "FirewallPolicyArn": "string",
  "FirewallPolicyChangeProtection": boolean,
  "SubnetChangeProtection": boolean,
  "SubnetMappings": [{
    "SubnetId": "string"
  }],
  "VpcId": "string"
},
"AwsNetworkFirewallFirewallPolicy": {
  "Description": "string",
  "FirewallPolicy": {
    "StatefulRuleGroupReferences": [{
      "ResourceArn": "string"
    }],
    "StatelessCustomActions": [{
      "ActionDefinition": {
        "PublishMetricAction": {
          "Dimensions": [{
            "Value": "string"
          }]
        }
      }
    ]
  },
  "ActionName": "string"
}],
  "StatelessDefaultActions": ["string"],
  "StatelessFragmentDefaultActions": ["string"],
  "StatelessRuleGroupReferences": [{
    "Priority": number,
    "ResourceArn": "string"
  }]
},
  "FirewallPolicyArn": "string",
  "FirewallPolicyId": "string",
  "FirewallPolicyName": "string"
},

```

```

"AwsNetworkFirewallRuleGroup": {
  "Capacity": number,
  "Description": "string",
  "RuleGroup": {
    "RulesSource": {
      "RulesSourceList": {
        "GeneratedRulesType": "string",
        "Targets": ["string"],
        "TargetTypes": ["string"]
      },
      "RulesString": "string",
      "StatefulRules": [{
        "Action": "string",
        "Header": {
          "Destination": "string",
          "DestinationPort": "string",
          "Direction": "string",
          "Protocol": "string",
          "Source": "string",
          "SourcePort": "string"
        },
        "RuleOptions": [{
          "Keyword": "string",
          "Settings": ["string"]
        }]
      }],
      "StatelessRulesAndCustomActions": {
        "CustomActions": [{
          "ActionDefinition": {
            "PublishMetricAction": {
              "Dimensions": [{
                "Value": "string"
              }]
            }
          },
          "ActionName": "string"
        }],
        "StatelessRules": [{
          "Priority": number,
          "RuleDefinition": {
            "Actions": ["string"],
            "MatchAttributes": {
              "DestinationPorts": [{
                "FromPort": number,

```

```

        "ToPort": number
      }],
      "Destinations": [{
        "AddressDefinition": "string"
      }],
      "Protocols": [number],
      "SourcePorts": [{
        "FromPort": number,
        "ToPort": number
      }],
      "Sources": [{
        "AddressDefinition": "string"
      }],
      "TcpFlags": [{
        "Flags": ["string"],
        "Masks": ["string"]
      }]
    }
  }
}]
},
"RuleVariables": {
  "IpSets": {
    "Definition": ["string"]
  },
  "PortSets": {
    "Definition": ["string"]
  }
},
"RuleGroupArn": "string",
"RuleGroupId": "string",
"RuleGroupName": "string",
"Type": "string"
},
"AwsOpenSearchServiceDomain": {
  "AccessPolicies": "string",
  "AdvancedSecurityOptions": {
    "Enabled": boolean,
    "InternalUserDatabaseEnabled": boolean,
    "MasterUserOptions": {
      "MasterUserArn": "string",
      "MasterUserName": "string",

```

```
    "MasterUserPassword": "string"
  },
  "Arn": "string",
  "ClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,
    "InstanceType": "string",
    "WarmCount": number,
    "WarmEnabled": boolean,
    "WarmType": "string",
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": number
    },
    "ZoneAwarenessEnabled": boolean
  },
  "DomainEndpoint": "string",
  "DomainEndpointOptions": {
    "CustomEndpoint": "string",
    "CustomEndpointCertificateArn": "string",
    "CustomEndpointEnabled": boolean,
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "DomainEndpoints": {
    "string": "string"
  },
  "DomainName": "string",
  "EncryptionAtRestOptions": {
    "Enabled": boolean,
    "KmsKeyId": "string"
  },
  "EngineVersion": "string",
  "Id": "string",
  "LogPublishingOptions": {
    "AuditLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    },
    "IndexSlowLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    }
  }
}
```



```

    },
    "SearchSlowLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    }
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": boolean
  },
  "ServiceSoftwareOptions": {
    "AutomatedUpdateDate": "string",
    "Cancellable": boolean,
    "CurrentVersion": "string",
    "Description": "string",
    "NewVersion": "string",
    "OptionalDeployment": boolean,
    "UpdateAvailable": boolean,
    "UpdateStatus": "string"
  },
  "VpcOptions": {
    "SecurityGroupIds": ["string"],
    "SubnetIds": ["string"]
  }
},
"AwsRdsDbCluster": {
  "ActivityStreamStatus": "string",
  "AllocatedStorage": number,
  "AssociatedRoles": [{
    "RoleArn": "string",
    "Status": "string"
  }],
  "AutoMinorVersionUpgrade": boolean,
  "AvailabilityZones": ["string"],
  "BackupRetentionPeriod": integer,
  "ClusterCreateTime": "string",
  "CopyTagsToSnapshot": boolean,
  "CrossAccountClone": boolean,
  "CustomEndpoints": ["string"],
  "DatabaseName": "string",
  "DbClusterIdentifier": "string",
  "DbClusterMembers": [{
    "DbClusterParameterGroupStatus": "string",
    "DbInstanceIdentifier": "string",
    "IsClusterWriter": boolean,

```

```

    "PromotionTier": integer
  }],
  "DbClusterOptionGroupMemberships": [{
    "DbClusterOptionGroupName": "string",
    "Status": "string"
  }],
  "DbClusterParameterGroup": "string",
  "DbClusterResourceId": "string",
  "DbSubnetGroup": "string",
  "DeletionProtection": boolean,
  "DomainMemberships": [{
    "Domain": "string",
    "Fqdn": "string",
    "IamRoleName": "string",
    "Status": "string"
  }],
  "EnabledCloudwatchLogsExports": ["string"],
  "Endpoint": "string",
  "Engine": "string",
  "EngineMode": "string",
  "EngineVersion": "string",
  "HostedZoneId": "string",
  "HttpEndpointEnabled": boolean,
  "IamDatabaseAuthenticationEnabled": boolean,
  "KmsKeyId": "string",
  "MasterUsername": "string",
  "MultiAz": boolean,
  "Port": integer,
  "PreferredBackupWindow": "string",
  "PreferredMaintenanceWindow": "string",
  "ReaderEndpoint": "string",
  "ReadReplicaIdentifiers": ["string"],
  "Status": "string",
  "StorageEncrypted": boolean,
  "VpcSecurityGroups": [{
    "Status": "string",
    "VpcSecurityGroupId": "string"
  }]
},
"AwsRdsDbClusterSnapshot": {
  "AllocatedStorage": integer,
  "AvailabilityZones": ["string"],
  "ClusterCreateTime": "string",
  "DbClusterIdentifier": "string",

```

```

    "DbClusterSnapshotAttributes": [{
      "AttributeName": "string",
      "AttributeValues": ["string"]
    }],
    "DbClusterSnapshotIdentifier": "string",
    "Engine": "string",
    "EngineVersion": "string",
    "IamDatabaseAuthenticationEnabled": boolean,
    "KmsKeyId": "string",
    "LicenseModel": "string",
    "MasterUsername": "string",
    "PercentProgress": integer,
    "Port": integer,
    "SnapshotCreateTime": "string",
    "SnapshotType": "string",
    "Status": "string",
    "StorageEncrypted": boolean,
    "VpcId": "string"
  },
  "AwsRdsDbInstance": {
    "AllocatedStorage": number,
    "AssociatedRoles": [{
      "RoleArn": "string",
      "FeatureName": "string",
      "Status": "string"
    }],
    "AutoMinorVersionUpgrade": boolean,
    "AvailabilityZone": "string",
    "BackupRetentionPeriod": number,
    "CACertificateIdentifier": "string",
    "CharacterSetName": "string",
    "CopyTagsToSnapshot": boolean,
    "DBClusterIdentifier": "string",
    "DBInstanceClass": "string",
    "DBInstanceIdentifier": "string",
    "DbInstancePort": number,
    "DbInstanceStatus": "string",
    "DbiResourceId": "string",
    "DBName": "string",
    "DbParameterGroups": [{
      "DbParameterGroupName": "string",
      "ParameterApplyStatus": "string"
    }],
    "DbSecurityGroups": ["string"],

```

```
"DbSubnetGroup": {
  "DbSubnetGroupArn": "string",
  "DbSubnetGroupDescription": "string",
  "DbSubnetGroupName": "string",
  "SubnetGroupStatus": "string",
  "Subnets": [{
    "SubnetAvailabilityZone": {
      "Name": "string"
    },
    "SubnetIdentifier": "string",
    "SubnetStatus": "string"
  }],
  "VpcId": "string"
},
"DeletionProtection": boolean,
"Endpoint": {
  "Address": "string",
  "Port": number,
  "HostedZoneId": "string"
},
"DomainMemberships": [{
  "Domain": "string",
  "Fqdn": "string",
  "IamRoleName": "string",
  "Status": "string"
}],
"EnabledCloudwatchLogsExports": ["string"],
"Engine": "string",
"EngineVersion": "string",
"EnhancedMonitoringResourceArn": "string",
"IAMDatabaseAuthenticationEnabled": boolean,
"InstanceCreateTime": "string",
"Iops": number,
"KmsKeyId": "string",
"LatestRestorableTime": "string",
"LicenseModel": "string",
"ListenerEndpoint": {
  "Address": "string",
  "HostedZoneId": "string",
  "Port": number
},
"MasterUsername": "admin",
"MaxAllocatedStorage": number,
"MonitoringInterval": number,
```

```
"MonitoringRoleArn": "string",
"MultiAz": boolean,
"OptionGroupMemberships": [{
  "OptionGroupName": "string",
  "Status": "string"
}],
"PendingModifiedValues": {
  "AllocatedStorage": number,
  "BackupRetentionPeriod": number,
  "CaCertificateIdentifier": "string",
  "DbInstanceClass": "string",
  "DbInstanceIdentifier": "string",
  "DbSubnetGroupName": "string",
  "EngineVersion": "string",
  "Iops": number,
  "LicenseModel": "string",
  "MasterUserPassword": "string",
  "MultiAZ": boolean,
  "PendingCloudWatchLogsExports": {
    "LogTypesToDisable": ["string"],
    "LogTypesToEnable": ["string"]
  },
  "Port": number,
  "ProcessorFeatures": [{
    "Name": "string",
    "Value": "string"
  }],
  "StorageType": "string"
},
"PerformanceInsightsEnabled": boolean,
"PerformanceInsightsKmsKeyId": "string",
"PerformanceInsightsRetentionPeriod": number,
"PreferredBackupWindow": "string",
"PreferredMaintenanceWindow": "string",
"ProcessorFeatures": [{
  "Name": "string",
  "Value": "string"
}],
"PromotionTier": number,
"PubliclyAccessible": boolean,
"ReadReplicaDBClusterIdentifiers": ["string"],
"ReadReplicaDBInstanceIdentifiers": ["string"],
"ReadReplicaSourceDBInstanceIdentifier": "string",
"SecondaryAvailabilityZone": "string",
```

```

    "StatusInfos": [{
      "Message": "string",
      "Normal": boolean,
      "Status": "string",
      "StatusType": "string"
    }],
    "StorageEncrypted": boolean,
    "TdeCredentialArn": "string",
    "Timezone": "string",
    "VpcSecurityGroups": [{
      "VpcSecurityGroupId": "string",
      "Status": "string"
    }]
  },
  "AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "string",
    "DbSecurityGroupDescription": "string",
    "DbSecurityGroupName": "string",
    "Ec2SecurityGroups": [{
      "Ec2SecurityGroupArn": "string",
      "Ec2SecurityGroupName": "string",
      "Ec2SecurityGroupOwnerId": "string",
      "Status": "string"
    }],
    "IpRanges": [{
      "CidrIp": "string",
      "Status": "string"
    }],
    "OwnerId": "string",
    "VpcId": "string"
  },
  "AwsRdsDbSnapshot": {
    "AllocatedStorage": integer,
    "AvailabilityZone": "string",
    "DbInstanceIdentifier": "string",
    "DbiResourceId": "string",
    "DbSnapshotIdentifier": "string",
    "Encrypted": boolean,
    "Engine": "string",
    "EngineVersion": "string",
    "IamDatabaseAuthenticationEnabled": boolean,
    "InstanceCreateTime": "string",
    "Iops": number,
    "KmsKeyId": "string",

```

```

    "LicenseModel": "string",
    "MasterUsername": "string",
    "OptionGroupName": "string",
    "PercentProgress": integer,
    "Port": integer,
    "ProcessorFeatures": [],
    "SnapshotCreateTime": "string",
    "SnapshotType": "string",
    "SourceDbSnapshotIdentifier": "string",
    "SourceRegion": "string",
    "Status": "string",
    "StorageType": "string",
    "TdeCredentialArn": "string",
    "Timezone": "string",
    "VpcId": "string"
  },
  "AwsRdsEventSubscription": {
    "CustomerAwsId": "string",
    "CustSubscriptionId": "string",
    "Enabled": boolean,
    "EventCategoriesList": ["string"],
    "EventSubscriptionArn": "string",
    "SnsTopicArn": "string",
    "SourceIdsList": ["string"],
    "SourceType": "string",
    "Status": "string",
    "SubscriptionCreationTime": "string"
  },
  "AwsRedshiftCluster": {
    "AllowVersionUpgrade": boolean,
    "AutomatedSnapshotRetentionPeriod": number,
    "AvailabilityZone": "string",
    "ClusterAvailabilityStatus": "string",
    "ClusterCreateTime": "string",
    "ClusterIdentifier": "string",
    "ClusterNodes": [{
      "NodeRole": "string",
      "PrivateIpAddress": "string",
      "PublicIpAddress": "string"
    }],
    "ClusterParameterGroups": [{
      "ClusterParameterStatusList": [{
        "ParameterApplyErrorDescription": "string",
        "ParameterApplyStatus": "string",

```

```

    "ParameterName": "string"
  ]],
  "ParameterApplyStatus": "string",
  "ParameterGroupName": "string"
  ]],
  "ClusterPublicKey": "string",
  "ClusterRevisionNumber": "string",
  "ClusterSecurityGroups": [{
    "ClusterSecurityGroupName": "string",
    "Status": "string"
  }],
  "ClusterSnapshotCopyStatus": {
    "DestinationRegion": "string",
    "ManualSnapshotRetentionPeriod": number,
    "RetentionPeriod": number,
    "SnapshotCopyGrantName": "string"
  },
  "ClusterStatus": "string",
  "ClusterSubnetGroupName": "string",
  "ClusterVersion": "string",
  "DBName": "string",
  "DeferredMaintenanceWindows": [{
    "DeferMaintenanceEndTime": "string",
    "DeferMaintenanceIdentifier": "string",
    "DeferMaintenanceStartTime": "string"
  }],
  "ElasticIpStatus": {
    "ElasticIp": "string",
    "Status": "string"
  },
  "ElasticResizeNumberOfNodeOptions": "string",
  "Encrypted": boolean,
  "Endpoint": {
    "Address": "string",
    "Port": number
  },
  "EnhancedVpcRouting": boolean,
  "ExpectedNextSnapshotScheduleTime": "string",
  "ExpectedNextSnapshotScheduleTimeStatus": "string",
  "HsmStatus": {
    "HsmClientCertificateIdentifier": "string",
    "HsmConfigurationIdentifier": "string",
    "Status": "string"
  },
  },

```



```

"IamRoles": [{
  "ApplyStatus": "string",
  "IamRoleArn": "string"
}],
"KmsKeyId": "string",
"LoggingStatus":{
  "BucketName": "string",
  "LastFailureMessage": "string",
  "LastFailureTime": "string",
  "LastSuccessfulDeliveryTime": "string",
  "LoggingEnabled": boolean,
  "S3KeyPrefix": "string"
},
"MaintenanceTrackName": "string",
"ManualSnapshotRetentionPeriod": number,
"MasterUsername": "string",
"NextMaintenanceWindowStartTime": "string",
"NodeType": "string",
"NumberOfNodes": number,
"PendingActions": ["string"],
"PendingModifiedValues": {
  "AutomatedSnapshotRetentionPeriod": number,
  "ClusterIdentifier": "string",
  "ClusterType": "string",
  "ClusterVersion": "string",
  "EncryptionType": "string",
  "EnhancedVpcRouting": boolean,
  "MaintenanceTrackName": "string",
  "MasterUserPassword": "string",
  "NodeType": "string",
  "NumberOfNodes": number,
  "PubliclyAccessible": "string"
},
"PreferredMaintenanceWindow": "string",
"PubliclyAccessible": boolean,
"ResizeInfo": {
  "AllowCancelResize": boolean,
  "ResizeType": "string"
},
"RestoreStatus": {
  "CurrentRestoreRateInMegaBytesPerSecond": number,
  "ElapsedTimeInSeconds": number,
  "EstimatedTimeToCompletionInSeconds": number,
  "ProgressInMegaBytes": number,

```

```

    "SnapshotSizeInMegaBytes": number,
    "Status": "string"
  },
  "SnapshotScheduleIdentifier": "string",
  "SnapshotScheduleState": "string",
  "VpcId": "string",
  "VpcSecurityGroups": [{
    "Status": "string",
    "VpcSecurityGroupId": "string"
  }]
},
"AwsRoute53HostedZone": {
  "HostedZone": {
    "Id": "string",
    "Name": "string",
    "Config": {
      "Comment": "string"
    }
  },
  "NameServers": ["string"],
  "QueryLoggingConfig": {
    "CloudWatchLogsLogGroupArn": {
      "CloudWatchLogsLogGroupArn": "string",
      "Id": "string",
      "HostedZoneId": "string"
    }
  },
  "Vpcs": [
    {
      "Id": "string",
      "Region": "string"
    }
  ]
},
"AwsS3AccessPoint": {
  "AccessPointArn": "string",
  "Alias": "string",
  "Bucket": "string",
  "BucketAccountId": "string",
  "Name": "string",
  "NetworkOrigin": "string",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": boolean,
    "BlockPublicPolicy": boolean,

```

```

    "IgnorePublicAcls": boolean,
    "RestrictPublicBuckets": boolean
  },
  "VpcConfiguration": {
    "VpcId": "string"
  }
},
"AwsS3AccountPublicAccessBlock": {
  "BlockPublicAcls": boolean,
  "BlockPublicPolicy": boolean,
  "IgnorePublicAcls": boolean,
  "RestrictPublicBuckets": boolean
},
"AwsS3Bucket": {
  "AccessControlList": "string",
  "BucketLifecycleConfiguration": {
    "Rules": [{
      "AbortIncompleteMultipartUpload": {
        "DaysAfterInitiation": number
      },
      "ExpirationDate": "string",
      "ExpirationInDays": number,
      "ExpiredObjectDeleteMarker": boolean,
      "Filter": {
        "Predicate": {
          "Operands": [{
            "Prefix": "string",
            "Type": "string"
          },
          {
            "Tag": {
              "Key": "string",
              "Value": "string"
            },
            "Type": "string"
          }
        ],
        "Type": "string"
      }
    }
  ],
  "Id": "string",
  "NoncurrentVersionExpirationInDays": number,
  "NoncurrentVersionTransitions": [{
    "Days": number,

```

```
    "StorageClass": "string"
  }],
  "Prefix": "string",
  "Status": "string",
  "Transitions": [{
    "Date": "string",
    "Days": number,
    "StorageClass": "string"
  }]
}]
},
"BucketLoggingConfiguration": {
  "DestinationBucketName": "string",
  "LogFilePrefix": "string"
},
"BucketName": "string",
"BucketNotificationConfiguration": {
  "Configurations": [{
    "Destination": "string",
    "Events": ["string"],
    "Filter": {
      "S3KeyFilter": {
        "FilterRules": [{
          "Name": "string",
          "Value": "string"
        }]
      }
    }
  }],
  "Type": "string"
}],
"BucketVersioningConfiguration": {
  "IsMfaDeleteEnabled": boolean,
  "Status": "string"
},
"BucketWebsiteConfiguration": {
  "ErrorDocument": "string",
  "IndexDocumentSuffix": "string",
  "RedirectAllRequestsTo": {
    "HostName": "string",
    "Protocol": "string"
  },
  "RoutingRules": [{
    "Condition": {
```

```

    "HttpErrorCodeReturnedEquals": "string",
    "KeyPrefixEquals": "string"
  },
  "Redirect": {
    "HostName": "string",
    "HttpRedirectCode": "string",
    "Protocol": "string",
    "ReplaceKeyPrefixWith": "string",
    "ReplaceKeyWith": "string"
  }
}]
},
"CreatedAt": "string",
"ObjectLockConfiguration": {
  "ObjectLockEnabled": "string",
  "Rule": {
    "DefaultRetention": {
      "Days": integer,
      "Mode": "string",
      "Years": integer
    }
  }
},
"OwnerAccountId": "string",
"OwnerId": "string",
"OwnerName": "string",
"PublicAccessBlockConfiguration": {
  "BlockPublicAcls": boolean,
  "BlockPublicPolicy": boolean,
  "IgnorePublicAcls": boolean,
  "RestrictPublicBuckets": boolean
},
"ServerSideEncryptionConfiguration": {
  "Rules": [{
    "ApplyServerSideEncryptionByDefault": {
      "KMSEMasterKeyID": "string",
      "SSEAlgorithm": "string"
    }
  }]
}
},
"AwsS3Object": {
  "ContentType": "string",
  "ETag": "string",

```

```
"LastModified": "string",
"ServerSideEncryption": "string",
"SSEKMSKeyId": "string",
"VersionId": "string"
},
"AwsSagemakerNotebookInstance": {
  "DirectInternetAccess": "string",
  "InstanceMetadataServiceConfiguration": {
    "MinimumInstanceMetadataServiceVersion": "string"
  },
  "InstanceType": "string",
  "LastModifiedTime": "string",
  "NetworkInterfaceId": "string",
  "NotebookInstanceArn": "string",
  "NotebookInstanceName": "string",
  "NotebookInstanceStatus": "string",
  "PlatformIdentifier": "string",
  "RoleArn": "string",
  "RootAccess": "string",
  "SecurityGroups": ["string"],
  "SubnetId": "string",
  "Url": "string",
  "VolumeSizeInGB": number
},
"AwsSecretsManagerSecret": {
  "Deleted": boolean,
  "Description": "string",
  "KmsKeyId": "string",
  "Name": "string",
  "RotationEnabled": boolean,
  "RotationLambdaArn": "string",
  "RotationOccurredWithinFrequency": boolean,
  "RotationRules": {
    "AutomaticallyAfterDays": integer
  }
},
"AwsSnsTopic": {
  "ApplicationSuccessFeedbackRoleArn": "string",
  "FirehoseFailureFeedbackRoleArn": "string",
  "FirehoseSuccessFeedbackRoleArn": "string",
  "HttpFailureFeedbackRoleArn": "string",
  "HttpSuccessFeedbackRoleArn": "string",
  "KmsMasterKeyId": "string",
  "Owner": "string",
```

```

    "SqsFailureFeedbackRoleArn": "string",
    "SqsSuccessFeedbackRoleArn": "string",
    "Subscription": {
        "Endpoint": "string",
        "Protocol": "string"
    },
    "TopicName": "string"
},
"AwsSqsQueue": {
    "DeadLetterTargetArn": "string",
    "KmsDataKeyReusePeriodSeconds": number,
    "KmsMasterKeyId": "string",
    "QueueName": "string"
},
"AwsSsmPatchCompliance": {
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "string",
            "CompliantCriticalCount": integer,
            "CompliantHighCount": integer,
            "CompliantInformationalCount": integer,
            "CompliantLowCount": integer,
            "CompliantMediumCount": integer,
            "CompliantUnspecifiedCount": integer,
            "ExecutionType": "string",
            "NonCompliantCriticalCount": integer,
            "NonCompliantHighCount": integer,
            "NonCompliantInformationalCount": integer,
            "NonCompliantLowCount": integer,
            "NonCompliantMediumCount": integer,
            "NonCompliantUnspecifiedCount": integer,
            "OverallSeverity": "string",
            "PatchBaselineId": "string",
            "PatchGroup": "string",
            "Status": "string"
        }
    }
},
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "string",
    "Name": "string",
    "Status": "string",
    "RoleArn": "string",
    "Type": "string",

```

```
"LoggingConfiguration": {
  "Level": "string",
  "IncludeExecutionData": boolean
},
"TracingConfiguration": {
  "Enabled": boolean
}
},
"AwsWafRateBasedRule": {
  "MatchPredicates": [{
    "DataId": "string",
    "Negated": boolean,
    "Type": "string"
  }],
  "MetricName": "string",
  "Name": "string",
  "RateKey": "string",
  "RateLimit": number,
  "RuleId": "string"
},
"AwsWafRegionalRateBasedRule": {
  "MatchPredicates": [{
    "DataId": "string",
    "Negated": boolean,
    "Type": "string"
  }],
  "MetricName": "string",
  "Name": "string",
  "RateKey": "string",
  "RateLimit": number,
  "RuleId": "string"
},
"AwsWafRegionalRule": {
  "MetricName": "string",
  "Name": "string",
  "RuleId": "string",
  "PredicateList": [{
    "DataId": "string",
    "Negated": boolean,
    "Type": "string"
  }]
},
"AwsWafRegionalRuleGroup": {
  "MetricName": "string",
```



```
"Name": "string",
"RuleGroupId": "string",
"Rules": [{
  "Action": {
    "Type": "string"
  },
  "Priority": number,
  "RuleId": "string",
  "Type": "string"
}]
},
"AwsWafRegionalWebAcl": {
  "DefaultAction": "string",
  "MetricName": "string",
  "Name": "string",
  "RulesList": [{
    "Action": {
      "Type": "string"
    },
    "Priority": number,
    "RuleId": "string",
    "Type": "string",
    "ExcludedRules": [{
      "ExclusionType": "string",
      "RuleId": "string"
    }],
    "OverrideAction": {
      "Type": "string"
    }
  }],
  "WebAclId": "string"
},
"AwsWafRule": {
  "MetricName": "string",
  "Name": "string",
  "PredicateList": [{
    "DataId": "string",
    "Negated": boolean,
    "Type": "string"
  }],
  "RuleId": "string"
},
"AwsWafRuleGroup": {
  "MetricName": "string",
```

```
"Name": "string",
"RuleGroupId": "string",
"Rules": [{
  "Action": {
    "Type": "string"
  },
  "Priority": number,
  "RuleId": "string",
  "Type": "string"
}]
},
"AwsWafv2RuleGroup": {
  "Arn": "string",
  "Capacity": number,
  "Description": "string",
  "Id": "string",
  "Name": "string",
  "Rules": [{
    "Action": {
      "Allow": {
        "CustomRequestHandling": {
          "InsertHeaders": [
            {
              "Name": "string",
              "Value": "string"
            },
            {
              "Name": "string",
              "Value": "string"
            }
          ]
        }
      }
    }
  ]
},
  "Name": "string",
  "Priority": number,
  "VisibilityConfig": {
    "CloudWatchMetricsEnabled": boolean,
    "MetricName": "string",
    "SampledRequestsEnabled": boolean
  }
}],
"VisibilityConfig": {
  "CloudWatchMetricsEnabled": boolean,
```

```
    "MetricName": "string",
    "SampledRequestsEnabled": boolean
  },
  "AwsWafWebAcl": {
    "DefaultAction": "string",
    "Name": "string",
    "Rules": [{
      "Action": {
        "Type": "string"
      },
      "ExcludedRules": [{
        "RuleId": "string"
      }],
      "OverrideAction": {
        "Type": "string"
      },
      "Priority": number,
      "RuleId": "string",
      "Type": "string"
    }],
    "WebAclId": "string"
  },
  "AwsWafv2WebAcl": {
    "Arn": "string",
    "Capacity": number,
    "CaptchaConfig": {
      "ImmunityTimeProperty": {
        "ImmunityTime": number
      }
    },
    "DefaultAction": {
      "Block": {}
    },
    "Description": "string",
    "ManagedbyFirewallManager": boolean,
    "Name": "string",
    "Rules": [{
      "Action": {
        "RuleAction": {
          "Block": {}
        }
      }
    }],
    "Name": "string",
```

```

    "Priority": number,
    "VisibilityConfig": {
      "SampledRequestsEnabled": boolean,
      "CloudWatchMetricsEnabled": boolean,
      "MetricName": "string"
    }
  ]],
  "VisibilityConfig": {
    "SampledRequestsEnabled": boolean,
    "CloudWatchMetricsEnabled": boolean,
    "MetricName": "string"
  },
  "AwsXrayEncryptionConfig": {
    "KeyId": "string",
    "Status": "string",
    "Type": "string"
  },
  "CodeRepository": {
    "CodeSecurityIntegrationArn": "string",
    "ProjectName": "string",
    "ProviderType": "string"
  },
  "Container": {
    "ContainerRuntime": "string",
    "ImageId": "string",
    "ImageName": "string",
    "LaunchedAt": "string",
    "Name": "string",
    "Privileged": boolean,
    "VolumeMounts": [{
      "Name": "string",
      "MountPath": "string"
    }]
  },
  "Other": {
    "string": "string"
  },
  "Id": "string",
  "Partition": "string",
  "Region": "string",
  "ResourceRole": "string",
  "Tags": {
    "string": "string"
  }

```

```
    },
    "Type": "string"
  ]],
  "SchemaVersion": "string",
  "Severity": {
    "Label": "string",
    "Normalized": number,
    "Original": "string"
  },
  "Sample": boolean,
  "SourceUrl": "string",
  "Threats": [{
    "FilePaths": [{
      "FileName": "string",
      "FilePath": "string",
      "Hash": "string",
      "ResourceId": "string"
    }],
    "ItemCount": number,
    "Name": "string",
    "Severity": "string"
  }],
  "ThreatIntelIndicators": [{
    "Category": "string",
    "LastObservedAt": "string",
    "Source": "string",
    "SourceUrl": "string",
    "Type": "string",
    "Value": "string"
  }],
  "Title": "string",
  "Types": ["string"],
  "UpdatedAt": "string",
  "UserDefinedFields": {
    "string": "string"
  },
  "VerificationState": "string",
  "Vulnerabilities": [{
    "CodeVulnerabilities": [{
      "Cwes": [
        "string",
        "string"
      ],
      "FilePath": {
```

```
    "EndLine": integer,
    "FileName": "string",
    "FilePath": "string",
    "StartLine": integer
  },
  "SourceArn": "string"
}],
"Cvss": [{
  "Adjustments": [{
    "Metric": "string",
    "Reason": "string"
  }],
  "BaseScore": number,
  "BaseVector": "string",
  "Source": "string",
  "Version": "string"
}],
"EpssScore": number,
"ExploitAvailable": "string",
"FixAvailable": "string",
"Id": "string",
"LastKnownExploitAt": "string",
"ReferenceUrls": ["string"],
"RelatedVulnerabilities": ["string"],
"Vendor": {
  "Name": "string",
  "Url": "string",
  "VendorCreatedAt": "string",
  "VendorSeverity": "string",
  "VendorUpdatedAt": "string"
},
"VulnerablePackages": [{
  "Architecture": "string",
  "Epoch": "string",
  "FilePath": "string",
  "FixedInVersion": "string",
  "Name": "string",
  "PackageManager": "string",
  "Release": "string",
  "Remediation": "string",
  "SourceLayerArn": "string",
  "SourceLayerHash": "string",
  "Version": "string"
}]
}]
```

```
    }],  
    "Workflow": {  
      "Status": "string"  
    },  
    "WorkflowState": "string"  
  }  
]
```

整合對 ASFF 欄位和值的影響

AWS Security Hub CSPM 為控制項提供兩種類型的整合：

- 合併控制項檢視 – 使用這種類型的合併，每個控制項在所有標準中都有一個識別符。此外，在 Security Hub CSPM 主控台上，控制頁面會顯示所有標準的所有控制項。
- 合併控制問題清單 – 使用這種類型的整合，Security Hub CSPM 會為控制項產生單一問題清單，即使控制項適用於多個啟用的標準。這可以減少問題清單雜訊。

您無法啟用或停用合併控制項檢視。如果您在 2023 年 2 月 23 日或之後啟用 Security Hub CSPM，則預設會啟用合併控制問題清單。否則，預設為停用。不過，對於組織，只有在管理員帳戶啟用合併控制問題清單時，才會為 Security Hub CSPM 成員帳戶啟用合併控制問題清單。若要進一步了解合併控制問題清單，請參閱 [產生和更新控制問題清單](#)。

這兩種類型的合併都會影響 中控制項調查結果的欄位和值 [AWS 安全調查結果格式 \(ASFF\)](#)。

主題

- [合併控制項檢視 – ASFF 變更](#)
- [合併控制調查結果 – ASFF 變更](#)
- [啟用合併控制調查結果前後IDs](#)
- [合併如何影響控制 IDs和標題](#)
- [更新整合的工作流程](#)

合併控制項檢視 – ASFF 變更

合併控制項檢視功能對 ASFF 中控制項調查結果的欄位和值進行了下列變更。如果您的工作流程不依賴這些 ASFF 欄位的值，則不需要採取任何動作。如果您有依賴這些欄位特定值的工作流程，請更新您的工作流程以使用目前的值。

ASFF 欄位	合併控制項檢視之前的範本值	合併控制項檢視之後的範例值，以及變更的說明
Compliance.SecurityControlId	不適用（新欄位）	EC2.2 跨標準引進單一控制項 ID。 ProductFields.RuleId 仍然為 CIS v1.2.0 控制項提供標準型控制項 ID。 ProductFields.ControlId 仍然為其他標準中的控制項提供標準型控制項 ID。
Compliance.AssociatedStandards	不適用（新欄位）	【{"StandardsId": "standard s/aws-foundational-security- best-practices/v/1.0.0"}】 顯示要在哪些標準中啟用控制項。
ProductFields.ArchivalReasons:0/Description	不適用（新欄位）	「調查結果處於封存狀態，因為已開啟或關閉合併控制調查結果。這會導致在產生新問題清單時封存先前狀態的問題清單。」 說明 Security Hub CSPM 封存現有問題清單的原因。
ProductFields.ArchivalReasons:0/ReasonCode	不適用（新欄位）	「CONSOLIDATED_CONTROL_FINDINGS_UPDATE」 提供 Security Hub CSPM 已封存現有問題清單的原因。
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation

ASFF 欄位	合併控制項檢視之前的範本值	合併控制項檢視之後的範例值，以及變更的說明 此欄位不再參考標準。
Remediation.Recommendation.Text	「如需如何修正此問題的指示，請參閱 AWS Security Hub CSPM PCI DSS 文件。」	「如需如何修正此問題的指示，請參閱 AWS Security Hub CSPM 控制文件。」 此欄位不再參考標準。
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation 此欄位不再參考標準。

合併控制調查結果 – ASFF 變更

如果您啟用合併控制調查結果，則 ASFF 中控制調查結果的欄位和值可能會受到下列變更的影響。這些變更是合併控制項檢視功能所引進的變更之外的變更。如果您的工作流程不依賴這些 ASFF 欄位的值，則不需要採取任何動作。如果您有依賴這些欄位特定值的工作流程，請更新您的工作流程以使用目前的值。

Tip

如果您使用 [v2 AWS .0.0 上的自動化安全回應](#) 解決方案，請注意它支援合併的控制問題清單。這表示如果您啟用合併控制問題清單，您可以維護目前的工作流程。

ASFF 欄位	啟用合併控制問題清單之前的範例值	啟用合併控制調查結果後的範例值，以及變更的說明
GeneratorId	aws-foundational-security-best-practices/v/1.0.0/Config.1	security-control/Config.1 此欄位不再參考標準。
Title	AWS Config 應啟用 PCI.Config.1	AWS Config 應啟用

ASFF 欄位	啟用合併控制問題清單之前的範例值	啟用合併控制調查結果後的範例值，以及變更的說明
		此欄位不再參考標準特定資訊。
Id	arn : aws : securityhub : eu-central-1 : 123456789012 : subscription/pci-dss/v/3.2.1/PCI.IAM.5/finding/ab6d6a26-a156-48f0-9403-115983e5a956	arn : aws : securityhub : eu-central-1 : 123456789012 : security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956 此欄位不再參考標準。
ProductFields.ControlId	PCI.EC2.2	已移除。請Compliance.SecurityControlId 改為參閱。 此欄位會移除，以便使用單一、標準無關的控制 ID。
ProductFields.RuleId	1.3	已移除。請Compliance.SecurityControlId 改為參閱。 此欄位會移除，以便使用單一、標準無關的控制 ID。
說明	此 PCI DSS 控制項會檢查目前帳戶和區域中是否 AWS Config 已啟用。	此 AWS 控制項會檢查目前帳戶和區域中 AWS Config 是否已啟用。 此欄位不再參考標準。

ASFF 欄位	啟用合併控制問題清單之前的範例值	啟用合併控制調查結果後的範例值，以及變更的說明
嚴重性	<pre>{ "嚴重性" : { "產品" : 90, "標籤" : "CRITICAL", "標準化" : 90, "Original" : "CRITICAL" } }</pre>	<pre>{ "嚴重性" : { "標籤" : "CRITICAL", "標準化" : 90, "Original" : "CRITICAL" } }</pre> Security Hub CSPM 不再使用產品欄位來描述調查結果的嚴重性。
類型	【「軟體和組態檢查/產業和法規標準/PCI-DSS」】	【「軟體和組態檢查/產業和法規標準」】 此欄位不再參考標準。
Compliance.Related Requirements	【「PCI DSS 10.5.2」， 「PCI DSS 11.5」， 「CIS AWS Foundations 2.5」】	【「PCI DSS v3.2.1/10.5.2」， 「PCI DSS v3.2.1/11.5」， 「CIS AWS Foundations Benchmark v1.2.0/2.5」】 此欄位顯示所有啟用標準中的相關需求。
CreatedAt	2022-05-05T08 : 18 : 13.138Z	2022-09-25T08 : 18 : 13.138Z 格式保持不變，但值會在您啟用合併控制調查結果時重設。
FirstObservedAt	2022-05-07T08 : 18 : 13.138Z	2022-09-28T08 : 18 : 13.138Z 格式保持不變，但值會在您啟用合併控制調查結果時重設。

ASFF 欄位	啟用合併控制問題清單之前的範例值	啟用合併控制調查結果後的範例值，以及變更的說明
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	已移除。請Remediation.Recommendation.Url 改為參閱。
ProductFields.StandardsArn	arn : aws : securityhub : : standards/aws-foundational-security-best-practices/v/1.0.0	已移除。請Compliance.AssociatedStandards 改為參閱。
ProductFields.StandardsControlArn	arn : aws : securityhub : us-east-1 : 123456789012 : control/aws-foundational-security-best-practices/v/1.0.0/Config.1	已移除。Security Hub CSPM 會針對跨標準的安全性檢查產生一個問題清單。
ProductFields.StandardsGuideArn	arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0	已移除。請Compliance.AssociatedStandards 改為參閱。
ProductFields.StandardsGuideSubscriptionArn	arn : aws : securityhub : us-east-2 : 123456789012 : subscription/cis-aws-foundations-benchmark/v/1.2.0	已移除。Security Hub CSPM 會針對跨標準的安全性檢查產生一個問題清單。
ProductFields.StandardsSubscriptionArn	arn : aws : securityhub : us-east-1 : 123456789012 : subscription/aws-foundational-security-best-practices/v/1.0.0	已移除。Security Hub CSPM 會針對跨標準的安全性檢查產生一個問題清單。

ASFF 欄位	啟用合併控制問題清單之前的範例值	啟用合併控制調查結果後的範例值，以及變更的說明
ProductFields.aws/securityhub/FindingId	arn : aws : securityhub : us-east-1 : : product/aws/securityhub/arn : aws : securityhub : us-east-1 : 123456789012 : subscription/aws-foundational-security-best-practices/v/1.0.0/Config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67	arn : aws : securityhub : us-east-1 : : product/aws/securityhub/arn : aws : securityhub : us-east-1 : 123456789012 : security-control/Config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 此欄位不再參考標準。

開啟合併控制調查結果後，客戶提供 ASFF 欄位的值

如果您啟用合併控制問題清單，Security Hub CSPM 會跨標準產生一個問題清單，並封存原始問題清單（每個標準都有不同的問題清單）。

您使用 Security Hub CSPM 主控台或 [BatchUpdateFindings](#) 操作對原始調查結果所做的更新，將不會保留在新的調查結果中。如有必要，您可以參考封存的問題清單來復原此資料。若要檢閱封存的問題清單，您可以使用 Security Hub CSPM 主控台上的問題清單頁面，並將記錄狀態篩選條件設定為封存。或者，您可以使用 Security Hub CSPM API [GetFindings](#) 的操作。

客戶提供的 ASFF 欄位	啟用合併控制問題清單之後的變更描述
可信度	重設為空白狀態。
重要性	重設為空白狀態。
注意	重設為空白狀態。
RelatedFindings	重設為空白狀態。
嚴重性	問題清單的預設嚴重性（符合控制項的嚴重性）。
類型	重設為標準無關值。
UserDefinedFields	重設為空白狀態。

客戶提供的 ASFF 欄位	啟用合併控制問題清單之後的變更描述
VerificationState	重設為空白狀態。
工作流程	新的失敗問題清單預設值為 NEW。新傳遞的問題清單的預設值為 RESOLVED。

啟用合併控制調查結果前後IDs

當您啟用合併控制調查結果時，下表列出控制項的產生器 ID 值變更。這些變更適用於自 2023 年 2 月 15 日起 Security Hub CSPM 支援的控制項。

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.1	security-control/CloudWatch.1
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.10	security-control/IAM.16
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.11	security-control/IAM.17
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.12	security-control/IAM.4
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.13	security-control/IAM.9
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.14	security-control/IAM.6
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.16	security-control/IAM.2
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.2	security-control/IAM.5

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.20	security-control/IAM.18
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.22	security-control/IAM.1
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.3	security-control/IAM.8
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.4	security-control/IAM.3
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.5	security-control/IAM.11
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.6	security-control/IAM.12
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.7	security-control/IAM.13
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.8	security-control/IAM.14
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.9	security-control/IAM.15
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.1	security-control/CloudTrail.1
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.2	security-control/CloudTrail.4
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.3	security-control/CloudTrail.6
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.4	security-control/CloudTrail.5

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.5	security-control/Config.1
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.6	security-control/CloudTrail.7
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.7	security-control/CloudTrail.2
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.8	security-control/KMS.4
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.9	security-control/EC2.6
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.1	security-control/CloudWatch.2
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.2	security-control/CloudWatch.3
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.3	security-control/CloudWatch.1
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.4	security-control/CloudWatch.4
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.5	security-control/CloudWatch.5
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.6	security-control/CloudWatch.6
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.7	security-control/CloudWatch.7
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.8	security-control/CloudWatch.8

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.9	security-control/CloudWatch.9
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.10	security-control/CloudWatch.10
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.11	security-control/CloudWatch.11
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.12	security-control/CloudWatch.12
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.13	security-control/CloudWatch.13
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.14	security-control/CloudWatch.14
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.1	security-control/EC2.13
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.2	security-control/EC2.14
arn : aws : securityhub : : ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.3	security-control/EC2.2
cis-aws-foundations-benchmark/v/1.4.0/1.10	security-control/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1.14	security-control/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1.16	security-control/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1.17	security-control/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	security-control/IAM.4
cis-aws-foundations-benchmark/v/1.4.0/1.5	security-control/IAM.9

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
cis-aws-foundations-benchmark/v/1.4.0/1.6	security-control/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1.7	security-control/CloudWatch.1
cis-aws-foundations-benchmark/v/1.4.0/1.8	security-control/IAM.15
cis-aws-foundations-benchmark/v/1.4.0/1.9	security-control/IAM.16
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	security-control/S3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	security-control/S3.1
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	security-control/S3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	security-control/EC2.7
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	security-control/RDS.3
cis-aws-foundations-benchmark/v/1.4.0/3.1	security-control/CloudTrail.1
cis-aws-foundations-benchmark/v/1.4.0/3.2	security-control/CloudTrail.4
cis-aws-foundations-benchmark/v/1.4.0/3.4	security-control/CloudTrail.5
cis-aws-foundations-benchmark/v/1.4.0/3.5	security-control/Config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	security-control/S3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	security-control/CloudTrail.2
cis-aws-foundations-benchmark/v/1.4.0/3.8	security-control/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	security-control/EC2.6
cis-aws-foundations-benchmark/v/1.4.0/4.3	security-control/CloudWatch.1
cis-aws-foundations-benchmark/v/1.4.0/4.4	security-control/CloudWatch.4
cis-aws-foundations-benchmark/v/1.4.0/4.5	security-control/CloudWatch.5

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
cis-aws-foundations-benchmark/v/1.4.0/4.6	security-control/CloudWatch.6
cis-aws-foundations-benchmark/v/1.4.0/4.7	security-control/CloudWatch.7
cis-aws-foundations-benchmark/v/1.4.0/4.8	security-control/CloudWatch.8
cis-aws-foundations-benchmark/v/1.4.0/4.9	security-control/CloudWatch.9
cis-aws-foundations-benchmark/v/1.4.0/4.10	security-control/CloudWatch.10
cis-aws-foundations-benchmark/v/1.4.0/4.11	security-control/CloudWatch.11
cis-aws-foundations-benchmark/v/1.4.0/4.12	security-control/CloudWatch.12
cis-aws-foundations-benchmark/v/1.4.0/4.13	security-control/CloudWatch.13
cis-aws-foundations-benchmark/v/1.4.0/4.14	security-control/CloudWatch.14
cis-aws-foundations-benchmark/v/1.4.0/5.1	security-control/EC2.21
cis-aws-foundations-benchmark/v/1.4.0/5.3	security-control/EC2.2
aws-foundational-security-best-practices/v/1.0.0/Account.1	security-control/Account.1
aws-foundational-security-best-practices/v/1.0.0/ACM.1	security-control/ACM.1
aws-foundational-security-best-practices/v/1.0.0/APIGateway.1	security-control/APIGateway.1
aws-foundational-security-best-practices/v/1.0.0/APIGateway.2	security-control/APIGateway.2
aws-foundational-security-best-practices/v/1.0.0/APIGateway.3	security-control/APIGateway.3
aws-foundational-security-best-practices/v/1.0.0/APIGateway.4	security-control/APIGateway.4

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/APIGateway.5	security-control/APIGateway.5
aws-foundational-security-best-practices/v/1.0.0/APIGateway.8	security-control/APIGateway.8
aws-foundational-security-best-practices/v/1.0.0/APIGateway.9	security-control/APIGateway.9
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.1	security-control/AutoScaling.1
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.2	security-control/AutoScaling.2
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.3	security-control/AutoScaling.3
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.5	security-control/AutoScaling.5
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.6	security-control/AutoScaling.6
aws-foundational-security-best-practices/v/1.0.0/AutoScaling.9	security-control/AutoScaling.9
aws-foundational-security-best-practices/v/1.0.0/CloudFront.1	security-control/CloudFront.1
aws-foundational-security-best-practices/v/1.0.0/CloudFront.3	security-control/CloudFront.3
aws-foundational-security-best-practices/v/1.0.0/CloudFront.4	security-control/CloudFront.4
aws-foundational-security-best-practices/v/1.0.0/CloudFront.5	security-control/CloudFront.5

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/CloudFront.6	security-control/CloudFront.6
aws-foundational-security-best-practices/v/1.0.0/CloudFront.7	security-control/CloudFront.7
aws-foundational-security-best-practices/v/1.0.0/CloudFront.8	security-control/CloudFront.8
aws-foundational-security-best-practices/v/1.0.0/CloudFront.9	security-control/CloudFront.9
aws-foundational-security-best-practices/v/1.0.0/CloudFront.10	security-control/CloudFront.10
aws-foundational-security-best-practices/v/1.0.0/CloudFront.12	security-control/CloudFront.12
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.1	security-control/CloudTrail.1
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2	security-control/CloudTrail.2
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.4	security-control/CloudTrail.4
aws-foundational-security-best-practices/v/1.0.0/CloudTrail.5	security-control/CloudTrail.5
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.1	security-control/CodeBuild.1
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.2	security-control/CodeBuild.2
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.3	security-control/CodeBuild.3

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/CodeBuild.4	security-control/CodeBuild.4
aws-foundational-security-best-practices/v/1.0.0/Config.1	security-control/Config.1
aws-foundational-security-best-practices/v/1.0.0/DMS.1	security-control/DMS.1
aws-foundational-security-best-practices/v/1.0.0/DynamoDB.1	security-control/DynamoDB.1
aws-foundational-security-best-practices/v/1.0.0/DynamoDB.2	security-control/DynamoDB.2
aws-foundational-security-best-practices/v/1.0.0/DynamoDB.3	security-control/DynamoDB.3
aws-foundational-security-best-practices/v/1.0.0/EC2.1	security-control/EC2.1
aws-foundational-security-best-practices/v/1.0.0/EC2.3	security-control/EC2.3
aws-foundational-security-best-practices/v/1.0.0/EC2.4	security-control/EC2.4
aws-foundational-security-best-practices/v/1.0.0/EC2.6	security-control/EC2.6
aws-foundational-security-best-practices/v/1.0.0/EC2.7	security-control/EC2.7
aws-foundational-security-best-practices/v/1.0.0/EC2.8	security-control/EC2.8
aws-foundational-security-best-practices/v/1.0.0/EC2.9	security-control/EC2.9

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/EC2.10	security-control/EC2.10
aws-foundational-security-best-practices/v/1.0.0/EC2.15	security-control/EC2.15
aws-foundational-security-best-practices/v/1.0.0/EC2.16	security-control/EC2.16
aws-foundational-security-best-practices/v/1.0.0/EC2.17	security-control/EC2.17
aws-foundational-security-best-practices/v/1.0.0/EC2.18	security-control/EC2.18
aws-foundational-security-best-practices/v/1.0.0/EC2.19	security-control/EC2.19
aws-foundational-security-best-practices/v/1.0.0/EC2.2	security-control/EC2.2
aws-foundational-security-best-practices/v/1.0.0/EC2.20	security-control/EC2.20
aws-foundational-security-best-practices/v/1.0.0/EC2.21	security-control/EC2.21
aws-foundational-security-best-practices/v/1.0.0/EC2.23	security-control/EC2.23
aws-foundational-security-best-practices/v/1.0.0/EC2.24	security-control/EC2.24
aws-foundational-security-best-practices/v/1.0.0/EC2.25	security-control/EC2.25
aws-foundational-security-best-practices/v/1.0.0/ECR.1	security-control/ECR.1

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/ECR.2	security-control/ECR.2
aws-foundational-security-best-practices/v/1.0.0/ECR.3	security-control/ECR.3
aws-foundational-security-best-practices/v/1.0.0/ECS.1	security-control/ECS.1
aws-foundational-security-best-practices/v/1.0.0/ECS.10	security-control/ECS.10
aws-foundational-security-best-practices/v/1.0.0/ECS.12	security-control/ECS.12
aws-foundational-security-best-practices/v/1.0.0/ECS.2	security-control/ECS.2
aws-foundational-security-best-practices/v/1.0.0/ECS.3	security-control/ECS.3
aws-foundational-security-best-practices/v/1.0.0/ECS.4	security-control/ECS.4
aws-foundational-security-best-practices/v/1.0.0/ECS.5	security-control/ECS.5
aws-foundational-security-best-practices/v/1.0.0/ECS.8	security-control/ECS.8
aws-foundational-security-best-practices/v/1.0.0/EFS.1	security-control/EFS.1
aws-foundational-security-best-practices/v/1.0.0/EFS.2	security-control/EFS.2
aws-foundational-security-best-practices/v/1.0.0/EFS.3	security-control/EFS.3

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/EFS.4	security-control/EFS.4
aws-foundational-security-best-practices/v/1.0.0/EKS.2	security-control/EKS.2
aws-foundational-security-best-practices/v/1.0.0/ElasticBeanstalk.1	security-control/ElasticBeanstalk.1
aws-foundational-security-best-practices/v/1.0.0/ElasticBeanstalk.2	security-control/ElasticBeanstalk.2
aws-foundational-security-best-practices/v/1.0.0/ELBv2.1	security-control/ELB.1
aws-foundational-security-best-practices/v/1.0.0/ELB.2	security-control/ELB.2
aws-foundational-security-best-practices/v/1.0.0/ELB.3	security-control/ELB.3
aws-foundational-security-best-practices/v/1.0.0/ELB.4	security-control/ELB.4
aws-foundational-security-best-practices/v/1.0.0/ELB.5	security-control/ELB.5
aws-foundational-security-best-practices/v/1.0.0/ELB.6	security-control/ELB.6
aws-foundational-security-best-practices/v/1.0.0/ELB.7	security-control/ELB.7
aws-foundational-security-best-practices/v/1.0.0/ELB.8	security-control/ELB.8
aws-foundational-security-best-practices/v/1.0.0/ELB.9	security-control/ELB.9

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/ELB.10	security-control/ELB.10
aws-foundational-security-best-practices/v/1.0.0/ELB.11	security-control/ELB.11
aws-foundational-security-best-practices/v/1.0.0/ELB.12	security-control/ELB.12
aws-foundational-security-best-practices/v/1.0.0/ELB.13	security-control/ELB.13
aws-foundational-security-best-practices/v/1.0.0/ELB.14	security-control/ELB.14
aws-foundational-security-best-practices/v/1.0.0/EMR.1	security-control/EMR.1
aws-foundational-security-best-practices/v/1.0.0/ES.1	security-control/ES.1
aws-foundational-security-best-practices/v/1.0.0/ES.2	security-control/ES.2
aws-foundational-security-best-practices/v/1.0.0/ES.3	security-control/ES.3
aws-foundational-security-best-practices/v/1.0.0/ES.4	security-control/ES.4
aws-foundational-security-best-practices/v/1.0.0/ES.5	security-control/ES.5
aws-foundational-security-best-practices/v/1.0.0/ES.6	security-control/ES.6
aws-foundational-security-best-practices/v/1.0.0/ES.7	security-control/ES.7

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/ES.8	security-control/ES.8
aws-foundational-security-best-practices/v/1.0.0/GuardDuty.1	security-control/GuardDuty.1
aws-foundational-security-best-practices/v/1.0.0/IAM.1	security-control/IAM.1
aws-foundational-security-best-practices/v/1.0.0/IAM.2	security-control/IAM.2
aws-foundational-security-best-practices/v/1.0.0/IAM.21	security-control/IAM.21
aws-foundational-security-best-practices/v/1.0.0/IAM.3	security-control/IAM.3
aws-foundational-security-best-practices/v/1.0.0/IAM.4	security-control/IAM.4
aws-foundational-security-best-practices/v/1.0.0/IAM.5	security-control/IAM.5
aws-foundational-security-best-practices/v/1.0.0/IAM.6	security-control/IAM.6
aws-foundational-security-best-practices/v/1.0.0/IAM.7	security-control/IAM.7
aws-foundational-security-best-practices/v/1.0.0/IAM.8	security-control/IAM.8
aws-foundational-security-best-practices/v/1.0.0/Kinesis.1	security-control/Kinesis.1
aws-foundational-security-best-practices/v/1.0.0/KMS.1	security-control/KMS.1

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/KMS.2	security-control/KMS.2
aws-foundational-security-best-practices/v/1.0.0/KMS.3	security-control/KMS.3
aws-foundational-security-best-practices/v/1.0.0/Lambda.1	security-control/Lambda.1
aws-foundational-security-best-practices/v/1.0.0/Lambda.2	security-control/Lambda.2
aws-foundational-security-best-practices/v/1.0.0/Lambda.5	security-control/Lambda.5
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.3	security-control/NetworkFirewall.3
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.4	security-control/NetworkFirewall.4
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.5	security-control/NetworkFirewall.5
aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.6	security-control/NetworkFirewall.6
aws-foundational-security-best-practices/v/1.0.0/Opensearch.1	security-control/Opensearch.1
aws-foundational-security-best-practices/v/1.0.0/Opensearch.2	security-control/Opensearch.2
aws-foundational-security-best-practices/v/1.0.0/Opensearch.3	security-control/Opensearch.3
aws-foundational-security-best-practices/v/1.0.0/Opensearch.4	security-control/Opensearch.4

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/Opensearch.5	security-control/Opensearch.5
aws-foundational-security-best-practices/v/1.0.0/Opensearch.6	security-control/Opensearch.6
aws-foundational-security-best-practices/v/1.0.0/Opensearch.7	security-control/Opensearch.7
aws-foundational-security-best-practices/v/1.0.0/Opensearch.8	security-control/Opensearch.8
aws-foundational-security-best-practices/v/1.0.0/RDS.1	security-control/RDS.1
aws-foundational-security-best-practices/v/1.0.0/RDS.10	security-control/RDS.10
aws-foundational-security-best-practices/v/1.0.0/RDS.11	security-control/RDS.11
aws-foundational-security-best-practices/v/1.0.0/RDS.12	security-control/RDS.12
aws-foundational-security-best-practices/v/1.0.0/RDS.13	security-control/RDS.13
aws-foundational-security-best-practices/v/1.0.0/RDS.14	security-control/RDS.14
aws-foundational-security-best-practices/v/1.0.0/RDS.15	security-control/RDS.15
aws-foundational-security-best-practices/v/1.0.0/RDS.16	security-control/RDS.16
aws-foundational-security-best-practices/v/1.0.0/RDS.17	security-control/RDS.17

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/RDS.19	security-control/RDS.19
aws-foundational-security-best-practices/v/1.0.0/RDS.2	security-control/RDS.2
aws-foundational-security-best-practices/v/1.0.0/RDS.20	security-control/RDS.20
aws-foundational-security-best-practices/v/1.0.0/RDS.21	security-control/RDS.21
aws-foundational-security-best-practices/v/1.0.0/RDS.22	security-control/RDS.22
aws-foundational-security-best-practices/v/1.0.0/RDS.23	security-control/RDS.23
aws-foundational-security-best-practices/v/1.0.0/RDS.24	security-control/RDS.24
aws-foundational-security-best-practices/v/1.0.0/RDS.25	security-control/RDS.25
aws-foundational-security-best-practices/v/1.0.0/RDS.3	security-control/RDS.3
aws-foundational-security-best-practices/v/1.0.0/RDS.4	security-control/RDS.4
aws-foundational-security-best-practices/v/1.0.0/RDS.5	security-control/RDS.5
aws-foundational-security-best-practices/v/1.0.0/RDS.6	security-control/RDS.6
aws-foundational-security-best-practices/v/1.0.0/RDS.7	security-control/RDS.7

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/RDS.8	security-control/RDS.8
aws-foundational-security-best-practices/v/1.0.0/RDS.9	security-control/RDS.9
aws-foundational-security-best-practices/v/1.0.0/Redshift.1	security-control/Redshift.1
aws-foundational-security-best-practices/v/1.0.0/Redshift.2	security-control/Redshift.2
aws-foundational-security-best-practices/v/1.0.0/Redshift.3	security-control/Redshift.3
aws-foundational-security-best-practices/v/1.0.0/Redshift.4	security-control/Redshift.4
aws-foundational-security-best-practices/v/1.0.0/Redshift.6	security-control/Redshift. 6
aws-foundational-security-best-practices/v/1.0.0/Redshift.7	security-control/Redshift. 7
aws-foundational-security-best-practices/v/1.0.0/Redshift.8	security-control/Redshift. 8
aws-foundational-security-best-practices/v/1.0.0/Redshift.9	security-control/Redshift.9
aws-foundational-security-best-practices/v/1.0.0/S3.1	security-control/S3.1
aws-foundational-security-best-practices/v/1.0.0/S3.12	security-control/S3.12
aws-foundational-security-best-practices/v/1.0.0/S3.13	security-control/S3.13

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/S3.2	security-control/S3.2
aws-foundational-security-best-practices/v/1.0.0/S3.3	security-control/S3.3
aws-foundational-security-best-practices/v/1.0.0/S3.5	security-control/S3.5
aws-foundational-security-best-practices/v/1.0.0/S3.6	security-control/S3.6
aws-foundational-security-best-practices/v/1.0.0/S3.8	security-control/S3.8
aws-foundational-security-best-practices/v/1.0.0/S3.9	security-control/S3.9
aws-foundational-security-best-practices/v/1.0.0/SageMaker.1	security-control/SageMaker.1
aws-foundational-security-best-practices/v/1.0.0/SageMaker.2	security-control/SageMaker.2
aws-foundational-security-best-practices/v/1.0.0/SageMaker.3	security-control/SageMaker.3
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.1	security-control/SecretsManager.1
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.2	security-control/SecretsManager.2
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.3	security-control/SecretsManager.3
aws-foundational-security-best-practices/v/1.0.0/SecretsManager.4	security-control/SecretsManager.4

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
aws-foundational-security-best-practices/v/1.0.0/SQS.1	security-control/SQS.1
aws-foundational-security-best-practices/v/1.0.0/SSM.1	security-control/SSM.1
aws-foundational-security-best-practices/v/1.0.0/SSM.2	security-control/SSM.2
aws-foundational-security-best-practices/v/1.0.0/SSM.3	security-control/SSM.3
aws-foundational-security-best-practices/v/1.0.0/SSM.4	security-control/SSM.4
aws-foundational-security-best-practices/v/1.0.0/WAF.1	security-control/WAF.1
aws-foundational-security-best-practices/v/1.0.0/WAF.2	security-control/WAF.2
aws-foundational-security-best-practices/v/1.0.0/WAF.3	security-control/WAF.3
aws-foundational-security-best-practices/v/1.0.0/WAF.4	security-control/WAF.4
aws-foundational-security-best-practices/v/1.0.0/WAF.6	security-control/WAF.6
aws-foundational-security-best-practices/v/1.0.0/WAF.7	security-control/WAF.7
aws-foundational-security-best-practices/v/1.0.0/WAF.8	security-control/WAF.8
aws-foundational-security-best-practices/v/1.0.0/WAF.10	security-control/WAF.10

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
pci-dss/v/3.2.1/PCI.AutoScaling.1	security-control/AutoScaling.1
pci-dss/v/3.2.1/PCI.CloudTrail.1	security-control/CloudTrail.2
pci-dss/v/3.2.1/PCI.CloudTrail.2	security-control/CloudTrail.3
pci-dss/v/3.2.1/PCI.CloudTrail.3	security-control/CloudTrail.4
pci-dss/v/3.2.1/PCI.CloudTrail.4	security-control/CloudTrail.5
pci-dss/v/3.2.1/PCI.CodeBuild.1	security-control/CodeBuild.1
pci-dss/v/3.2.1/PCI.CodeBuild.2	security-control/CodeBuild.2
pci-dss/v/3.2.1/PCI.Config.1	security-control/Config.1
pci-dss/v/3.2.1/PCI.CW.1	security-control/CloudWatch.1
pci-dss/v/3.2.1/PCI.DMS.1	security-control/DMS.1
pci-dss/v/3.2.1/PCI.EC2.1	security-control/EC2.1
pci-dss/v/3.2.1/PCI.EC2.2	security-control/EC2.2
pci-dss/v/3.2.1/PCI.EC2.4	security-control/EC2.12
pci-dss/v/3.2.1/PCI.EC2.5	security-control/EC2.13
pci-dss/v/3.2.1/PCI.EC2.6	security-control/EC2.6
pci-dss/v/3.2.1/PCI.ELBv2.1	security-control/ELB.1
pci-dss/v/3.2.1/PCI.ES.1	security-control/ES.2
pci-dss/v/3.2.1/PCI.ES.2	security-control/ES.1
pci-dss/v/3.2.1/PCI.GuardDuty.1	security-control/GuardDuty.1
pci-dss/v/3.2.1/PCI.IAM.1	security-control/IAM.4

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
pci-dss/v/3.2.1/PCI.IAM.2	security-control/IAM.2
pci-dss/v/3.2.1/PCI.IAM.3	security-control/IAM.1
pci-dss/v/3.2.1/PCI.IAM.4	security-control/IAM.6
pci-dss/v/3.2.1/PCI.IAM.5	security-control/IAM.9
pci-dss/v/3.2.1/PCI.IAM.6	security-control/IAM.19
pci-dss/v/3.2.1/PCI.IAM.7	security-control/IAM.8
pci-dss/v/3.2.1/PCI.IAM.8	security-control/IAM.10
pci-dss/v/3.2.1/PCI.KMS.1	security-control/KMS.4
pci-dss/v/3.2.1/PCI.Lambda.1	security-control/Lambda.1
pci-dss/v/3.2.1/PCI.Lambda.2	security-control/Lambda.3
pci-dss/v/3.2.1/PCI.Opensearch.1	security-control/Opensearch.2
pci-dss/v/3.2.1/PCI.Opensearch.2	security-control/Opensearch.1
pci-dss/v/3.2.1/PCI.RDS.1	security-control/RDS.1
pci-dss/v/3.2.1/PCI.RDS.2	security-control/RDS.2
pci-dss/v/3.2.1/PCI.Redshift.1	security-control/Redshift.1
pci-dss/v/3.2.1/PCI.S3.1	security-control/S3.3
pci-dss/v/3.2.1/PCI.S3.2	security-control/S3.2
pci-dss/v/3.2.1/PCI.S3.3	security-control/S3.7
pci-dss/v/3.2.1/PCI.S3.5	security-control/S3.5
pci-dss/v/3.2.1/PCI.S3.6	security-control/S3.1

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
pci-dss/v/3.2.1/PCI.SageMaker.1	security-control/SageMaker.1
pci-dss/v/3.2.1/PCI.SSM.1	security-control/SSM.2
pci-dss/v/3.2.1/PCI.SSM.2	security-control/SSM.3
pci-dss/v/3.2.1/PCI.SSM.3	security-control/SSM.1
service-managed-aws-control-tower/v/1.0.0/ACM.1	security-control/ACM.1
service-managed-aws-control-tower/v/1.0.0/API Gateway.1	security-control/APIGateway.1
service-managed-aws-control-tower/v/1.0.0/API Gateway.2	security-control/APIGateway.2
service-managed-aws-control-tower/v/1.0.0/API Gateway.3	security-control/APIGateway.3
service-managed-aws-control-tower/v/1.0.0/API Gateway.4	security-control/APIGateway.4
service-managed-aws-control-tower/v/1.0.0/API Gateway.5	security-control/APIGateway.5
service-managed-aws-control-tower/v/1.0.0/AutoScaling.1	security-control/AutoScaling.1
service-managed-aws-control-tower/v/1.0.0/AutoScaling.2	security-control/AutoScaling.2
service-managed-aws-control-tower/v/1.0.0/AutoScaling.3	security-control/AutoScaling.3
service-managed-aws-control-tower/v/1.0.0/AutoScaling.4	security-control/AutoScaling.4

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/AutoScaling.5	security-control/AutoScaling.5
service-managed-aws-control-tower/v/1.0.0/AutoScaling.6	security-control/AutoScaling.6
service-managed-aws-control-tower/v/1.0.0/AutoScaling.9	security-control/AutoScaling.9
service-managed-aws-control-tower/v/1.0.0/CloudTrail.1	security-control/CloudTrail.1
service-managed-aws-control-tower/v/1.0.0/CloudTrail.2	security-control/CloudTrail.2
service-managed-aws-control-tower/v/1.0.0/CloudTrail.4	security-control/CloudTrail.4
service-managed-aws-control-tower/v/1.0.0/CloudTrail.5	security-control/CloudTrail.5
service-managed-aws-control-tower/v/1.0.0/CodeBuild.1	security-control/CodeBuild.1
service-managed-aws-control-tower/v/1.0.0/CodeBuild.2	security-control/CodeBuild.2
service-managed-aws-control-tower/v/1.0.0/CodeBuild.4	security-control/CodeBuild.4
service-managed-aws-control-tower/v/1.0.0/CodeBuild.5	security-control/CodeBuild.5
service-managed-aws-control-tower/v/1.0.0/DMS.1	security-control/DMS.1
service-managed-aws-control-tower/v/1.0.0/DynamoDB.1	security-control/DynamoDB.1

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/ DynamoDB.2	security-control/DynamoDB.2
service-managed-aws-control-tower/v/1.0.0/ EC2.1	security-control/EC2.1
service-managed-aws-control-tower/v/1.0.0/ EC2.2	security-control/EC2.2
service-managed-aws-control-tower/v/1.0.0/ EC2.3	security-control/EC2.3
service-managed-aws-control-tower/v/1.0.0/ EC2.4	security-control/EC2.4
service-managed-aws-control-tower/v/1.0.0/ EC2.6	security-control/EC2.6
service-managed-aws-control-tower/v/1.0.0/ EC2.7	security-control/EC2.7
service-managed-aws-control-tower/v/1.0.0/ EC2.8	security-control/EC2.8
service-managed-aws-control-tower/v/1.0.0/ EC2.9	security-control/EC2.9
service-managed-aws-control-tower/v/1.0.0/ EC2.10	security-control/EC2.10
service-managed-aws-control-tower/v/1.0.0/ EC2.15	security-control/EC2.15
service-managed-aws-control-tower/v/1.0.0/ EC2.16	security-control/EC2.16
service-managed-aws-control-tower/v/1.0.0/ EC2.17	security-control/EC2.17

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/EC2.18	security-control/EC2.18
service-managed-aws-control-tower/v/1.0.0/EC2.19	security-control/EC2.19
service-managed-aws-control-tower/v/1.0.0/EC2.20	security-control/EC2.20
service-managed-aws-control-tower/v/1.0.0/EC2.21	security-control/EC2.21
service-managed-aws-control-tower/v/1.0.0/EC2.22	security-control/EC2.22
service-managed-aws-control-tower/v/1.0.0/ECR.1	security-control/ECR.1
service-managed-aws-control-tower/v/1.0.0/ECR.2	security-control/ECR.2
service-managed-aws-control-tower/v/1.0.0/ECR.3	security-control/ECR.3
service-managed-aws-control-tower/v/1.0.0/ECS.1	security-control/ECS.1
service-managed-aws-control-tower/v/1.0.0/ECS.2	security-control/ECS.2
service-managed-aws-control-tower/v/1.0.0/ECS.3	security-control/ECS.3
service-managed-aws-control-tower/v/1.0.0/ECS.4	security-control/ECS.4
service-managed-aws-control-tower/v/1.0.0/ECS.5	security-control/ECS.5

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/ECS.8	security-control/ECS.8
service-managed-aws-control-tower/v/1.0.0/ECS.10	security-control/ECS.10
service-managed-aws-control-tower/v/1.0.0/ECS.12	security-control/ECS.12
service-managed-aws-control-tower/v/1.0.0/EFS.1	security-control/EFS.1
service-managed-aws-control-tower/v/1.0.0/EFS.2	security-control/EFS.2
service-managed-aws-control-tower/v/1.0.0/EFS.3	security-control/EFS.3
service-managed-aws-control-tower/v/1.0.0/EFS.4	security-control/EFS.4
service-managed-aws-control-tower/v/1.0.0/EKS.2	security-control/EKS.2
service-managed-aws-control-tower/v/1.0.0/ELB.2	security-control/ELB.2
service-managed-aws-control-tower/v/1.0.0/ELB.3	security-control/ELB.3
service-managed-aws-control-tower/v/1.0.0/ELB.4	security-control/ELB.4
service-managed-aws-control-tower/v/1.0.0/ELB.5	security-control/ELB.5
service-managed-aws-control-tower/v/1.0.0/ELB.6	security-control/ELB.6

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/ELB.7	security-control/ELB.7
service-managed-aws-control-tower/v/1.0.0/ELB.8	security-control/ELB.8
service-managed-aws-control-tower/v/1.0.0/ELB.9	security-control/ELB.9
service-managed-aws-control-tower/v/1.0.0/ELB.10	security-control/ELB.10
service-managed-aws-control-tower/v/1.0.0/ELB.12	security-control/ELB.12
service-managed-aws-control-tower/v/1.0.0/ELB.13	security-control/ELB.13
service-managed-aws-control-tower/v/1.0.0/ELB.14	security-control/ELB.14
service-managed-aws-control-tower/v/1.0.0/ELBv2.1	security-control/ELBv2.1
service-managed-aws-control-tower/v/1.0.0/EMR.1	security-control/EMR.1
service-managed-aws-control-tower/v/1.0.0/ES.1	security-control/ES.1
service-managed-aws-control-tower/v/1.0.0/ES.2	security-control/ES.2
service-managed-aws-control-tower/v/1.0.0/ES.3	security-control/ES.3
service-managed-aws-control-tower/v/1.0.0/ES.4	security-control/ES.4

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/ES.5	security-control/ES.5
service-managed-aws-control-tower/v/1.0.0/ES.6	security-control/ES.6
service-managed-aws-control-tower/v/1.0.0/ES.7	security-control/ES.7
service-managed-aws-control-tower/v/1.0.0/ES.8	security-control/ES.8
service-managed-aws-control-tower/v/1.0.0/ElasticBeanstalk.1	security-control/ElasticBeanstalk.1
service-managed-aws-control-tower/v/1.0.0/ElasticBeanstalk.2	security-control/ElasticBeanstalk.2
service-managed-aws-control-tower/v/1.0.0/GuardDuty.1	security-control/GuardDuty.1
service-managed-aws-control-tower/v/1.0.0/IAM.1	security-control/IAM.1
service-managed-aws-control-tower/v/1.0.0/IAM.2	security-control/IAM.2
service-managed-aws-control-tower/v/1.0.0/IAM.3	security-control/IAM.3
service-managed-aws-control-tower/v/1.0.0/IAM.4	security-control/IAM.4
service-managed-aws-control-tower/v/1.0.0/IAM.5	security-control/IAM.5
service-managed-aws-control-tower/v/1.0.0/IAM.6	security-control/IAM.6

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/IAM.7	security-control/IAM.7
service-managed-aws-control-tower/v/1.0.0/IAM.8	security-control/IAM.8
service-managed-aws-control-tower/v/1.0.0/IAM.21	security-control/IAM.21
service-managed-aws-control-tower/v/1.0.0/Kinesis.1	security-control/Kinesis.1
service-managed-aws-control-tower/v/1.0.0/KMS.1	security-control/KMS.1
service-managed-aws-control-tower/v/1.0.0/KMS.2	security-control/KMS.2
service-managed-aws-control-tower/v/1.0.0/KMS.3	security-control/KMS.3
service-managed-aws-control-tower/v/1.0.0/Lambda.1	security-control/Lambda.1
service-managed-aws-control-tower/v/1.0.0/Lambda.2	security-control/Lambda.2
service-managed-aws-control-tower/v/1.0.0/Lambda.5	security-control/Lambda.5
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.3	security-control/NetworkFirewall.3
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.4	security-control/NetworkFirewall.4
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.5	security-control/NetworkFirewall.5

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.6	security-control/NetworkFirewall.6
service-managed-aws-control-tower/v/1.0.0/Opensearch.1	security-control/Opensearch.1
service-managed-aws-control-tower/v/1.0.0/Opensearch.2	security-control/Opensearch.2
service-managed-aws-control-tower/v/1.0.0/Opensearch.3	security-control/Opensearch.3
service-managed-aws-control-tower/v/1.0.0/Opensearch.4	security-control/Opensearch.4
service-managed-aws-control-tower/v/1.0.0/Opensearch.5	security-control/Opensearch.5
service-managed-aws-control-tower/v/1.0.0/Opensearch.6	security-control/Opensearch.6
service-managed-aws-control-tower/v/1.0.0/Opensearch.7	security-control/Opensearch.7
service-managed-aws-control-tower/v/1.0.0/Opensearch.8	security-control/Opensearch.8
service-managed-aws-control-tower/v/1.0.0/RDS.1	security-control/RDS.1
service-managed-aws-control-tower/v/1.0.0/RDS.2	security-control/RDS.2
service-managed-aws-control-tower/v/1.0.0/RDS.3	security-control/RDS.3
service-managed-aws-control-tower/v/1.0.0/RDS.4	security-control/RDS.4

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/RDS.5	security-control/RDS.5
service-managed-aws-control-tower/v/1.0.0/RDS.6	security-control/RDS.6
service-managed-aws-control-tower/v/1.0.0/RDS.8	security-control/RDS.8
service-managed-aws-control-tower/v/1.0.0/RDS.9	security-control/RDS.9
service-managed-aws-control-tower/v/1.0.0/RDS.10	security-control/RDS.10
service-managed-aws-control-tower/v/1.0.0/RDS.11	security-control/RDS.11
service-managed-aws-control-tower/v/1.0.0/RDS.13	security-control/RDS.13
service-managed-aws-control-tower/v/1.0.0/RDS.17	security-control/RDS.17
service-managed-aws-control-tower/v/1.0.0/RDS.18	security-control/RDS.18
service-managed-aws-control-tower/v/1.0.0/RDS.19	security-control/RDS.19
service-managed-aws-control-tower/v/1.0.0/RDS.20	security-control/RDS.20
service-managed-aws-control-tower/v/1.0.0/RDS.21	security-control/RDS.21
service-managed-aws-control-tower/v/1.0.0/RDS.22	security-control/RDS.22

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/RDS.23	security-control/RDS.23
service-managed-aws-control-tower/v/1.0.0/RDS.25	security-control/RDS.25
service-managed-aws-control-tower/v/1.0.0/Redshift.1	security-control/Redshift.1
service-managed-aws-control-tower/v/1.0.0/Redshift.2	security-control/Redshift.2
service-managed-aws-control-tower/v/1.0.0/Redshift.4	security-control/Redshift.4
service-managed-aws-control-tower/v/1.0.0/Redshift.6	security-control/Redshift. 6
service-managed-aws-control-tower/v/1.0.0/Redshift.7	security-control/Redshift. 7
service-managed-aws-control-tower/v/1.0.0/Redshift.8	security-control/Redshift. 8
service-managed-aws-control-tower/v/1.0.0/Redshift.9	security-control/Redshift.9
service-managed-aws-control-tower/v/1.0.0/S3.1	security-control/S3.1
service-managed-aws-control-tower/v/1.0.0/S3.2	security-control/S3.2
service-managed-aws-control-tower/v/1.0.0/S3.3	security-control/S3.3
service-managed-aws-control-tower/v/1.0.0/S3.5	security-control/S3.5

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/S3.6	security-control/S3.6
service-managed-aws-control-tower/v/1.0.0/S3.8	security-control/S3.8
service-managed-aws-control-tower/v/1.0.0/S3.9	security-control/S3.9
service-managed-aws-control-tower/v/1.0.0/S3.12	security-control/S3.12
service-managed-aws-control-tower/v/1.0.0/S3.13	security-control/S3.13
service-managed-aws-control-tower/v/1.0.0/SageMaker.1	security-control/SageMaker.1
service-managed-aws-control-tower/v/1.0.0/SecretsManager.1	security-control/SecretsManager.1
service-managed-aws-control-tower/v/1.0.0/SecretsManager.2	security-control/SecretsManager.2
service-managed-aws-control-tower/v/1.0.0/SecretsManager.3	security-control/SecretsManager.3
service-managed-aws-control-tower/v/1.0.0/SecretsManager.4	security-control/SecretsManager.4
service-managed-aws-control-tower/v/1.0.0/SQS.1	security-control/SQS.1
service-managed-aws-control-tower/v/1.0.0/SSM.1	security-control/SSM.1
service-managed-aws-control-tower/v/1.0.0/SSM.2	security-control/SSM.2

啟用合併控制問題清單之前的 GeneratorID	啟用合併控制問題清單後的 GeneratorID
service-managed-aws-control-tower/v/1.0.0/SSM.3	security-control/SSM.3
service-managed-aws-control-tower/v/1.0.0/SSM.4	security-control/SSM.4
service-managed-aws-control-tower/v/1.0.0/WAF.2	security-control/WAF.2
service-managed-aws-control-tower/v/1.0.0/WAF.3	security-control/WAF.3
service-managed-aws-control-tower/v/1.0.0/WAF.4	security-control/WAF.4

合併如何影響控制 IDs和標題

合併控制項檢視和合併的控制項調查結果會將控制 IDs和標題跨標準標準化。安全控制 ID 和安全控制標題一詞是指這些標準無關的值。

Security Hub CSPM 主控台會顯示標準無關的安全控制 IDs和安全控制標題，無論您的帳戶是否啟用或停用合併控制調查結果。不過，如果您的帳戶停用合併控制調查結果，Security Hub CSPM 調查結果會包含 PCI DSS 和 CIS v1.2.0 的標準特定控制標題。此外，Security Hub CSPM 調查結果包含標準特定的控制 ID 和安全控制 ID。如需整合如何影響控制問題清單的範例，請參閱 [控制問題清單的範例](#)。

對於屬於[AWS Control Tower 服務受管標準](#)的控制項，啟用合併控制項問題清單時，CT. 會從問題清單中的控制項 ID 和標題中移除字首。

若要在 Security Hub CSPM 中停用安全控制，您必須停用對應至安全控制的所有標準控制。下表顯示安全控制 IDs和標題與標準特定控制 IDs和標題的映射。屬於 AWS 基礎安全最佳實務 (FSBP) 標準的控制項 IDs 和標題已經是標準無關的。如需符合網際網路安全中心 (CIS) v3.0.0 要求的控制項映射，請參閱 [將控制項映射至每個版本中的 CIS 需求](#)。若要在此資料表上執行您自己的指令碼，您可以將[其下載為 .csv 檔案](#)。

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS v1.2.0	1.1 避免使用根使用者	【CloudWatch.1】應該存在日誌指標篩選條件和警示以使用「根」使用者
CIS v1.2.0	1.10 確保 IAM 密碼政策防止密碼重複使用	【IAM.16】 確保 IAM 密碼政策防止密碼重複使用
CIS v1.2.0	1.11 確保 IAM 密碼政策在 90 天內過期密碼	【IAM.17】 確保 IAM 密碼政策在 90 天內過期密碼
CIS v1.2.0	1.12 確保不存在根使用者存取金鑰	【IAM.4】 IAM 根使用者存取金鑰不應存在
CIS v1.2.0	1.13 確定已啟用根使用者的 MFA	【IAM.9】 應為根使用者啟用 MFA
CIS v1.2.0	1.14 確定已啟用根使用者的硬體 MFA	[IAM.6] 應為根使用者啟用硬體 MFA
CIS v1.2.0	1.16 確保 IAM 政策僅連接到群組或角色	【IAM.2】 IAM 使用者不應連接 IAM 政策
CIS v1.2.0	1.2 確保所有具有主控台密碼的 IAM 使用者都已啟用多重驗證 (MFA)	[IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
CIS v1.2.0	1.20 確定已建立支援角色以使用 管理事件 支援	【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援
CIS v1.2.0	1.22 確保未建立允許完整 "*" : "*" 管理權限的 IAM 政策	【IAM.1】 IAM 政策不應允許完整的「*」管理權限
CIS v1.2.0	1.3 確定停用 90 天 (含) 以上未使用的登入資料	【IAM.8】 應移除未使用的 IAM 使用者登入資料
CIS v1.2.0	1.4 確保每 90 天或更短期限輪換存取金鑰	【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
CIS v1.2.0	1.5 確保 IAM 密碼政策至少需要一個大寫字母	【IAM.11】 確保 IAM 密碼政策至少需要一個大寫字母

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS v1.2.0	1.6 確保 IAM 密碼政策至少需要一個小寫字母	【IAM.12】 確保 IAM 密碼政策至少需要一個小寫字母
CIS v1.2.0	1.7 確保 IAM 密碼政策至少需要一個符號	【IAM.13】 確保 IAM 密碼政策至少需要一個符號
CIS v1.2.0	1.8 確保 IAM 密碼政策至少需要一個數字	【IAM.14】 確保 IAM 密碼政策至少需要一個數字
CIS v1.2.0	1.9 確保 IAM 密碼政策要求密碼長度下限為 14 或更高	【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高
CIS v1.2.0	2.1 確保所有區域都已啟用 CloudTrail	【CloudTrail.1】 CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤
CIS v1.2.0	2.2 確保 CloudTrail 日誌檔案驗證已啟用	【CloudTrail.4】 應啟用 CloudTrail 日誌檔案驗證
CIS v1.2.0	2.3 確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取	【CloudTrail.6】 確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取
CIS v1.2.0	2.4 確保 CloudTrail 追蹤與 CloudWatch Logs 整合	【CloudTrail.5】 CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合
CIS v1.2.0	2.5 確保 AWS Config 已啟用	【Config.1】 AWS Config 應啟用並使用服務連結角色進行資源記錄
CIS v1.2.0	2.6 確保 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄	【CloudTrail.7】 確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄
CIS v1.2.0	2.7 確保使用 KMS CMKs 對 CloudTrail 日誌進行靜態加密	【CloudTrail.2】 CloudTrail 應啟用靜態加密

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS v1.2.0	2.8 確定輪換客戶建立的 CMK	【KMS.4】應啟用 AWS KMS 金鑰輪換
CIS v1.2.0	2.9 確定所有 VPC 中皆已啟用 VPC 流程記錄	【EC2.6】應在所有 VPC 中啟用 VPCs 流程記錄
CIS v1.2.0	3.1 確定未經授權的 API 呼叫中存在日誌指標篩選條件和警示	【CloudWatch.2】確保未經授權的 API 呼叫存在日誌指標篩選條件和警示
CIS v1.2.0	3.10 確定安全群組變更存在日誌指標篩選條件和警示	【CloudWatch.10】確保安全群組變更存在日誌指標篩選條件和警示
CIS v1.2.0	3.11 確定網路存取控制清單 (NACL) 變更存在日誌指標篩選條件和警示	【CloudWatch.11】確定網路存取控制清單 (NACL) 的變更存在日誌指標篩選條件和警示
CIS v1.2.0	3.12 確定網路閘道變更存在日誌指標篩選條件和警示	【CloudWatch.12】確保網路閘道變更存在日誌指標篩選條件和警示
CIS v1.2.0	3.13 確定路由表變更存在日誌指標篩選條件和警示	【CloudWatch.13】確保路由表變更存在日誌指標篩選條件和警示
CIS v1.2.0	3.14 確定 VPC 變更存在日誌指標篩選條件和警示	【CloudWatch.14】確保 VPC 變更存在日誌指標篩選條件和警示
CIS v1.2.0	3.2 確保沒有 MFA 的管理主控台登入存在日誌指標篩選條件和警示	【CloudWatch.3】確保沒有 MFA 的管理主控台登入存在日誌指標篩選條件和警示
CIS v1.2.0	3.3 確保根使用者的用量存在日誌指標篩選條件和警示	【CloudWatch.1】應該存在日誌指標篩選條件和警示以使用「根」使用者
CIS v1.2.0	3.4 確保 IAM 政策變更存在日誌指標篩選條件和警示	【CloudWatch.4】確保 IAM 政策變更存在日誌指標篩選條件和警示

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS v1.2.0	3.5 確保 CloudTrail 組態變更存在日誌指標篩選條件和警示	【CloudWatch.5】確保 CloudTrail 組態變更存在日誌指標篩選條件和警示
CIS v1.2.0	3.6 確保 AWS 管理主控台 驗證失敗時存在日誌指標篩選條件和警示	【CloudWatch.6】確保 AWS 管理主控台 驗證失敗時存在日誌指標篩選條件和警示
CIS v1.2.0	3.7 確定停用或排定刪除客戶建立的 CMK，存在日誌指標篩選條件和警示	【CloudWatch.7】確保日誌指標篩選條件和警示存在，以停用或排程刪除客戶受管金鑰
CIS v1.2.0	3.8 確定 S3 儲存貯體政策變更存在日誌指標篩選條件和警示	【CloudWatch.8】確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示
CIS v1.2.0	3.9 確保 AWS Config 組態變更存在日誌指標篩選條件和警示	【CloudWatch.9】確保 AWS Config 組態變更存在日誌指標篩選條件和警示
CIS v1.2.0	4.1 確保無安全群組允許從 0.0.0.0/0 輸入連接埠 22	【EC2.13】安全群組不應允許從 0.0.0.0/0 或 :::/0 傳入連接埠 22
CIS v1.2.0	4.2 確保無安全群組允許從 0.0.0.0/0 輸入連接埠 3389	【EC2.14】安全群組不應允許從 0.0.0.0/0 或 :::/0 傳入連接埠 3389
CIS v1.2.0	4.3 確保每個 VPC 的預設安全群組都會限制所有流量	【EC2.2】VPC 預設安全群組不應允許傳入或傳出流量
CIS 1.4.0 版	1.10 確保所有具有主控台密碼的 IAM 使用者都已啟用多重要素驗證 (MFA)	[IAM.5] 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA
CIS 1.4.0 版	1.14 確保每 90 天或更短時間輪換存取金鑰	【IAM.3】IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次
CIS 1.4.0 版	1.16 確保未連接允許完整 "*" : "*" 管理權限的 IAM 政策	【IAM.1】IAM 政策不應允許完整的「*」管理權限

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS 1.4.0 版	1.17 確定已建立支援角色來使用 管理事件 支援	【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援
CIS 1.4.0 版	1.4 確保根使用者帳戶存取金鑰不存在	【IAM.4】 IAM 根使用者存取金鑰不應存在
CIS 1.4.0 版	1.5 確定根使用者帳戶已啟用 MFA	【IAM.9】 應為根使用者啟用 MFA
CIS 1.4.0 版	1.6 確定已啟用根使用者帳戶的硬體 MFA	[IAM.6] 應為根使用者啟用硬體 MFA
CIS 1.4.0 版	1.7 避免將根使用者用於管理和日常任務	【CloudWatch.1】 應該存在日誌指標篩選條件和警示以使用「根」使用者
CIS 1.4.0 版	1.8 確保 IAM 密碼政策的長度下限為 14 或更高	【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高
CIS 1.4.0 版	1.9 確保 IAM 密碼政策防止密碼重複使用	【IAM.16】 確保 IAM 密碼政策防止密碼重複使用
CIS 1.4.0 版	2.1.2 確保 S3 儲存貯體政策設定為拒絕 HTTP 請求	【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL
CIS 1.4.0 版	應啟用 2.1.5.1 S3 封鎖公開存取設定	【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定
CIS 1.4.0 版	2.1.5.2 S3 封鎖公開存取設定應在儲存貯體層級啟用	【S3.8】 S3 一般用途儲存貯體應封鎖公開存取
CIS 1.4.0 版	2.2.1 確保已啟用 EBS 磁碟區加密	【EC2.7】 應啟用 EBS 預設加密
CIS 1.4.0 版	2.3.1 確定已啟用 RDS 執行個體的加密	[RDS.3] RDS 資料庫執行個體應啟用靜態加密
CIS 1.4.0 版	3.1 確保所有區域都已啟用 CloudTrail	【CloudTrail.1】 CloudTrail 應該啟用並設定至少一個包含讀取和寫入管理事件的多區域追蹤

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS 1.4.0 版	3.2 確保已啟用 CloudTrail 日誌檔案驗證	【CloudTrail.4】應啟用 CloudTrail 日誌檔案驗證
CIS 1.4.0 版	3.4 確保 CloudTrail 追蹤與 CloudWatch Logs 整合	【CloudTrail.5】CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合
CIS 1.4.0 版	3.5 確保所有區域 AWS Config 都已啟用	【Config.1】AWS Config 應啟用並使用服務連結角色進行資源記錄
CIS 1.4.0 版	3.6 確保 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄	【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄
CIS 1.4.0 版	3.7 確保 CloudTrail 日誌使用 KMS CMKs 進行靜態加密	[CloudTrail.2] CloudTrail 應啟用靜態加密
CIS 1.4.0 版	3.8 確保已啟用客戶建立CMKs 輪換	【KMS.4】應啟用 AWS KMS 金鑰輪換
CIS 1.4.0 版	3.9 確保所有 VPC 中都已啟用 VPCs 流程記錄	【EC2.6】應在所有 VPC 中啟用 VPCs 流程記錄
CIS 1.4.0 版	4.4 確保 IAM 政策變更存在日誌指標篩選條件和警示	【CloudWatch.4】確保 IAM 政策變更存在日誌指標篩選條件和警示
CIS 1.4.0 版	4.5 確保 CloudTrail 組態變更存在日誌指標篩選條件和警示	【CloudWatch.5】確保 CloudTrail 組態變更存在日誌指標篩選條件和警示
CIS 1.4.0 版	4.6 確保 AWS 管理主控台 驗證失敗時存在日誌指標篩選條件和警示	【CloudWatch.6】確保 AWS 管理主控台 驗證失敗時存在日誌指標篩選條件和警示
CIS 1.4.0 版	4.7 確保日誌指標篩選條件和警示存在，以停用或排程刪除客戶建立的 CMKs	【CloudWatch.7】確保日誌指標篩選條件和警示存在，以停用或排程刪除客戶受管金鑰

標準	標準控制項 ID 和標題	安全控制 ID 和標題
CIS 1.4.0 版	4.8 確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示	【CloudWatch.8】確保 S3 儲存貯體政策變更存在日誌指標篩選條件和警示
CIS 1.4.0 版	4.9 確保 AWS Config 組態變更存在日誌指標篩選條件和警示	【CloudWatch.9】確保 AWS Config 組態變更存在日誌指標篩選條件和警示
CIS 1.4.0 版	4.10 確保安全群組變更存在日誌指標篩選條件和警示	【CloudWatch.10】確保安全群組變更存在日誌指標篩選條件和警示
CIS 1.4.0 版	4.11 確保網路存取控制清單 (NACL) 的變更存在日誌指標篩選條件和警示	【CloudWatch.11】確定網路存取控制清單 (NACL) 的變更存在日誌指標篩選條件和警示
CIS 1.4.0 版	4.12 確保網路閘道變更存在日誌指標篩選條件和警示	【CloudWatch.12】確保網路閘道變更存在日誌指標篩選條件和警示
CIS 1.4.0 版	4.13 確保路由表變更存在日誌指標篩選條件和警示	【CloudWatch.13】確保路由表變更存在日誌指標篩選條件和警示
CIS 1.4.0 版	4.14 確保 VPC 變更存在日誌指標篩選條件和警示	【CloudWatch.14】確保 VPC 變更存在日誌指標篩選條件和警示
CIS 1.4.0 版	5.1 確保網路 ACLs 不允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠	【EC2.21】網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389
CIS 1.4.0 版	5.3 確保每個 VPC 的預設安全群組會限制所有流量	【EC2.2】VPC 預設安全群組不應允許傳入或傳出流量
PCI DSS v3.2.1	PCI.AutoScaling.1 與負載平衡器相關的自動擴展群組應使用負載平衡器運作狀態檢查	【AutoScaling.1】與負載平衡器相關的 Auto Scaling 群組應使用 ELB 運作狀態檢查
PCI DSS v3.2.1	PCI.CloudTrail.1 CloudTrail 日誌應使用 AWS KMS CMKs 進行靜態加密	[CloudTrail.2] CloudTrail 應啟用靜態加密

標準	標準控制項 ID 和標題	安全控制 ID 和標題
PCI DSS v3.2.1	應啟用 PCI.CloudTrail.2 CloudTrail	【CloudTrail.3】至少應啟用一個 CloudTrail 追蹤
PCI DSS v3.2.1	應啟用 PCI.CloudTrail.3 CloudTrail 日誌檔案驗證	【CloudTrail.4】應啟用 CloudTrail 日誌檔案驗證
PCI DSS v3.2.1	PCI.CloudTrail.4 CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合	【CloudTrail.5】CloudTrail 追蹤應與 Amazon CloudWatch Logs 整合
PCI DSS v3.2.1	PCI.CodeBuild.1 CodeBuild GitHub 或 Bitbucket 來源儲存庫 URLs 應使用 OAuth	【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料
PCI DSS v3.2.1	PCI.CodeBuild.2 CodeBuild 專案環境變數不應包含純文字登入資料	【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料
PCI DSS v3.2.1	AWS Config 應啟用 PCI.Config.1	【Config.1】AWS Config 應啟用並使用服務連結角色進行資源記錄
PCI DSS v3.2.1	PCI.CW.1 應使用「根」使用者的日誌指標篩選條件和警示	【CloudWatch.1】應該存在日誌指標篩選條件和警示以使用「根」使用者
PCI DSS v3.2.1	PCI.DMS.1 Database Migration Service 複寫執行個體不應為公有	【DMS.1】Database Migration Service 複寫執行個體不應為公有
PCI DSS v3.2.1	PCI.EC2.1 EBS 快照不應可公開還原	【EC2.1】Amazon EBS 快照不應設定為可公開還原
PCI DSS v3.2.1	PCI.EC2.2 VPC 預設安全群組應禁止傳入和傳出流量	【EC2.2】VPC 預設安全群組不應允許傳入或傳出流量
PCI DSS v3.2.1	應移除 PCI.EC2.4 未使用的 EC2 EIPs	【EC2.12】應移除未使用的 Amazon EC2 EIPs
PCI DSS v3.2.1	PCI.EC2.5 安全群組不應允許從 0.0.0.0/0 傳入連接埠 22	【EC2.13】安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 22

標準	標準控制項 ID 和標題	安全控制 ID 和標題
PCI DSS v3.2.1	應在所有 VPC 中啟用 PCI.EC2.6 VPCs 流程記錄	【EC2.6】 應在所有 VPC 中啟用 VPCs 流程記錄
PCI DSS v3.2.1	PCI.ELBv2.1 Application Load Balancer 應設定為將所有 HTTP 請求重新導向至 HTTPS	【ELB.1】 Application Load Balancer 應設定為將所有 HTTP 請求重新導向至 HTTPS
PCI DSS v3.2.1	PCI.ES.1 Elasticsearch 網域應該位於 VPC 中	【ES.2】 不應公開存取 Elasticsearch 網域
PCI DSS v3.2.1	PCI.ES.2 Elasticsearch 網域應該啟用靜態加密	【ES.1】 Elasticsearch 網域應該啟用靜態加密
PCI DSS v3.2.1	應啟用 PCI.GuardDuty.1 GuardDuty	【GuardDuty.1】 應啟用 GuardDuty
PCI DSS v3.2.1	PCI.IAM.1 IAM 根使用者存取金鑰不應存在	【IAM.4】 IAM 根使用者存取金鑰不應存在
PCI DSS v3.2.1	PCI.IAM.2 IAM 使用者不應連接 IAM 政策	【IAM.2】 IAM 使用者不應連接 IAM 政策
PCI DSS v3.2.1	PCI.IAM.3 IAM 政策不應允許完整的「*」管理權限	【IAM.1】 IAM 政策不應允許完整的「*」管理權限
PCI DSS v3.2.1	應為根使用者啟用 PCI.IAM.4 硬體 MFA	【IAM.6】 應為根使用者啟用硬體 MFA
PCI DSS v3.2.1	應為根使用者啟用 PCI.IAM.5 Virtual MFA	【IAM.9】 應為根使用者啟用 MFA
PCI DSS v3.2.1	應為所有 IAM 使用者啟用 PCI.IAM.6 MFA	【IAM.19】 應為所有 IAM 使用者啟用 MFA
PCI DSS v3.2.1	如果未在預先定義的天數內使用 PCI.IAM.7 IAM 使用者憑證，則應停用	【IAM.8】 應移除未使用的 IAM 使用者登入資料

標準	標準控制項 ID 和標題	安全控制 ID 和標題
PCI DSS v3.2.1	IAM 使用者的 PCI.IAM.8 密碼政策應具有強大的組態	【IAM.10】 IAM 使用者的密碼政策應具有強大的組態
PCI DSS v3.2.1	應啟用 PCI.KMS.1 客戶主金鑰 (CMK) 輪換	【KMS.4】 應啟用 AWS KMS 金鑰輪換
PCI DSS v3.2.1	PCI.Lambda.1 Lambda 函數應禁止公開存取	【Lambda.1】 Lambda 函數政策應禁止公開存取
PCI DSS v3.2.1	PCI.Lambda.2 Lambda 函數應該位於 VPC 中	【Lambda.3】 Lambda 函數應該位於 VPC 中
PCI DSS v3.2.1	PCI.Opensearch.1 OpenSearch 網域應該位於 VPC 中	【Opensearch.2】 不應公開存取 OpenSearch 網域
PCI DSS v3.2.1	PCI.Opensearch.2 EBS 快照不應可公開還原	【Opensearch.1】 OpenSearch 網域應該啟用靜態加密
PCI DSS v3.2.1	PCI.RDS.1 RDS 快照應為私有	【RDS.1】 RDS 快照應為私有
PCI DSS v3.2.1	PCI.RDS.2 RDS 資料庫執行個體應禁止公開存取	【RDS.2】 RDS 資料庫執行個體應禁止公開存取，由 PubliclyAccessible 組態決定
PCI DSS v3.2.1	PCI.Redshift.1 Amazon Redshift 叢集應禁止公開存取	【Redshift.1】 Amazon Redshift 叢集應禁止公開存取
PCI DSS v3.2.1	PCI.S3.1 S3 儲存貯體應禁止公有寫入存取	【S3.3】 S3 一般用途儲存貯體應封鎖公有寫入存取
PCI DSS v3.2.1	PCI.S3.2 S3 儲存貯體應禁止公開讀取存取	【S3.2】 S3 一般用途儲存貯體應封鎖公開讀取存取
PCI DSS v3.2.1	PCI.S3.3 S3 儲存貯體應啟用跨區域複寫	【S3.7】 S3 一般用途儲存貯體應使用跨區域複寫
PCI DSS v3.2.1	PCI.S3.5 S3 儲存貯體應要求請求使用 Secure Socket Layer	【S3.5】 S3 一般用途儲存貯體應要求請求使用 SSL

標準	標準控制項 ID 和標題	安全控制 ID 和標題
PCI DSS v3.2.1	應啟用 PCI.S3.6 S3 封鎖公開存取設定	【S3.1】 S3 一般用途儲存貯體應啟用封鎖公開存取設定
PCI DSS v3.2.1	PCI.SageMaker.1 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取	【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取
PCI DSS v3.2.1	Systems Manager 管理的 PCI.SSM.1 EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態	【SSM.2】 Systems Manager 管理的 Amazon EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態
PCI DSS v3.2.1	Systems Manager 管理的 PCI.SSM.2 EC2 執行個體應具有 COMPLIANT 的關聯合規狀態	【SSM.3】 Systems Manager 管理的 Amazon EC2 執行個體應具有 COMPLIANT 的關聯合規狀態
PCI DSS v3.2.1	PCI.SSM.3 EC2 執行個體應該由 管理 AWS Systems Manager	【SSM.1】 Amazon EC2 執行個體應該由 管理 AWS Systems Manager

更新整合的工作流程

如果您的工作流程不依賴控制調查結果中任何欄位的特定格式，則不需要任何動作。

如果您的工作流程依賴控制調查結果中一或多個欄位的特定格式，如上表所述，您應該更新您的工作流程。例如，如果您建立的 Amazon EventBridge 規則觸發特定控制項 ID 的動作，例如在控制項 ID 等於 CIS 2.7 時叫用 AWS Lambda 函數，請更新規則以使用 CloudTrail.2,這是該控制項 Compliance.SecurityControlId 欄位的值。

如果您建立的[自訂洞見](#)使用任何已變更的欄位或值，請更新這些洞見以使用新的欄位或值。

必要的頂層 ASFF 屬性

安全性 AWS 問題清單格式 (ASFF) 中的下列頂層屬性是 Security Hub CSPM 中所有問題清單的必要項目。如需這些屬性的詳細資訊，請參閱 AWS Security Hub API 參考[AwsSecurityFinding](#)中的。

AwsAccountId

調查結果套用的 AWS 帳戶 ID。

範例

```
"AwsAccountId": "111111111111"
```

CreatedAt

指出問題清單擷取的潛在安全問題或事件建立的時間。

範例

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

說明

問題清單的描述。此欄位可以是非特定的範例文字或問題清單執行個體的特定詳細資訊。

對於 Security Hub CSPM 產生的控制項調查結果，此欄位提供控制項的說明。

如果您開啟[合併控制調查結果](#)，此欄位不會參考標準。

範例

```
"Description": "This AWS control checks whether AWS Config is enabled in the current account and Region."
```

GeneratorId

產生問題清單的解決方案特定元件 (邏輯分散式單位) 識別符。

對於 Security Hub CSPM 產生的控制調查結果，如果您開啟[合併的控制調查結果](#)，則此欄位不會參考標準。

範例

```
"GeneratorId": "security-control/Config.1"
```

Id

問題清單的產品特定識別符。對於 Security Hub CSPM 產生的控制調查結果，此欄位會提供調查結果的 Amazon Resource Name (ARN)。

如果您開啟[合併控制調查結果](#)，此欄位不會參考標準。

範例

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

Security Hub CSPM 產生的 Amazon Resource Name (ARN)，可在產品向 Security Hub CSPM 註冊後唯一識別第三方調查結果產品。

此欄位的格式為 `arn:partition:securityhub:region:account-id:product/company-id/product-id`。

- 對於與 Security Hub CSPM 整合 AWS 服務的，`company-id` 必須是 "aws"，而 `product-id` 必須是 AWS 公有服務名稱。由於 AWS 產品和服務未與帳戶建立關聯，因此 ARN 的 `account-id` 區段為空白。尚未與 Security Hub CSPM 整合 AWS 服務的會被視為第三方產品。
- 針對公有產品，`company-id` 和 `product-id` 必須是註冊時指定的 ID 值。
- 針對私有產品，`company-id` 必須是帳戶 ID。 `product-id` 必須是預留的 "default" 字詞，或註冊時指定的 ID。

範例

```
// Private ARN
"ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/default"

// Public ARN
"ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
"ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-pro"
```

Resources

物件 `Resources` 陣列提供一組資源資料類型，描述調查結果所參考 AWS 的資源。如需 `Resources` 物件可能包含之欄位的詳細資訊，包括需要哪些欄位，請參閱 AWS Security Hub API 參考 [Resource](#) 中的。如需特定 `Resources` 物件的範例 AWS 服務，請參閱 [Resources ASFF 物件](#)。

範例

```

"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
      "DetailedResultsLocation": "Path_to_Folder_Or_File",
      "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
          "Code": "COMPLETE",
          "Reason": "Unsupportedfield"
        }
      },
      "SensitiveData": [
        {
          "Category": "PERSONAL_INFORMATION",
          "Detections": [
            {
              "Count": 34,
              "Type": "GE_PERSONAL_ID",
              "Occurrences": {
                "LineRanges": [
                  {
                    "Start": 1,
                    "End": 10,
                    "StartColumn": 20
                  }
                ],
                "Pages": [],
                "Records": [],
                "Cells": []
              }
            }
          ],
          "Count": 59,
          "Type": "EMAIL_ADDRESS",
          "Occurrences": {
            "Pages": [
              {
                "PageNumber": 1,

```

```

        "OffsetRange": {
            "Start": 1,
            "End": 100,
            "StartColumn": 10
        },
        "LineRange": {
            "Start": 1,
            "End": 100,
            "StartColumn": 10
        }
    }
}
},
{
    "Count": 2229,
    "Type": "URL",
    "Occurrences": {
        "LineRanges": [
            {
                "Start": 1,
                "End": 13
            }
        ]
    }
},
{
    "Count": 13826,
    "Type": "NameDetection",
    "Occurrences": {
        "Records": [
            {
                "RecordIndex": 1,
                "JsonPath": "$.ssn.value"
            }
        ]
    }
},
{
    "Count": 32,
    "Type": "AddressDetection"
}
],
"TotalCount": 32

```

```

    }
  ],
  "CustomDataIdentifiers": {
    "Detections": [
      {
        "Arn": "1712be25e7c7f53c731fe464f1c869b8",
        "Name": "1712be25e7c7f53c731fe464f1c869b8",
        "Count": 2
      }
    ],
    "TotalCount": 2
  }
},
{
  "Type": "AwsEc2Instance",
  "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
  "Partition": "aws",
  "Region": "us-west-2",
  "ResourceRole": "Target",
  "Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": true
  },
  "Details": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IPv4Addresses": ["1.1.1.1"],
    "IPv6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    }
  },
  "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
  ],
  "SubnetId": "PublicSubnet",

```



```
"Type": "i3.xlarge",
"VirtualizationType": "hvm",
"VpcId": "TestVPCIPv6"
}

]
```

SchemaVersion

要格式化問題清單的結構描述版本。此欄位的值必須是 AWS 識別的正式發佈版本之一。在目前版本中，AWS 安全調查結果格式結構描述版本為 2018-10-08。

範例

```
"SchemaVersion": "2018-10-08"
```

嚴重性

定義問題清單的重要性。如需此物件的詳細資訊，請參閱《AWS Security Hub API 參考[Severity](#)》中的。

Severity 是調查結果中最上層的物件，並巢狀在 FindingProviderFields 物件下。

只能使用 [BatchUpdateFindings](#) API 更新調查結果的最上層 Severity 物件的值。

若要提供嚴重性資訊，問題清單提供者應在提出 [BatchImportFindings](#) API 請求 FindingProviderFields 時更新 下的 Severity 物件。

如果新調查結果的 BatchImportFindings 請求僅提供 Label 或僅提供 Normalized，Security Hub CSPM 會自動填入另一個欄位的值。

也可以填入 Product 和 Original 欄位。

如果頂層 Finding.Severity 物件存在但 Finding.FindingProviderFields 不存在，Security Hub CSPM 會建立 FindingProviderFields.Severity 物件並將整個物件複製到 Finding.Severity object 其中。這可確保原始供應商提供的詳細資訊會保留在 FindingProviderFields.Severity 結構中，即使覆寫頂層 Severity 物件也是如此。

問題清單嚴重性不會將牽涉之資產或基礎資源的重要性納入考量。重要性的定義是與問題清單相關聯之資源的重要性層級。例如，與關鍵任務應用程式相關聯的資源比與非生產測試相關聯的資源具有更高的重要性。如果要擷取資源重要性的資訊，請使用 Criticality 欄位。

將問題清單的原生嚴重性分數轉譯為 ASFF Severity.Label 中的 值時，建議使用下列指引。

- INFORMATIONAL – 此類別可能包括 PASSED、WARNING 或 NOT AVAILABLE 檢查的調查結果或敏感資料識別。
- LOW – 可能導致未來入侵的問題清單。例如，此類別可能包含漏洞、組態弱點和公開密碼。
- MEDIUM – 指出主動入侵，但未指出對手完成其目標的調查結果。例如，此類別可能包含惡意軟體活動、駭客活動和異常行為偵測。
- HIGH 或 CRITICAL – 指出對手完成其目標的調查結果，例如作用中的資料遺失或入侵，或是拒絕服務。

範例

```
"Severity": {
  "Label": "CRITICAL",
  "Normalized": 90,
  "Original": "CRITICAL"
}
```

Title

問題清單的標題。此欄位可以包含非特定的範例文字或此問題清單執行個體的特定詳細資訊。

對於控制項調查結果，此欄位提供控制項的標題。如果您開啟[合併控制問題清單](#)，則此欄位不會參考標準。

範例

```
"Title": "AWS Config should be enabled"
```

類型

一或多個格式為 *namespace/category/classifier* 的問題清單類型，可分類問題清單。如果您開啟[合併控制問題清單](#)，則此欄位不會參考標準。

Types 應僅使用 [BatchUpdateFindings](#) API 更新。

尋找想要提供 值的提供者時，Types 應使用 Types 下的 屬性[FindingProviderFields](#)。

在下列清單中，最上層項目符號是命名空間，第二層項目符號是類別，第三層項目符號是分類器。我們建議調查結果提供者使用定義的命名空間來協助排序和分組調查結果。定義的類別和分類器也可以使用，但不是必要的。只有軟體和組態檢查命名空間有定義的分類器。

您可以定義namespace/category/classifier的部分路徑。例如，下列調查結果類型都是有效的：

- TTP
- TTPs/Defense Evasion
- TTPs/Defense Evasion/CloudTrailStopped

下列清單中的策略、技術和程序 (TTPs) 類別符合 [MITRE ATT&CK Matrix™](#)。異常行為命名空間反映一般異常行為，例如一般統計異常，且與特定 TTP 不相符。不過，您可使用異常行為和 TTP 問題清單類型來分類問題清單。

命名空間、類別和分類器的清單：

- 軟體和組態檢查
 - 漏洞
 - CVE
 - AWS 安全最佳實務
 - 網路連線能力
 - 執行時間行為分析
 - 產業和法規標準
 - AWS 基礎安全最佳實務
 - CIS 主機強化基準
 - CIS AWS Foundations 基準
 - PCI-DSS
 - 雲端安全性聯盟控制
 - ISO 90001 控制
 - ISO 27001 控制
 - ISO 27017 控制
 - ISO 27018 控制
 - SOC 1
 - SOC 2
 - HIPAA 控制 (美國)
 - NIST 800-53 控制 (美國)
 - NIST CSF 控制 (美國)

- IRAP 控制 (澳大利亞)
- K-ISMS 控制 (韓國)
- MTCS 控制 (新加坡)
- FISC 控制 (日本)
- 個人編號法案控制 (日本)
- ENS 控制 (西班牙)
- Cyber Essentials Plus 控制 (英國)
- G-Cloud 控制 (英國)
- C5 控制 (德國)
- IT-Grundschutz 控制 (德國)
- GDPR 控制 (歐洲)
- TISAX 控制 (歐洲)
- 修補管理
- TTP
 - 初始存取
 - 執行
 - Persistence
 - 權限提升
 - 防禦逃脫
 - 登入資料存取
 - 探索
 - 水平擴散
 - 收集
 - 命令和控制
- 效果
 - 資料曝光
 - 資料外洩
 - 資料銷毀
 - 拒絕服務
- 資源耗用

- 異常行為
 - 應用程式
 - 網路流程
 - IP 位址
 - 使用者
 - VM
 - 容器
 - 無伺服器
 - 流程
 - 資料庫
 - 資料
- 敏感資料識別
 - PII
 - 密碼
 - 法律聲明
 - 金融
 - 安全
 - 商業

範例

```
"Types": [  
  "Software and Configuration Checks/Vulnerabilities/CVE"  
]
```

UpdatedAt

指出調查結果提供者上次更新調查結果記錄的時間。

此時間戳記反映調查結果記錄上次或最近更新的時間。因此，它可能與LastObservedAt時間戳記不同，時間戳記會反映事件或漏洞上次或最近觀察到的時間。

更新問題清單記錄時，您必須將此時間戳記更新為目前的時間戳記。建立問題清單記錄時，CreatedAt和 UpdatedAt時間戳記必須相同。更新調查結果記錄後，此欄位的值必須比包含的所有先前值更新。

請注意，UpdatedAt無法使用 [BatchUpdateFindings](#) 操作更新。您只能使用 [BatchImportFindings](#) 操作進行更新。

範例

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

選用最上層 ASFF 屬性

安全性 AWS 調查結果格式 (ASFF) 中的下列最上層屬性是 Security Hub CSPM 中調查結果的選用屬性。如需這些屬性的詳細資訊，請參閱 AWS Security Hub API 參考中的 [AwsSecurityFinding](#)。

Action

[Action](#) 物件提供有關影響資源或對資源採取之動作的詳細資訊。

範例

```
"Action": {
  "ActionType": "PORT_PROBE",
  "PortProbeAction": {
    "PortProbeDetails": [
      {
        "LocalPortDetails": {
          "Port": 80,
          "PortName": "HTTP"
        },
        "LocalIpDetails": {
          "IpAddressV4": "192.0.2.0"
        },
        "RemoteIpDetails": {
          "Country": {
            "CountryName": "Example Country"
          },
          "City": {
            "CityName": "Example City"
          },
          "GeoLocation": {
            "Lon": 0,
            "Lat": 0
          },
          "Organization": {
            "AsnOrg": "ExampleAS0",
```

```

        "Org": "ExampleOrg",
        "Isp": "ExampleISP",
        "Asn": 64496
      }
    }
  ],
  "Blocked": false
}

```

AwsAccountName

調查結果套用 AWS 帳戶 到的名稱。

範例

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

產生調查結果之產品的公司名稱。對於以控制項為基礎的調查結果，公司是 AWS。

Security Hub CSPM 會自動為每個調查結果填入此屬性。您無法使用 [BatchImportFindings](#) 或 進行更新 [BatchUpdateFindings](#)。例外狀況是當您使用自訂整合時。請參閱 [the section called “自訂產品整合”](#)。

當您使用 Security Hub CSPM 主控台依公司名稱篩選問題清單時，請使用此屬性。當您使用 Security Hub CSPM API 依公司名稱篩選問題清單時，您可以使用 下的 `aws/securityhub/CompanyName` 屬性 `ProductFields`。Security Hub CSPM 不會同步這兩個屬性。

範例

```
"CompanyName": "AWS"
```

合規

[Compliance](#) 物件通常會提供有關控制項調查結果的詳細資訊，例如適用的標準和控制項檢查的狀態。

範例

```
"Compliance": {
```

```

    "AssociatedStandards": [
      {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
      {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
      {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
      "NIST.800-53.r5 AC-4",
      "NIST.800-53.r5 AC-4(21)",
      "NIST.800-53.r5 SC-7",
      "NIST.800-53.r5 SC-7(11)",
      "NIST.800-53.r5 SC-7(16)",
      "NIST.800-53.r5 SC-7(21)",
      "NIST.800-53.r5 SC-7(4)",
      "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters": [
      {
        "Name": "authorizedTcpPorts",
        "Value": ["80", "443"]
      },
      {
        "Name": "authorizedUdpPorts",
        "Value": ["427"]
      }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
      {
        "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
        "Description": "This finding has a compliance status of NOT AVAILABLE because AWS Config sent Security Hub CSPM a finding with a compliance state of Not Applicable. The potential reasons for a Not Applicable finding from Config are that (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule itself includes scenarios where Not Applicable is returned. The specific reason why Not Applicable is returned is not available in the Config rule evaluation."
      }
    ]
  }
}

```

可信用度

調查結果準確識別其預期識別的行為或問題的可能性。

Confidence 應該只使用 更新 [BatchUpdateFindings](#)。

尋找想要提供 值的提供者時，Confidence 應使用 Confidence 下的 屬性 [FindingProviderFields](#)。請參閱 [the section called “使用 更新問題清單 FindingProviderFields”](#)。

Confidence 是以 0–100 為基準，使用比例比例來評分。0 表示 0% 可信度，100 表示 100% 可信度。例如，根據網路流量統計偏差的資料外洩偵測具有低可信度，因為尚未驗證實際的外洩。

範例

```
"Confidence": 42
```

重要性

指派給與問題清單相關聯資源的重要性層級。

Criticality 應僅透過呼叫 [BatchUpdateFindings](#) API 操作來更新。請勿使用 更新此物件 [BatchImportFindings](#)。

尋找想要提供 值的提供者時，Criticality 應使用 Criticality 下的 屬性 [FindingProviderFields](#)。請參閱 [the section called “使用 更新問題清單 FindingProviderFields”](#)。

Criticality 以 0–100 為基準，使用僅支援完整整數的比率比例。0 分表示不重要的基礎資源，100 分預留給最重要的資源。

對於每個資源，指派 時請考慮下列事項 Criticality：

- 受影響的資源是否包含敏感資料（例如具有 PII 的 S3 儲存貯體）？
- 受影響的資源是否可讓對手深化其存取權或擴展其能力，以執行其他惡意活動（例如，遭入侵的 sysadmin 帳戶）？
- 此資源是否為企業重要資產（例如，若遭入侵可能造成重大收益損失的業務系統）？

您可使用下列準則：

- 支援關鍵任務系統或包含高度敏感資料的資源可以在 75–100 範圍內評分。
- 支援重要（但非關鍵系統）或包含中等重要資料的資源可以在 25–74 範圍內評分。
- 支援不重要系統或包含非敏感資料的資源應在 0–24 範圍內評分。

範例

```
"Criticality": 99
```

偵測

Detection 物件提供來自 Amazon GuardDuty 延伸威脅偵測之攻擊序列調查結果的詳細資訊。當多個事件符合潛在可疑活動時，GuardDuty 會產生攻擊序列調查結果。若要在 AWS Security Hub CSPM 中接收 GuardDuty 攻擊序列調查結果，您必須在帳戶中啟用 GuardDuty。如需詳細資訊，請參閱 [《Amazon GuardDuty 使用者指南》中的 Amazon GuardDuty 延伸威脅偵測](#)。Amazon GuardDuty

範例

```
"Detection": {
  "Sequence": {
    "Uid": "111111111111-184ec3b9-cf8d-452d-9aad-f5bdb7afb010",
    "Actors": [{
      "Id": "USER:AR0A987654321EXAMPLE:i-b188560f:1234567891",
      "Session": {
        "Uid": "1234567891",
        "MfAStatus": "DISABLED",
        "CreatedTime": "1716916944000",
        "Issuer": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      },
      "User": {
        "CredentialUid": "ASIAIOSFODNN7EXAMPLE",
        "Name": "ec2_instance_role_production",
        "Type": "AssumedRole",
        "Uid": "AR0A987654321EXAMPLE:i-b188560f",
        "Account": {
          "Uid": "AccountId",
          "Name": "AccountName"
        }
      }
    }
  ],
  "Endpoints": [{
    "Id": "EndpointId",
    "Ip": "203.0.113.1",
    "Domain": "example.com",
    "Port": 4040,
    "Location": {
      "City": "New York",
      "Country": "US",
```

```

    "Lat": 40.7123,
    "Lon": -74.0068
  },
  "AutonomousSystem": {
    "Name": "AnyCompany",
    "Number": 64496
  },
  "Connection": {
    "Direction": "INBOUND"
  }
}],
"Signals": [{
  "Id": "arn:aws:guardduty:us-east-1:123456789012:detector/
d0bfe135ab8b4dd8c3eaae7df9900073/finding/535a382b1bcc44d6b219517a29058fb7",
  "Title": "Someone ran a penetration test tool on your account.",
  "ActorIds": ["USER:AR0A987654321EXAMPLE:i-b188560f:1234567891"],
  "Count": 19,
  "FirstSeenAt": 1716916943000,
  "SignalIndicators": [
    {
      "Key": "ATTACK_TACTIC",
      "Title": "Attack Tactic",
      "Values": [
        "Impact"
      ]
    },
    {
      "Key": "HIGH_RISK_API",
      "Title": "High Risk Api",
      "Values": [
        "s3:DeleteObject"
      ]
    },
    {
      "Key": "ATTACK_TECHNIQUE",
      "Title": "Attack Technique",
      "Values": [
        "Data Destruction"
      ]
    }
  ],
  "LastSeenAt": 1716916944000,
  "Name": "Test:IAMUser/KaliLinux",
  "ResourceIds": [

```

```
    "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  ],
  "Type": "FINDING"
}],
"SequenceIndicators": [
  {
    "Key": "ATTACK_TACTIC",
    "Title": "Attack Tactic",
    "Values": [
      "Discovery",
      "Exfiltration",
      "Impact"
    ]
  },
  {
    "Key": "HIGH_RISK_API",
    "Title": "High Risk Api",
    "Values": [
      "s3:DeleteObject",
      "s3:GetObject",
      "s3:ListBuckets",
      "s3:ListObjects"
    ]
  },
  {
    "Key": "ATTACK_TECHNIQUE",
    "Title": "Attack Technique",
    "Values": [
      "Cloud Service Discovery",
      "Data Destruction"
    ]
  }
]
}
```

FindingProviderFields

FindingProviderFields 包含下列屬性：

- Confidence
- Criticality
- RelatedFindings

- Severity
- Types

上述欄位會巢狀在 FindingProviderFields 物件下，但具有與最上層 ASFF 欄位同名的類比。當問題清單提供者將新問題清單傳送至 Security Hub CSPM 時，如果 FindingProviderFields 物件根據對應的頂層欄位為空白，Security Hub CSPM 會自動填入物件。

尋找提供者可以使用 Security Hub FindingProviderFields [BatchImportFindings](#) CSPM API 的操作進行更新。尋找提供者無法使用 更新此物件 [BatchUpdateFindings](#)。

如需 Security Hub CSPM 如何處理從 BatchImportFindings 到 FindingProviderFields 和對應頂層屬性的更新的詳細資訊，請參閱 [the section called “使用 更新問題清單 FindingProviderFields”](#)。

客戶可以使用 BatchUpdateFindings 操作更新最上層欄位。客戶無法更新 FindingProviderFields。

範例

```
"FindingProviderFields": {
  "Confidence": 42,
  "Criticality": 99,
  "RelatedFindings": [
    {
      "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000"
    }
  ],
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

指出首次觀察到問題清單所擷取的潛在安全問題或事件。

此時間戳記會指定第一次觀察到事件或漏洞的時間。因此，它可能與 CreatedAt 時間戳記不同，時間戳記會反映此調查結果記錄的建立時間。

對於 Security Hub CSPM 產生和更新的控制調查結果，此時間戳記也可以指出資源最近變更的合規狀態。對於其他類型的問題清單，此時間戳記在問題清單記錄的更新之間應不可變，但如果確定更準確的時間戳記，則可以更新。

範例

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

指出安全性調查結果產品何時最近觀察到問題清單所擷取的潛在安全問題或事件。

此時間戳記指定事件或漏洞上次或最近觀察到的時間。因此，它可能與UpdatedAt時間戳記不同，時間戳記會反映此調查結果記錄上次或最近更新的時間。

您可以提供此時間戳記，但在第一次觀察時不需要。如果您在第一次觀察時填入此欄位，時間戳記應與FirstObservedAt時間戳記相同。您應該更新此欄位，以在每次觀察到問題清單時，反映上次或最近觀察到的時間戳記。

範例

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

惡意軟體

[Malware](#) 物件提供與問題清單相關的惡意程式清單。

範例

```
"Malware": [  
  {  
    "Name": "Stringler",  
    "Type": "COIN_MINER",  
    "Path": "/usr/sbin/stringler",  
    "State": "OBSERVED"  
  }  
]
```

網路（已淘汰）

[Network](#) 物件提供有關問題清單的網路相關資訊。

此物件已淘汰。若要提供此資料，您可以將資料映射至 中的資源Resources，或使用 Action 物件。

範例

```
"Network": {
  "Direction": "IN",
  "OpenPortRange": {
    "Begin": 443,
    "End": 443
  },
  "Protocol": "TCP",
  "SourceIPv4": "1.2.3.4",
  "SourceIPv6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
  "SourcePort": "42",
  "SourceDomain": "example1.com",
  "SourceMac": "00:0d:83:b1:c0:8e",
  "DestinationIPv4": "2.3.4.5",
  "DestinationIPv6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
  "DestinationPort": "80",
  "DestinationDomain": "example2.com"
}
```

NetworkPath

[NetworkPath](#) 物件提供與問題清單相關的網路路徑資訊。中的每個項目都NetworkPath代表路徑的元件。

範例

```
"NetworkPath" : [
  {
    "ComponentId": "abc-01a234bc56d8901ee",
    "ComponentType": "AWS::EC2::InternetGateway",
    "Egress": {
      "Destination": {
        "Address": [ "192.0.2.0/24" ],
        "PortRanges": [
          {
            "Begin": 443,
            "End": 443
          }
        ]
      }
    },
    "Protocol": "TCP",
    "Source": {
```

```

        "Address": ["203.0.113.0/24"]
    },
    "Ingress": {
        "Destination": {
            "Address": [ "198.51.100.0/24" ],
            "PortRanges": [
                {
                    "Begin": 443,
                    "End": 443
                }
            ]
        },
        "Protocol": "TCP",
        "Source": {
            "Address": [ "203.0.113.0/24" ]
        }
    }
}
]

```

注意

Note 物件會指定使用者定義的備註，您可以將其新增至問題清單。

問題清單提供者可以提供問題清單的初始備註，但之後便無法新增備註。您只能使用 [更新備註BatchUpdateFindings](#)。

範例

```

"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}

```

PatchSummary

[PatchSummary](#) 物件會根據選取的合規標準，提供執行個體的修補程式合規狀態摘要。

範例

```

"PatchSummary" : {

```



```
"FailedCount" : 0,
"Id" : "pb-123456789098",
"InstalledCount" : 100,
"InstalledOtherCount" : 1023,
"InstalledPendingReboot" : 0,
"InstalledRejectedCount" : 0,
"MissingCount" : 100,
"Operation" : "Install",
"OperationEndTime" : "2018-09-27T23:39:31Z",
"OperationStartTime" : "2018-09-27T23:37:31Z",
"RebootOption" : "RebootIfNeeded"
}
```

流程

[Process](#) 物件提供有關問題清單的程序相關詳細資訊。

範例：

```
"Process": {
  "LaunchedAt": "2018-09-27T22:37:31Z",
  "Name": "syslogd",
  "ParentPid": 56789,
  "Path": "/usr/sbin/syslogd",
  "Pid": 12345,
  "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

指出 Security Hub CSPM 收到問題清單並開始處理的時間。

這與 CreatedAt 和 UpdatedAt 不同，這是與調查結果提供者與安全問題和調查結果互動相關的必要時間戳記。ProcessedAt 時間戳記指出 Security Hub CSPM 何時開始處理問題清單。處理完成後，問題清單會出現在使用者帳戶中。

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

一種資料類型，其中安全調查結果產品可以包含不屬於已定義 AWS 安全調查結果格式的其他解決方案特定詳細資訊。

對於 Security Hub CSPM 控制項產生的調查結果，ProductFields 包含控制項的相關資訊。請參閱 [the section called “產生和更新控制問題清單”](#)。

此欄位不應包含備援資料，且不得包含與 AWS Security Finding Format 欄位衝突的資料。

「aws/」字首僅代表 AWS 產品和服務的預留命名空間，不得與第三方整合的問題清單一起提交。

雖然非必要，但產品應該將欄位名稱格式化為 company-id/product-id/field-name，其中 company-id 和 product-id 符合問題清單 ProductArn 所提供的內容。

當 Security Hub CSPM 封存現有的問題清單時，Archival 會使用參考欄位。例如，Security Hub CSPM 會在您停用控制項或標準以及開啟或關閉 [合併控制項問題清單時封存現有的問題清單](#)。

此欄位也可能包含標準的相關資訊，其中包含產生調查結果的控制項。

範例

```
"ProductFields": {
  "API", "DeleteTrail",
  "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because consolidated control findings has been turned on or off. This causes findings in the previous state to be archived when new findings are being generated.",
  "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
  "aws/inspector/AssessmentTargetName": "My prod env",
  "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
  "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
  "generico/secure-pro/Action.Type", "AWS_API_CALL",
  "generico/secure-pro/Count": "6",
  "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

提供產生調查結果的產品名稱。對於以控制項為基礎的調查結果，產品名稱為 Security Hub CSPM。

Security Hub CSPM 會自動為每個調查結果填入此屬性。您無法使用 [BatchImportFindings](#) 或進行更新 [BatchUpdateFindings](#)。例外狀況是當您使用自訂整合時。請參閱 [the section called “自訂產品整合”](#)。

當您使用 Security Hub CSPM 主控台依產品名稱篩選問題清單時，請使用此屬性。

當您使用 Security Hub CSPM API 依產品名稱篩選問題清單時，您可以使用 下的 aws/securityhub/ProductName 屬性 ProductFields。

Security Hub CSPM 不會同步這兩個屬性。

RecordState

提供問題清單的記錄狀態。

根據預設，會將服務一開始產生的問題清單視為 ACTIVE。

ARCHIVED 狀態表示問題清單應被隱藏看不到。封存的問題清單不會立即刪除。您可以搜尋、檢閱和報告這些項目。如果刪除關聯的資源、資源不存在或停用控制項，Security Hub CSPM 會自動封存以控制項為基礎的調查結果。

RecordState 旨在尋找提供者，並且只能使用 [BatchImportFindings](#) 操作更新。您無法使用 [BatchUpdateFindings](#) 操作進行更新。

若要追蹤調查問題清單的狀態，請使用 [Workflow](#) 而非 RecordState。

如果記錄狀態從 變更為 ARCHIVED ACTIVE，且調查結果的工作流程狀態為 NOTIFIED 或 RESOLVED，Security Hub CSPM 會自動將工作流程狀態變更為 NEW。

範例

```
"RecordState": "ACTIVE"
```

區域

指定 AWS 區域 從中產生調查結果的。

Security Hub CSPM 會自動為每個調查結果填入此屬性。您無法使用 [BatchImportFindings](#) 或 進行更新 [BatchUpdateFindings](#)。

範例

```
"Region": "us-west-2"
```

RelatedFindings

提供與目前問題清單相關的問題清單。

RelatedFindings 應該只使用 [BatchUpdateFindings](#) API 操作更新。您不應該使用 更新此物件 [BatchImportFindings](#)。

對於[BatchImportFindings](#)請求，問題清單提供者應使用 下的 RelatedFindings 物件[FindingProviderFields](#)。

若要檢視RelatedFindings屬性的描述，請參閱 AWS Security Hub API 參考[RelatedFinding](#)中的。

範例

```
"RelatedFindings": [
  { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
    "Id": "123e4567-e89b-12d3-a456-426655440000" },
  { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
    "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

RiskAssessment

範例

```
"RiskAssessment": {
  "Posture": {
    "FindingTotal": 4,
    "Indicators": [
      {
        "Type": "Reachability",
        "Findings": [
          {
            "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/1234567890abcdef0",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
            "Title": "Finding title"
          },
          {
            "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/abcdef01234567890",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
            "Title": "Finding title"
          }
        ]
      }
    ],
  },
}
```

```

    {
      "Type": "Vulnerability",
      "Findings": [
        {
          "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/021345abcdef6789",
          "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
          "Title": "Finding title"
        },
        {
          "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/021345ghijkl6789",
          "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
          "Title": "Finding title"
        }
      ]
    }
  ]
}

```

修補

[Remediation](#) 物件可提供處理問題清單的建議修補步驟資訊。

範例

```

"Remediation": {
  "Recommendation": {
    "Text": "For instructions on how to fix this issue, see the AWS Security Hub CSPM documentation for EC2.2.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
  }
}

```

樣本

指定問題清單是否為範例問題清單。

```
"Sample": true
```

SourceUrl

SourceUrl 物件提供 URL，可連結至有關問題清單產品中目前問題清單的頁面。

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

[ThreatIntelIndicator](#) 物件會提供與問題清單相關的威脅情報詳細資訊。

範例

```
"ThreatIntelIndicators": [  
  {  
    "Category": "BACKDOOR",  
    "LastObservedAt": "2018-09-27T23:37:31Z",  
    "Source": "Threat Intel Weekly",  
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",  
    "Type": "IPV4_ADDRESS",  
    "Value": "8.8.8.8",  
  }  
]
```

威脅

[Threats](#) 物件提供調查結果偵測到之威脅的詳細資訊。

範例

```
"Threats": [{  
  "FilePaths": [{  
    "FileName": "b.txt",  
    "FilePath": "/tmp/b.txt",  
    "Hash": "sha256",  
    "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"  
  }],  
  "ItemCount": 3,  
  "Name": "Iot.linux.mirai.vwisi",  
  "Severity": "HIGH"  
}]
```

UserDefinedFields

提供與調查結果相關聯的名稱值字串對清單。這些是新增到問題清單的自訂使用者定義欄位。這些欄位可以透過您的特定組態自動產生。

尋找提供者不應將此欄位用於產品產生的資料。反之，問題清單提供者可以將 ProductFields 欄位用於未對應至任何標準 AWS 安全性問題清單格式欄位的資料。

這些欄位只能使用 [BatchUpdateFindings](#) 更新。

範例

```
"UserDefinedFields": {
  "reviewedByCio": "true",
  "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

提供調查結果的真實性。問題清單產品可為UNKNOWN此欄位提供 的值。如果問題清單產品的系統中有有意義的類比，問題清單產品應該提供此欄位的值。調查問題清單後，使用者判斷或動作通常會填入此欄位。

問題清單提供者可以提供此屬性的初始值，但之後便無法更新該值。您只能使用 [更新此屬性BatchUpdateFindings](#)。

```
"VerificationState": "Confirmed"
```

漏洞

[Vulnerabilities](#) 物件提供與調查結果相關聯的漏洞清單。

範例

```
"Vulnerabilities" : [
  {
    "CodeVulnerabilities": [{
      "Cwes": [
        "CWE-798",
        "CWE-799"
      ],
      "FilePath": {
        "EndLine": 421,
```

```

        "FileName": "package-lock.json",
        "FilePath": "package-lock.json",
        "StartLine": 420
    },
    "SourceArn": "arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
  ]],
  "Cvss": [
    {
      "BaseScore": 4.7,
      "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
      "Version": "V3"
    },
    {
      "BaseScore": 4.7,
      "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
      "Version": "V2"
    }
  ],
  "EpssScore": 0.015,
  "ExploitAvailable": "YES",
  "FixAvailable": "YES",
  "Id": "CVE-2020-12345",
  "LastKnownExploitAt": "2020-01-16T00:01:35Z",
  "ReferenceUrls": [
    "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
    "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
  ],
  "RelatedVulnerabilities": ["CVE-2020-12345"],
  "Vendor": {
    "Name": "Alas",
    "Url": "https://alas.aws.amazon.com/ALAS-2020-1337.html",
    "VendorCreatedAt": "2020-01-16T00:01:43Z",
    "VendorSeverity": "Medium",
    "VendorUpdatedAt": "2020-01-16T00:01:43Z"
  },
  "VulnerablePackages": [
    {
      "Architecture": "x86_64",
      "Epoch": "1",
      "FilePath": "/tmp",
      "FixedInVersion": "0.14.0",
      "Name": "openssl",
      "PackageManager": "OS",

```



```

        "Release": "16.amzn2.0.3",
        "Remediation": "Update aws-crt to 0.14.0",
        "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
        "SourceLayerHash":
            "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
        "Version": "1.0.2k"
    }
}
]

```

工作流程

[Workflow](#) 物件會提供關於問題清單調查狀態的相關資訊。

此欄位旨在供客戶搭配修復、協同運作和票證工具使用。這不適用於問題清單提供者。

您只能使用 更新 Workflow 欄位 [BatchUpdateFindings](#)。客戶也只能從主控台進行更新。請參閱 [the section called “設定問題清單的工作流程狀態”](#)。

範例

```

"Workflow": {
    "Status": "NEW"
}

```

WorkflowState (已淘汰)

此物件已淘汰，並已由 Workflow 物件的 Status 欄位取代。

此欄位提供調查結果的工作流程狀態。問題清單產品可針對此欄位提供 NEW 值。如果問題清單產品系統中有意義的類比，問題清單產品可針對此欄位提供值。

範例

```

"WorkflowState": "NEW"

```

Resources ASFF 物件

在 AWS 安全調查結果格式 (ASFF) 中，Resources 物件會提供調查結果所涉及資源的相關資訊。它包含最多 32 個資源物件的陣列。若要判斷資源名稱的格式，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。如需每個資源物件的範例，請從下列清單中選取資源。

主題

- [ASFF 中的資源屬性](#)
- [AwsAmazonMQ ASFF 中的 資源](#)
- [AwsApiGateway ASFF 中的 資源](#)
- [AwsAppSync ASFF 中的 資源](#)
- [AwsAthena ASFF 中的 資源](#)
- [AwsAutoScaling ASFF 中的 資源](#)
- [AwsBackup ASFF 中的 資源](#)
- [AwsCertificateManager ASFF 中的 資源](#)
- [AwsCloudFormation ASFF 中的 資源](#)
- [AwsCloudFront ASFF 中的 資源](#)
- [AwsCloudTrail ASFF 中的 資源](#)
- [AwsCloudWatch ASFF 中的 資源](#)
- [AwsCodeBuild ASFF 中的 資源](#)
- [AwsDms ASFF 中的 資源](#)
- [AwsDynamoDB ASFF 中的 資源](#)
- [AwsEc2 ASFF 中的 資源](#)
- [AwsEcr ASFF 中的 資源](#)
- [AwsEcs ASFF 中的 資源](#)
- [AwsEfs ASFF 中的 資源](#)
- [AwsEks ASFF 中的 資源](#)
- [AwsElasticBeanstalk ASFF 中的 資源](#)
- [AwsElasticSearch ASFF 中的 資源](#)
- [AwsElb ASFF 中的 資源](#)
- [AwsEventBridge ASFF 中的 資源](#)
- [AwsGuardDuty ASFF 中的 資源](#)
- [AwsIam ASFF 中的 資源](#)
- [AwsKinesis ASFF 中的 資源](#)
- [AwsKms ASFF 中的 資源](#)

- [AwsLambda](#)
- [AwsMsk ASFF 中的 資源](#)
- [AwsNetworkFirewall ASFF 中的 資源](#)
- [AwsOpenSearchService ASFF 中的 資源](#)
- [AwsRds ASFF 中的 資源](#)
- [AwsRedshift ASFF 中的 資源](#)
- [AwsRoute53 ASFF 中的 資源](#)
- [AwsS3 ASFF 中的 資源](#)
- [AwsSageMaker ASFF 中的 資源](#)
- [AwsSecretsManager ASFF 中的 資源](#)
- [AwsSns ASFF 中的 資源](#)
- [AwsSqs ASFF 中的 資源](#)
- [AwsSsm ASFF 中的 資源](#)
- [AwsStepFunctions ASFF 中的 資源](#)
- [AwsWaf ASFF 中的 資源](#)
- [AwsXray ASFF 中的 資源](#)
- [CodeRepository ASFF 中的 物件](#)
- [Container ASFF 中的 物件](#)
- [Other ASFF 中的 物件](#)

ASFF 中的資源屬性

以下是 AWS 安全性調查結果格式 (ASFF) 中Resources物件的描述和範例。如需有關這些欄位的詳細資訊，請參閱 [Resources](#)。

ApplicationArn

識別問題清單所涉及應用程式的 Amazon Resource Name (ARN)。

範例

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/SampleApp/1234567890abcdef0"
```

ApplicationName

識別問題清單所涉及的應用程式名稱。

範例

```
"ApplicationName": "SampleApp"
```

DataClassification

[DataClassification](#) 欄位提供有關在資源上偵測到的敏感資料的資訊。

範例

```
"DataClassification": {
  "DetailedResultsLocation": "Path_to_Folder_Or_File",
  "Result": {
    "MimeType": "text/plain",
    "SizeClassified": 2966026,
    "AdditionalOccurrences": false,
    "Status": {
      "Code": "COMPLETE",
      "Reason": "Unsupportedfield"
    },
  },
  "SensitiveData": [
    {
      "Category": "PERSONAL_INFORMATION",
      "Detections": [
        {
          "Count": 34,
          "Type": "GE_PERSONAL_ID",
          "Occurrences": {
            "LineRanges": [
              {
                "Start": 1,
                "End": 10,
                "StartColumn": 20
              }
            ],
          },
          "Pages": [],
          "Records": [],
          "Cells": []
        }
      ]
    }
  ],
}
```

```

{
  "Count": 59,
  "Type": "EMAIL_ADDRESS",
  "Occurrences": {
    "Pages": [
      {
        "PageNumber": 1,
        "OffsetRange": {
          "Start": 1,
          "End": 100,
          "StartColumn": 10
        },
        "LineRange": {
          "Start": 1,
          "End": 100,
          "StartColumn": 10
        }
      }
    ]
  }
},
{
  "Count": 2229,
  "Type": "URL",
  "Occurrences": {
    "LineRanges": [
      {
        "Start": 1,
        "End": 13
      }
    ]
  }
},
{
  "Count": 13826,
  "Type": "NameDetection",
  "Occurrences": {
    "Records": [
      {
        "RecordIndex": 1,
        "JsonPath": "$.ssn.value"
      }
    ]
  }
}

```

```

        },
        {
            "Count": 32,
            "Type": "AddressDetection"
        }
    ],
    "TotalCount": 32
}
],
"CustomDataIdentifiers": {
    "Detections": [
        {
            "Arn": "1712be25e7c7f53c731fe464f1c869b8",
            "Name": "1712be25e7c7f53c731fe464f1c869b8",
            "Count": 2,
        }
    ],
    "TotalCount": 2
}
}
}
}

```

詳細資訊

[Details](#) 欄位提供使用適當物件之單一資源的其他資訊。每個資源都必須在物件中的個別資源Resources物件中提供。

請注意，如果調查結果大小超過 240 KB 的上限，則會從調查結果中移除Details物件。對於使用 AWS Config 規則的控制項調查結果，您可以在 AWS Config 主控台上檢視資源詳細資訊。

Security Hub CSPM 為其支援的資源類型提供一組可用的資源詳細資訊。這些詳細資訊對應至 Type 物件的值。盡可能使用提供的類型。

例如，如果資源是 S3 儲存貯體，請將資源設定為 TypeAwsS3Bucket，並在 [AwsS3Bucket](#) 物件中提供資源詳細資訊。

[Other](#) 物件可讓您提供自訂欄位和值。在下列情況下，您可以使用 Other 物件：

- 資源類型（資源 的值Type）沒有對應的詳細資訊物件。若要提供資源的詳細資訊，您可以使用 [Other](#) 物件。
- 資源類型的 物件不包含您要填入的所有欄位。在此情況下，請使用資源類型的詳細資訊物件來填入可用的欄位。使用 Other 物件來填入不在類型特定物件中的欄位。

- 資源類型不是提供的類型之一。在此情況下，將 `Resource.Type` 設定為 `Other`，並使用 `Other` 物件填入詳細資訊。

範例

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IPv4Addresses": ["1.1.1.1"],
    "IPv6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
      {
        "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIPv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bde52c97d235b7b4752f9f688566fe6de",
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd" }
}
```

Id

指定資源類型的識別符。

對於 Amazon Resource Name (ARNs) 識別 AWS 的資源，這是 ARN。

對於缺少 ARNs AWS 的資源，這是建立資源之 AWS 服務定義的識別符。

對於非AWS 資源，這是與資源相關聯的唯一識別符。

範例

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

分割區

資源所在的分割區。分割區是 的群組 AWS 區域。每個 的範圍 AWS 帳戶 都是一個分割區。

支援下列分割區：

- aws – AWS 區域
- aws-cn - 中國區域
- aws-us-gov – AWS GovCloud (US) Region

範例

```
"Partition": "aws"
```

區域

AWS 區域 此資源所在的 程式碼。如需區域代碼清單，請參閱[區域端點](#)。

範例

```
"Region": "us-west-2"
```

ResourceRole

識別調查結果中資源的角色。資源是調查結果活動的目標或執行活動的動作者。

範例

```
"ResourceRole": "target"
```


Tags (標籤)

此欄位提供問題清單所涉及資源的標籤索引鍵和值資訊。您可以標記 AWS Resource Groups 標記 API `GetResources` 操作 [支援的資源](#)。Security Hub CSPM 透過 [服務連結角色](#) 呼叫此操作，並在 AWS Security Finding Format (ASFF) `Resource.Id` 欄位填入資源 ARN 時擷取 AWS 資源標籤。系統會忽略無效的資源 IDs。

您可以將資源標籤新增至 Security Hub CSPM 擷取的問題清單，包括整合 AWS 服務 和第三方產品的問題清單。

新增標籤會告訴您在處理問題清單時與資源相關聯的標籤。您只能針對具有關聯標籤的資源包含 Tags 屬性。如果資源沒有相關聯的標籤，請不要在問題清單中包含 Tags 屬性。

在問題清單中包含資源標籤，不需要建置資料擴充管道或手動擴充安全問題清單的中繼資料。您也可以使用標籤來搜尋或篩選問題清單和洞見，並建立 [自動化規則](#)。

如需適用於標籤的限制資訊，請參閱 [標籤命名限制和要求](#)。

您只能提供存在於此欄位中 AWS 資源上的標籤。若要提供未在 AWS 安全調查結果格式中定義的資料，請使用 `Other` 詳細資訊子欄位。

範例

```
"Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": "true"
}
```

Type

您要提供詳細資訊的資源類型。

盡可能使用提供的資源類型之一，例如 `AwsEc2Instance` 或 `AwsS3Bucket`。

如果資源類型不符合任何提供的資源類型，請將資源設定為 `Type Other`，並使用 `Other` 詳細資訊子欄位填入詳細資訊。

支援的值會列在 [資源](#) 下。

範例

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ ASFF 中的 資源

以下是 AwsAmazonMQ 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsAmazonMQBroker

AwsAmazonMQBroker 提供 Amazon MQ 代理程式的相關資訊，這是在 Amazon MQ 上執行的訊息代理程式環境。

下列範例顯示AwsAmazonMQBroker物件的 ASFF。若要檢視AwsAmazonMQBroker屬性的說明，請參閱 AWS Security Hub API 參考中的 [AwsAmazonMQBroker](#)。

範例

```
"AwsAmazonMQBroker": {
  "AutoMinorVersionUpgrade": true,
  "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "BrokerName": "TestBroker",
  "Configuration": {
    "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Revision": 1
  },
  "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
  "EncryptionOptions": {
    "UseAwsOwnedKey": true
  },
  "EngineType": "ActiveMQ",
  "EngineVersion": "5.17.2",
  "HostInstanceType": "mq.t2.micro",
  "Logs": {
    "Audit": false,
    "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
    "General": false,
    "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
  },
  "MaintenanceWindowStartTime": {
    "DayOfWeek": "MONDAY",
```

```

    "TimeOfDay": "22:00",
    "TimeZone": "UTC"
  },
  "PubliclyAccessible": true,
  "SecurityGroups": [
    "sg-021345abcdef6789"
  ],
  "StorageType": "efs",
  "SubnetIds": [
    "subnet-1234567890abcdef0",
    "subnet-abcdef01234567890"
  ],
  "Users": [
    {
      "Username": "admin"
    }
  ]
}

```

AwsApiGateway ASFF 中的 資源

以下是 AwsApiGateway 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsApiGatewayRestApi

AwsApiGatewayRestApi 物件包含 Amazon API Gateway 第 1 版中 REST API 的相關資訊。

以下是安全AwsApiGatewayRestApi調查結果格式 AWS (ASFF) 中的範例調查結果。若要檢視AwsApiGatewayRestApi屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsApiGatewayRestApiDetails](#)。

範例

```

AwsApiGatewayRestApi: {
  "Id": "exampleapi",
  "Name": "Security Hub",
  "Description": "AWS Security Hub",
  "CreateDate": "2018-11-18T10:20:05-08:00",
  "Version": "2018-10-26",
  "BinaryMediaTypes" : ["-*~1*"],
  "MinimumCompressionSize": 1024,

```

```

    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
}

```

AwsApiGatewayStage

AwsApiGatewayStage 物件提供第 1 版 Amazon API Gateway 階段的相關資訊。

以下是安全AwsApiGatewayStage調查結果格式 AWS (ASFF) 中的範例調查結果。若要檢視AwsApiGatewayStage屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsApiGatewayStageDetails](#)。

範例

```

"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},

```

```

    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"\${context.requestId}\", \"extendedRequestId\": \"\${context.extendedRequestId}\", \"ownerAccountId\": \"\${context.accountId}\", \"requestAccountId\": \"\${context.identity.accountId}\", \"callerPrincipal\": \"\${context.identity.caller}\", \"httpMethod\": \"\${context.httpMethod}\", \"resourcePath\": \"\${context.resourcePath}\", \"status\": \"\${context.status}\", \"requestTime\": \"\${context.requestTime}\", \"responseLatencyMs\": \"\${context.responseLatency}\", \"errorMessage\": \"\${context.error.message}\", \"errorResponseType\": \"\${context.error.responseType}\", \"apiId\": \"\${context.apiId}\", \"awsEndpointRequestId\": \"\${context.awsEndpointRequestId}\", \"domainName\": \"\${context.domainName}\", \"stage\": \"\${context.stage}\", \"xrayTraceId\": \"\${context.xrayTraceId}\", \"sourceIp\": \"\${context.identity.sourceIp}\", \"user\": \"\${context.identity.user}\", \"userAgent\": \"\${context.identity.userAgent}\", \"userArn\": \"\${context.identity.userArn}\", \"integrationLatency\": \"\${context.integrationLatency}\", \"integrationStatus\": \"\${context.integrationStatus}\", \"authorizerIntegrationLatency\": \"\${context.authorizer.integrationLatency}\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}

```

AwsApiGatewayV2Api

AwsApiGatewayV2Api 物件包含 Amazon API Gateway 中第 2 版 API 的相關資訊。

以下是安全AwsApiGatewayV2Api調查結果格式 AWS (ASFF) 中的範例調查結果。若要檢視AwsApiGatewayV2Api屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsApiGatewayV2ApiDetails](#)。

範例

```
"AwsApiGatewayV2Api": {
  "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
  "ApiId": "a1b2c3d4",
  "ApiKeySelectionExpression": "$request.header.x-api-key",
  "CreateDate": "2020-03-28T00:32:37Z",
  "Description": "ApiGatewayV2 Api",
  "Version": "string",
  "Name": "my-api",
  "ProtocolType": "HTTP",
  "RouteSelectionExpression": "$request.method $request.path",
  "CorsConfiguration": {
    "AllowOrigins": [ "*" ],
    "AllowCredentials": true,
    "ExposeHeaders": [ "string" ],
    "MaxAge": 3000,
    "AllowMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowHeaders": [ "*" ]
  }
}
```

AwsApiGatewayV2Stage

AwsApiGatewayV2Stage 包含 Amazon API Gateway 第 2 版階段的相關資訊。

以下是安全AwsApiGatewayV2Stage調查結果格式 AWS (ASFF) 中的範例調查結果。若要檢視AwsApiGatewayV2Stage屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsApiGatewayV2StageDetails](#)。

範例

```
"AwsApiGatewayV2Stage": {
  "CreateDate": "2020-04-08T00:36:05Z",
  "Description": "ApiGatewayV2",
  "DefaultRouteSettings": {
    "DetailedMetricsEnabled": false,
    "LoggingLevel": "INFO",
```

```

        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"${context.requestId}\", \"extendedRequestId\": \"${context.extendedRequestId}\", \"ownerAccountId\": \"${context.accountId}\", \"requestAccountId\": \"${context.identity.accountId}\", \"callerPrincipal\": \"${context.identity.caller}\", \"httpMethod\": \"${context.httpMethod}\", \"resourcePath\": \"${context.resourcePath}\", \"status\": \"${context.status}\", \"requestTime\": \"${context.requestTime}\", \"responseLatencyMs\": \"${context.responseLatency}\", \"errorMessage\": \"${context.error.message}\", \"errorResponseType\": \"${context.error.responseType}\", \"apiId\": \"${context.apiId}\", \"awsEndpointRequestId\": \"${context.awsEndpointRequestId}\", \"domainName\": \"${context.domainName}\", \"stage\": \"${context.stage}\", \"xrayTraceId\": \"${context.xrayTraceId}\", \"sourceIp\": \"${context.identity.sourceIp}\", \"user\": \"${context.identity.user}\", \"userAgent\": \"${context.identity.userAgent}\", \"userArn\": \"${context.identity.userArn}\", \"integrationLatency\": \"${context.integrationLatency}\", \"integrationStatus\": \"${context.integrationStatus}\", \"authorizerIntegrationLatency\": \"${context.authorizer.integrationLatency}\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}

```

AwsAppSync ASFF 中的 資源

以下是 AwsAppSync 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi 提供 AWS AppSync GraphQL API 的相關資訊，這是應用程式的頂層建構。

下列範例顯示AwsAppSyncGraphQLApi物件的 ASFF。若要檢視AwsAppSyncGraphQLApi屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsAppSyncGraphQLApi](#)。

範例

```
"AwsAppSyncGraphQLApi": {
  "AdditionalAuthenticationProviders": [
    {
      "AuthenticationType": "AWS_LAMBDA",
      "LambdaAuthorizerConfig": {
        "AuthorizerResultTtlInSeconds": 300,
        "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
      }
    },
    {
      "AuthenticationType": "AWS_IAM"
    }
  ],
  "ApiId": "021345abcdef6789",
  "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
  "AuthenticationType": "API_KEY",
  "Id": "021345abcdef6789",
  "LogConfig": {
    "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-graphqlapi-logs-eu-central-1",
    "ExcludeVerboseContent": true,
    "FieldLogLevel": "ALL"
  },
  "Name": "My AppSync App",
  "XrayEnabled": true,
}
```

AwsAthena ASFF 中的 資源

以下是 AwsAthena 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsAthenaWorkGroup

AwsAthenaWorkGroup 提供 Amazon Athena 工作群組的相關資訊。工作群組可協助您區隔使用者、團隊、應用程式或工作負載。它還可協助您設定資料處理和追蹤成本的限制。

下列範例顯示AwsAthenaWorkGroup物件的 ASFF。若要檢視AwsAthenaWorkGroup屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsAthenaWorkGroup](#)。

範例

```
"AwsAthenaWorkGroup": {
  "Description": "My workgroup for prod workloads",
  "Name": "MyWorkgroup",
  "WorkgroupConfiguration" {
    "ResultConfiguration": {
      "EncryptionConfiguration": {
        "EncryptionOption": "SSE_KMS",
        "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      }
    }
  },
  "State": "ENABLED"
}
```

AwsAutoScaling ASFF 中的 資源

以下是 AwsAutoScaling 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsAutoScalingAutoScalingGroup

AwsAutoScalingAutoScalingGroup 物件提供自動擴展群組的詳細資訊。

以下是 AWS 安全AwsAutoScalingAutoScalingGroup調查結果格式 (ASFF) 中的範例調查結果。若要檢視AwsAutoScalingAutoScalingGroup屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsAutoScalingAutoScalingGroupDetails](#)。

範例

```

"AwsAutoScalingAutoScalingGroup": {
  "CreatedTime": "2017-10-17T14:47:11Z",
  "HealthCheckGracePeriod": 300,
  "HealthCheckType": "EC2",
  "LaunchConfigurationName": "mylaunchconf",
  "LoadBalancerNames": [],
  "LaunchTemplate": {
    "LaunchTemplateId": "string",
    "LaunchTemplateName": "string",
    "Version": "string"
  },
  "MixedInstancesPolicy": {
    "InstancesDistribution": {
      "OnDemandAllocationStrategy": "prioritized",
      "OnDemandBaseCapacity": number,
      "OnDemandPercentageAboveBaseCapacity": number,
      "SpotAllocationStrategy": "lowest-price",
      "SpotInstancePools": number,
      "SpotMaxPrice": "string"
    },
    "LaunchTemplate": {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "string",
        "LaunchTemplateName": "string",
        "Version": "string"
      },
      "CapacityRebalance": true,
      "Overrides": [
        {
          "InstanceType": "string",
          "WeightedCapacity": "string"
        }
      ]
    }
  }
}

```

AwsAutoScalingLaunchConfiguration

AwsAutoScalingLaunchConfiguration 物件提供啟動組態的詳細資訊。

以下是 AWS 安全 `AwsAutoScalingLaunchConfiguration` 調查結果格式 (ASFF) 中的範例調查結果。

若要檢視 `AwsAutoScalingLaunchConfiguration` 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsAutoScalingLaunchConfigurationDetails](#)。

範例

```
AwsAutoScalingLaunchConfiguration: {
  "LaunchConfigurationName": "newtest",
  "ImageId": "ami-058a3739b02263842",
  "KeyName": "55hundredinstance",
  "SecurityGroups": [ "sg-01fce87ad6e019725" ],
  "ClassicLinkVpcSecurityGroups": [],
  "UserData": "...Base64-Encoded user data..."
  "InstanceType": "a1.metal",
  "KernelId": "",
  "RamdiskId": "ari-a51cf9cc",
  "BlockDeviceMappings": [
    {
      "DeviceName": "/dev/sdh",
      "Ebs": {
        "VolumeSize": 30,
        "VolumeType": "gp2",
        "DeleteOnTermination": false,
        "Encrypted": true,
        "SnapshotId": "snap-ffaa1e69",
        "VirtualName": "ephemeral1"
      }
    },
    {
      "DeviceName": "/dev/sdb",
      "NoDevice": true
    },
    {
      "DeviceName": "/dev/sda1",
      "Ebs": {
        "SnapshotId": "snap-02420cd3d2dea1bc0",
        "VolumeSize": 8,
        "VolumeType": "gp2",
        "DeleteOnTermination": true,
        "Encrypted": false
      }
    }
  ]
}
```

```

    },
    {
      "DeviceName": "/dev/sdi",
      "Ebs": {
        "VolumeSize": 20,
        "VolumeType": "gp2",
        "DeleteOnTermination": false,
        "Encrypted": true
      }
    },
    {
      "DeviceName": "/dev/sdc",
      "NoDevice": true
    }
  ],
  "InstanceMonitoring": {
    "Enabled": false
  },
  "CreatedTime": 1620842933453,
  "EbsOptimized": false,
  "AssociatePublicIpAddress": true,
  "SpotPrice": "0.045"
}

```

AwsBackup ASFF 中的 資源

以下是 AwsBackup 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsBackupBackupPlan

AwsBackupBackupPlan 物件提供備份計畫的相關資訊 AWS Backup。AWS Backup 備份計畫是一種政策表達式，可定義您要備份 AWS 資源的時間和方式。

下列範例顯示 AwsBackupBackupPlan 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsBackupBackupPlan屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsBackupBackupPlan](#)。

範例

```

"AwsBackupBackupPlan": {
  "BackupPlan": {

```

```

"AdvancedBackupSettings": [{
  "BackupOptions": {
    "WindowsVSS": "enabled"
  },
  "ResourceType": "EC2"
}],
"BackupPlanName": "test",
"BackupPlanRule": [{
  "CompletionWindowMinutes": 10080,
  "CopyActions": [{
    "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
    "Lifecycle": {
      "DeleteAfterDays": 365,
      "MoveToColdStorageAfterDays": 30
    }
  }],
  "Lifecycle": {
    "DeleteAfterDays": 35
  },
  "RuleName": "DailyBackups",
  "ScheduleExpression": "cron(0 5 ? * * *)",
  "StartWindowMinutes": 480,
  "TargetBackupVault": "Default"
},
{
  "CompletionWindowMinutes": 10080,
  "CopyActions": [{
    "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
    "Lifecycle": {
      "DeleteAfterDays": 365,
      "MoveToColdStorageAfterDays": 30
    }
  }],
  "Lifecycle": {
    "DeleteAfterDays": 35
  },
  "RuleName": "Monthly",
  "ScheduleExpression": "cron(0 5 1 * ? *)",
  "StartWindowMinutes": 480,
  "TargetBackupVault": "Default"
}]
},

```

```

    "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
  }

```

AwsBackupBackupVault

AwsBackupBackupVault 物件提供備份保存庫的相關資訊 AWS Backup。AWS Backup 備份文件庫是存放和組織備份的容器。

下列範例顯示 AwsBackupBackupVault 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsBackupBackupVault屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsBackupBackupVault](#)。

範例

```

"AwsBackupBackupVault": {
  "AccessPolicy": {
    "Statement": [{
      "Action": [
        "backup:DeleteBackupVault",
        "backup:DeleteBackupVaultAccessPolicy",
        "backup:DeleteRecoveryPoint",
        "backup:StartCopyJob",
        "backup:StartRestoreJob",
        "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
        "AWS": "*"
      },
      "Resource": "*"
    }],
    "Version": "2012-10-17"
  },
  "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
  "BackupVaultName": "aws/efs/automatic-backup-vault",
  "EncryptionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
  "Notifications": {

```

```

    "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
"COPY_JOB_STARTED"],
    "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
  }
}

```

AwsBackupRecoveryPoint

AwsBackupRecoveryPoint 物件提供備份的相關資訊 AWS Backup，也稱為復原點。AWS Backup 復原點代表資源在指定時間的內容。

下列範例顯示 AwsBackupRecoveryPoint 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsBackupBackupVault屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsBackupRecoveryPoint](#)。

範例

```

"AwsBackupRecoveryPoint": {
  "BackupSizeInBytes": 0,
  "BackupVaultName": "aws/efs/automatic-backup-vault",
  "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/automatic-backup-vault",
  "CalculatedLifecycle": {
    "DeleteAt": "2021-08-30T06:51:58.271Z",
    "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
  },
  "CompletionDate": "2021-07-26T07:21:40.361Z",
  "CreatedBy": {
    "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
    "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
    "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
    "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
  },
  "CreationDate": "2021-07-26T06:51:58.271Z",
  "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-ba38-838bf8d06ca0",
  "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup",
  "IsEncrypted": true,
  "LastRestoreTime": "2021-07-26T06:51:58.271Z",
  "Lifecycle": {
    "DeleteAfterDays": 35,

```

```

    "MoveToColdStorageAfterDays": 15
  },
  "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-f1d5-4587-a7fd-0774c6e91268",
  "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/fs-15bd31a1",
  "ResourceType": "EFS",
  "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/automatic-backup-vault",
  "Status": "COMPLETED",
  "StatusMessage": "Failure message",
  "StorageClass": "WARM"
}

```

AwsCertificateManager ASFF 中的 資源

以下是 AwsCertificateManager 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsCertificateManagerCertificate

AwsCertificateManagerCertificate 物件提供 AWS Certificate Manager (ACM) 憑證的詳細資訊。

以下是 AWS 安全AwsCertificateManagerCertificate調查結果格式 (ASFF) 中的範例調查結果。若要檢視AwsCertificateManagerCertificate屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsCertificateManagerCertificateDetails](#)。

範例

```

"AwsCertificateManagerCertificate": {
  "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-authority/example",
  "CreatedAt": "2019-05-24T18:12:02.000Z",
  "DomainName": "example.amazondomains.com",
  "DomainValidationOptions": [
    {
      "DomainName": "example.amazondomains.com",
      "ResourceRecord": {
        "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
        "Type": "CNAME",
        "Value": "_example.acm-validations.aws."
      }
    }
  ]
}

```



```

    },
    "ValidationDomain": "example.amazondomains.com",
    "ValidationEmails": [sample_email@sample.com],
    "ValidationMethod": "DNS",
    "ValidationStatus": "SUCCESS"
  }
],
"ExtendedKeyUsages": [
  {
    "Name": "TLS_WEB_SERVER_AUTHENTICATION",
    "Oid": "1.3.6.1.5.5.7.3.1"
  },
  {
    "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
    "Oid": "1.3.6.1.5.5.7.3.2"
  }
],
"FailureReason": "",
"ImportedAt": "2018-08-17T00:13:00.000Z",
"InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
"IssuedAt": "2020-04-26T00:41:17.000Z",
"Issuer": "Amazon",
"KeyAlgorithm": "RSA-1024",
"KeyUsages": [
  {
    "Name": "DIGITAL_SIGNATURE",
  },
  {
    "Name": "KEY_ENCIPHERMENT",
  }
],
"NotAfter": "2021-05-26T12:00:00.000Z",
"NotBefore": "2020-04-26T00:00:00.000Z",
"Options": {
  "CertificateTransparencyLoggingPreference": "ENABLED",
}
"RenewalEligibility": "ELIGIBLE",
"RenewalSummary": {
  "DomainValidationOptions": [
    {
      "DomainName": "example.amazondomains.com",
      "ResourceRecord": {
        "Name":
"_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",

```

```

        "Type": "CNAME",
        "Value": "_example.acm-validations.aws.com",
    },
    "ValidationDomain": "example.amazondomains.com",
    "ValidationEmails": ["sample_email@sample.com"],
    "ValidationMethod": "DNS",
    "ValidationStatus": "SUCCESS"
  }
],
"RenewalStatus": "SUCCESS",
"RenewalStatusReason": "",
"UpdatedAt": "2020-04-26T00:41:35.000Z",
},
"Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
"SignatureAlgorithm": "SHA256WITHRSA",
"Status": "ISSUED",
"Subject": "CN=example.amazondomains.com",
"SubjectAlternativeNames": ["example.amazondomains.com"],
"Type": "AMAZON_ISSUED"
}

```

AwsCloudFormation ASFF 中的 資源

以下是 AwsCloudFormation 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsCloudFormationStack

AwsCloudFormationStack 物件提供有關巢狀為最上層範本中資源之堆疊的詳細資訊 AWS CloudFormation。

下列範例顯示 AwsCloudFormationStack 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsCloudFormationStack屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsCloudFormationStackDetails](#)。

範例

```

"AwsCloudFormationStack": {
  "Capabilities": [
    "CAPABILITY_IAM",
    "CAPABILITY_NAMED_IAM"
  ],

```

```

"CreationTime": "2022-02-18T15:31:53.161Z",
"Description": "AWS CloudFormation Sample",
"DisableRollback": true,
"DriftInformation": {
  "StackDriftStatus": "DRIFTED"
},
"EnableTerminationProtection": false,
"LastUpdatedTime": "2022-02-18T15:31:53.161Z",
"NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
],
"Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
}],
"RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
"StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
"StackName": "sample-stack",
"StackStatus": "CREATE_COMPLETE",
"StackStatusReason": "Success",
"TimeoutInMinutes": 1
}

```

AwsCloudFront ASFF 中的 資源

以下是 AwsCloudFront 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsCloudFrontDistribution

AwsCloudFrontDistribution 物件提供 Amazon CloudFront 分佈組態的詳細資訊。

以下是 AWS 安全 AwsCloudFrontDistribution 調查結果格式 (ASFF) 中的範例調查結果。若要檢視 AwsCloudFrontDistribution 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsCloudFrontDistributionDetails](#)。

範例

```

"AwsCloudFrontDistribution": {
  "CacheBehaviors": {

```

```
    "Items": [
      {
        "ViewerProtocolPolicy": "https-only"
      }
    ],
  },
  "DefaultCacheBehavior": {
    "ViewerProtocolPolicy": "https-only"
  },
  "DefaultRootObject": "index.html",
  "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
  "Etag": "E37H0T42DHPVYH",
  "LastModifiedTime": "2015-08-31T21:11:29.093Z",
  "Logging": {
    "Bucket": "myawslogbucket.s3.amazonaws.com",
    "Enabled": false,
    "IncludeCookies": false,
    "Prefix": "myawslog/"
  },
  "OriginGroups": {
    "Items": [
      {
        "FailoverCriteria": {
          "StatusCodes": {
            "Items": [
              200,
              301,
              404
            ]
          },
          "Quantity": 3
        }
      }
    ]
  },
  "Origins": {
    "Items": [
      {
        "CustomOriginConfig": {
          "HttpPort": 80,
          "HttpsPort": 443,
          "OriginKeepaliveTimeout": 60,
          "OriginProtocolPolicy": "match-viewer",
          "OriginReadTimeout": 30,
```

```

        "OriginSslProtocols": {
            "Items": ["SSLv3", "TLSv1"],
            "Quantity": 2
        }
    },
    ],
},
    ],
    "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
    "Id": "my-origin",
    "OriginPath": "/production",
    "S3OriginConfig": {
        "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
    }
    ],
},
    "Status": "Deployed",
    "ViewerCertificate": {
        "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
        "Certificate": "ASCAJRRE5XYF52TKRY5M4",
        "CertificateSource": "iam",
        "CloudFrontDefaultCertificate": true,
        "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
        "MinimumProtocolVersion": "TLSv1.2_2021",
        "SslSupportMethod": "sni-only"
    },
    "WebAclId": "waf-1234567890"
}

```

AwsCloudTrail ASFF 中的 資源

以下是 AwsCloudTrail 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsCloudTrailTrail

AwsCloudTrailTrail 物件提供線索的詳細資訊 AWS CloudTrail 。

以下是安全AwsCloudTrailTrail調查結果格式 AWS (ASFF) 中的範例調查結果。若要檢視AwsCloudTrailTrail屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsCloudTrailTrailDetails](#)。

範例

```
"AwsCloudTrailTrail": {
  "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
  "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
  "HasCustomEventSelectors": true,
  "HomeRegion": "us-west-2",
  "IncludeGlobalServiceEvents": true,
  "IsMultiRegionTrail": true,
  "IsOrganizationTrail": false,
  "KmsKeyId": "kmsKeyId",
  "LogFileValidationEnabled": true,
  "Name": "regression-trail",
  "S3BucketName": "cloudtrail-bucket",
  "S3KeyPrefix": "s3KeyPrefix",
  "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
  "SnsTopicName": "snsTopicName",
  "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

AwsCloudWatch ASFF 中的 資源

以下是 AwsCloudWatch 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsCloudWatchAlarm

AwsCloudWatchAlarm 物件提供 Amazon CloudWatch 警示的詳細資訊，可在警示變更狀態時監看指標或執行動作。

下列範例顯示 AwsCloudWatchAlarm 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsCloudWatchAlarm 屬性的說明，請參閱 AWS Security Hub API 參考中的 [AwsCloudWatchAlarmDetails](#)。

範例

```
"AwsCloudWatchAlarm": {
  "ActionsEnabled": true,
```

```

"AlarmActions": [
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
],
"AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
"AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
"AlarmDescription": "Alarm Example",
"AlarmName": "Example",
"ComparisonOperator": "GreaterThanOrEqualToThreshold",
"DatapointsToAlarm": 1,
"Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
}],
"EvaluateLowSampleCountPercentile": "evaluate",
"EvaluationPeriods": 1,
"ExtendedStatistic": "p99.9",
"InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
],
"MetricName": "Sample Metric",
"Namespace": "YourNamespace",
"OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
],
"Period": 1,
"Statistic": "SampleCount",
"Threshold": 12.3,
"ThresholdMetricId": "t1",
"TreatMissingData": "notBreaching",
"Unit": "Kilobytes/Second"
}

```

AwsCodeBuild ASFF 中的 資源

以下是 AwsCodeBuild 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsCodeBuildProject

AwsCodeBuildProject 物件提供了 AWS CodeBuild 專案的資訊。

以下是安全AwsCodeBuildProject調查結果格式 AWS (ASFF) 中的範例調查結果。若要檢視AwsCodeBuildProject屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsCodeBuildProjectDetails](#)。

範例

```
"AwsCodeBuildProject": {
  "Artifacts": [
    {
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "OverrideArtifactName": boolean,
      "Packaging": "string",
      "Path": "string",
      "Type": "string"
    }
  ],
  "SecondaryArtifacts": [
    {
      "ArtifactIdentifier": "string",
      "EncryptionDisabled": boolean,
      "Location": "string",
      "Name": "string",
      "NamespaceType": "string",
      "OverrideArtifactName": boolean,
      "Packaging": "string",
      "Path": "string",
      "Type": "string"
    }
  ],
  "EncryptionKey": "string",
  "Certificate": "string",
  "Environment": {
    "Certificate": "string",
    "EnvironmentVariables": [
      {
        "Name": "string",
        "Type": "string",
        "Value": "string"
      }
    ]
  }
}
```



```

    ],
    "ImagePullCredentialsType": "string",
    "PrivilegedMode": boolean,
    "RegistryCredential": {
        "Credential": "string",
        "CredentialProvider": "string"
    },
    "Type": "string"
},
"LogsConfig": {
    "CloudWatchLogs": {
        "GroupName": "string",
        "Status": "string",
        "StreamName": "string"
    },
    "S3Logs": {
        "EncryptionDisabled": boolean,
        "Location": "string",
        "Status": "string"
    }
},
"Name": "string",
"ServiceRole": "string",
"Source": {
    "Type": "string",
    "Location": "string",
    "GitCloneDepth": integer
},
"VpcConfig": {
    "VpcId": "string",
    "Subnets": ["string"],
    "SecurityGroupIds": ["string"]
}
}

```

AwsDms ASFF 中的 資源

以下是 AwsDms 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsDmsEndpoint

AwsDmsEndpoint 物件提供有關 AWS Database Migration Service (AWS DMS) 端點的資訊。端點提供資料存放區的連線、資料存放區類型和位置資訊。

下列範例顯示 AwsDmsEndpoint 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsDmsEndpoint屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsDmsEndpointDetails](#)。

範例

```
"AwsDmsEndpoint": {
  "CertificateArn": "arn:aws:dms:us-east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
  "DatabaseName": "Test",
  "EndpointArn": "arn:aws:dms:us-east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJBPNPK6MJQVFVQA",
  "EndpointIdentifier": "target-db",
  "EndpointType": "TARGET",
  "EngineName": "mariadb",
  "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Port": 3306,
  "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
  "SslMode": "verify-ca",
  "Username": "admin"
}
```

AwsDmsReplicationInstance

AwsDmsReplicationInstance 物件提供有關 AWS Database Migration Service (AWS DMS) 複寫執行個體的資訊。DMS 使用複寫執行個體來連線至來源資料存放區、讀取來源資料，以及格式化資料以供目標資料存放區使用。

下列範例顯示 AwsDmsReplicationInstance 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsDmsReplicationInstance屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsDmsReplicationInstanceDetails](#)。

範例

```
"AwsDmsReplicationInstance": {
  "AllocatedStorage": 50,
  "AutoMinorVersionUpgrade": true,
```

```

    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}

```

AwsDmsReplicationTask

AwsDmsReplicationTask 物件提供有關 AWS Database Migration Service (AWS DMS) 複製任務的資訊。複製任務會將一組資料從來源端點移至目標端點。

下列範例顯示 **AwsDmsReplicationInstance** 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 **AwsDmsReplicationInstance** 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsDmsReplicationInstance](#)。

範例

```

"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-east-1:123456789012:task:YDYU0HZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4Y0UGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
    "ReplicationTaskSettings": "{\\"Logging\\":{\\"EnableLogging\\":false,\\"EnableLogContext\\":false,\\"LogComponents\\":[\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"TRANSFORMATION\\"],\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"SOURCE_UNLOAD\\"],\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"IO\\"],\\"Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",\\"Id\\":\\"TARGET_LOAD\\"},

```

```
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"PERFORMANCE\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"SOURCE_CAPTURE\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"SORTER\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"REST_SERVER\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"VALIDATOR_EXT\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"TARGET_APPLY\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"TASK_MANAGER\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"TABLES_MANAGER\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"METADATA_MANAGER\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"FILE_FACTORY\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"COMMON\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"ADDONS\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"DATA_STRUCTURE\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"COMMUNICATION\\"},
{
  "Severity\\":\\"LOGGER_SEVERITY_DEFAULT\\",
  "Id\\":\\"FILE_TRANSFER\\"}],
"CloudWatchLogGroup\\":null,
"CloudWatchLogStream\\":null,
"StreamBufferSettings\\":{
  "StreamBufferCount\\":3,
  "CtrlStreamBufferSizeInMB\\":5,
  "StreamBufferSizeInMB\\":8},
"ErrorBehavior\\":{
  "FailOnNoTablesCaptured\\":true,
  "ApplyErrorUpdatePolicy\\":\\"LOG_ERROR\\",
  "FailOnTransactionConsistencyBreached\\":false,
  "RecoverableErrorThrottlingMax\\":1800,
  "DataErrorEscalationPolicy\\":\\"SUSPEND_TABLE\\",
  "ApplyErrorEscalationCount\\":0,
  "RecoverableErrorStopRetryAfterThrottlingMax\\":true,
  "RecoverableErrorThrottling\\":true,
  "ApplyErrorFailOnTruncationDdl\\":false,
  "DataTruncationErrorPolicy\\":\\"LOG_ERROR\\",
  "ApplyErrorInsertPolicy\\":\\"LOG_ERROR\\",
  "EventErrorPolicy\\":\\"IGNORE\\",
  "ApplyErrorEscalationPolicy\\":\\"LOG_ERROR\\",
  "RecoverableErrorCount\\":-1,
  "DataErrorEscalationCount\\":0,
  "TableErrorEscalationPolicy\\":\\"STOP_TASK\\",
  "RecoverableErrorInterval\\":5,
  "ApplyErrorDeletePolicy\\":\\"IGNORE_RECORD\\",
  "TableErrorEscalationCount\\":0,
  "FullLoadIgnoreConflicts\\":true,
  "DataErrorPolicy\\":\\"LOG_ERROR\\",
  "TableErrorPolicy\\":\\"SUSPEND_TABLE\\"},
"TTSettings\\":{
  "TTS3Settings\\":null,
  "TTRecordSettings\\":null,
  "EnableTT\\":false},
"FullLoadSettings\\":{
  "CommitRate\\":10000,
  "StopTaskCachedChangesApplied\\":false,
  "StopTaskCachedChangesNotApplied\\":false,
  "MaxFullLoadSubTasks\\":8,
  "TransactionConsistencyTimeout\\":600,
  "CreatePkAfterFullLoad\\":false,
  "TargetTablePrepMode\\":\\"DO_NOTHING\\"},
"TargetMetadata\\":{
  "ParallelApplyBufferSize\\":0,
  "ParallelApplyQueuesPerThread\\":0,
  "ParallelApplyThreads\\":0,
  "TargetSchema\\":\\"\\",
  "InlineLobMaxSize\\":0,
  "ParallelLoadQueuesPerThread\\":0,
  "SupportLobs\\":true,
  "LobChunkSize\\":64,
  "TaskRecoveryTableEnabled\\":false,
  "ParallelLoadThreads\\":0,
  "LobMaxSize\\":0,
  "BatchApplyEnabled\\":false,
  "FullLobMode\\":true,
  "LimitedSizeLobMode\\":false,
  "LoadMaxFileSize\\":0,
  "ParallelLoadBufferSize\\":0},
"BeforeImageSettings\\":null,
"ControlTablesSettings\\":{
  "historyTimeslotInMinutes\\":5,
  "HistoryTimeslotInMinutes\\":5,
  "StatusTableEnabled\\":false,
  "SuspendedTablesTableEnabled\\":false,
  "HistoryTableEnabled\\":false,
  "ControlSchema\\":\\"\\",
  "FullLoadExceptionTableEnabled\\":false},
"LoopbackPreventionSettings\\":null,
"CharacterSetSettings\\":null,
"FailTaskWhenCleanTaskResourceFailed\\":false,
"ChangeProcessingTuning\\":{
  "StatementCacheSize\\":50,
  "CommitTimeout\\":1,
  "BatchApplyPreserveTransaction\\":true,
  "BatchApplyTimeoutMin\\":1,
  "BatchSplitSize\\":0,
  "BatchApplyTimeoutMax\\":30,
  "MinTransactionSize\\":1000,
```

```
\ "MemoryKeepTime\" : 60, \ "BatchApplyMemoryLimit\" : 500, \ "MemoryLimitTotal\" : 1024},
\ "ChangeProcessingDdlHandlingPolicy\" : { \ "HandleSourceTableDropped\" : true,
\ "HandleSourceTableTruncated\" : true, \ "HandleSourceTableAltered\" : true},
\ "PostProcessingRules\" : null}],
  \ "SourceEndpointArn\" : \"arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHY0KVCRNHAKJ4Q3RUXACNGFGYWRI\",
  \ "TableMappings\" : \"[{ \ "rules\" : [{ \ "rule-type\" : \ "selection\", \ "rule-id\" :
\ "969761702\", \ "rule-name\" : \ "969761702\", \ "object-locator\" : { \ "schema-name\" : \ \"%table
\", \ "table-name\" : \ \"%example\" }, \ "rule-action\" : \ "exclude\", \ "filters\" : [] } ] } ]\",
  \ "TargetEndpointArn\" : \"arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LB0QB3CZY33F7XV253NAJVBPNK6MJQVVFVQA\"
}
```

AwsDynamoDB ASFF 中的 資源

以下是 AwsDynamoDB 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsDynamoDbTable

AwsDynamoDbTable 物件提供 Amazon DynamoDB 資料表的詳細資訊。

以下是安全AwsDynamoDbTable調查結果格式 (ASFF) 中 AWS 的範例調查結果。若要檢視AwsDynamoDbTable屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsDynamoDbTableDetails](#)。

範例

```
"AwsDynamoDbTable": {
  "AttributeDefinitions": [
    {
      "AttributeName": "attribute1",
      "AttributeType": "value 1"
    },
    {
      "AttributeName": "attribute2",
      "AttributeType": "value 2"
    },
    {
      "AttributeName": "attribute3",
      "AttributeType": "value 3"
    }
  ]
}
```

```

    ],
    "BillingModeSummary": {
      "BillingMode": "PAY_PER_REQUEST",
      "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
    },
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
      {
        "Backfilling": false,
        "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
        "IndexName": "standardsControlArnIndex",
        "IndexSizeBytes": 1862513,
        "IndexStatus": "ACTIVE",
        "ItemCount": 20,
        "KeySchema": [
          {
            "AttributeName": "City",
            "KeyType": "HASH"
          },
          {
            "AttributeName": "Date",
            "KeyType": "RANGE"
          }
        ],
        "Projection": {
          "NonKeyAttributes": ["predictorName"],
          "ProjectionType": "ALL"
        },
        "ProvisionedThroughput": {
          "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
          "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
          "NumberOfDecreasesToday": 0,
          "ReadCapacityUnits": 100,
          "WriteCapacityUnits": 50
        }
      },
    ],
    "GlobalTableVersion": "V1",
    "ItemCount": 2705,
    "KeySchema": [
      {
        "AttributeName": "zipcode",

```

```

        "KeyType": "HASH"
    }
],
    "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
    "LatestStreamLabel": "2019-12-03T23:23:10.248",
    "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes": [
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
        }
    ],

```

```

        "RegionName": "regionName",
        "ReplicaStatus": "CREATING",
        "ReplicaStatusDescription": "replicaStatusDescription"
    }
],
"RestoreSummary" : {
    "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/backup/backup1",
    "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
    "RestoreDateTime": "2020-06-22T17:40:12.322Z",
    "RestoreInProgress": true
},
"SseDescription": {
    "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
    "Status": "ENABLED",
    "SseType": "KMS",
    "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
},
"StreamSpecification" : {
    "StreamEnabled": true,
    "StreamViewType": "NEW_IMAGE"
},
"TableId": "example-table-id-1",
"TableName": "example-table",
"TableSizeBytes": 1862513,
"TableStatus": "ACTIVE"
}

```

AwsEc2 ASFF 中的 資源

以下是 AwsEc2 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsEc2ClientVpnEndpoint

AwsEc2ClientVpnEndpoint 物件提供 AWS Client VPN 端點的相關資訊。Client VPN 端點是您建立和設定以啟用和管理用戶端 VPN 工作階段的資源。它是所有用戶端 VPN 工作階段的終止點。

下列範例顯示 AwsEc2ClientVpnEndpoint 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsEc2ClientVpnEndpoint 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2ClientVpnEndpointDetails](#)。

範例

```
"AwsEc2ClientVpnEndpoint": {
  "AuthenticationOptions": [
    {
      "MutualAuthentication": {
        "ClientRootCertificateChainArn": "arn:aws:acm:us-east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "Type": "certificate-authentication"
    }
  ],
  "ClientCidrBlock": "10.0.0.0/22",
  "ClientConnectOptions": {
    "Enabled": false
  },
  "ClientLoginBannerOptions": {
    "Enabled": false
  },
  "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
  "ConnectionLogOptions": {
    "Enabled": false
  },
  "Description": "test",
  "DnsServer": ["10.0.0.0"],
  "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "SecurityGroupIdSet": [
    "sg-0f7a177b82b443691"
  ],
  "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/cvpn-endpoint-00c5d11fc4729f2a5",
  "SessionTimeoutHours": 24,
  "SplitTunnel": false,
  "TransportProtocol": "udp",
  "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
  "VpnPort": 443
}
```

AwsEc2Eip

AwsEc2Eip 物件提供彈性 IP 地址的相關資訊。

下列範例顯示 AwsEc2Eip 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEc2Eip屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2EipDetails](#)。

範例

```
"AwsEc2Eip": {
  "InstanceId": "instance1",
  "PublicIp": "192.0.2.04",
  "AllocationId": "eipalloc-example-id-1",
  "AssociationId": "eipassoc-example-id-1",
  "Domain": "vpc",
  "PublicIpv4Pool": "anycompany",
  "NetworkBorderGroup": "eu-central-1",
  "NetworkInterfaceId": "eni-example-id-1",
  "NetworkInterfaceOwnerId": "777788889999",
  "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

AwsEc2Instance 物件提供 Amazon EC2 執行個體的詳細資訊。

下列範例顯示 AwsEc2Instance 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEc2Instance屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2InstanceDetails](#)。

範例

```
"AwsEc2Instance": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
  "ImageId": "ami-1234",
  "IPv4Addresses": [ "1.1.1.1" ],
  "IPv6Addresses": [ "2001:db8:1234:1a2b::123" ],
  "KeyName": "my_keypair",
  "LaunchedAt": "2018-05-08T16:46:19.000Z",
  "MetadataOptions": {
    "HttpEndpoint": "enabled",
    "HttpProtocolIpv6": "enabled",
    "HttpPutResponseHopLimit": 1,
    "HttpTokens": "optional",
    "InstanceMetadataTags": "disabled",
  },
  "Monitoring": {
```

```
    "State": "disabled"
  },
  "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
  ],
  "SubnetId": "subnet-123",
  "Type": "i3.xlarge",
  "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

AwsEc2LaunchTemplate 物件包含指定執行個體組態資訊的 Amazon Elastic Compute Cloud 啟動範本詳細資訊。

下列範例顯示 AwsEc2LaunchTemplate 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEc2LaunchTemplate屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2LaunchTemplateDetails](#)。

範例

```
"AwsEc2LaunchTemplate": {
  "DefaultVersionNumber": "1",
  "ElasticGpuSpecifications": ["string"],
  "ElasticInferenceAccelerators": ["string"],
  "Id": "lt-0a16e9802800bdd85",
  "ImageId": "ami-0d5eff06f840b45e9",
  "LatestVersionNumber": "1",
  "LaunchTemplateData": {
    "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
        "DeleteonTermination": true,
        "Encrypted": true,
        "SnapshotId": "snap-01047646ec075f543",
        "VolumeSize": 8,
        "VolumeType": "gp2"
      }
    }
  ],
  "MetadataOptions": {
    "HttpTokens": "enabled",
```

```

    "HttpPutResponseHopLimit" : 1
  },
  "Monitoring": {
    "Enabled": true,
    "NetworkInterfaces": [{
      "AssociatePublicIpAddress" : true,
    }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
  }
}

```

AwsEc2NetworkAcl

AwsEc2NetworkAcl 物件包含 Amazon EC2 網路存取控制清單 (ACL) 的詳細資訊。

下列範例顯示 AwsEc2NetworkAcl 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEc2NetworkAcl屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2NetworkAclDetails](#)。

範例

```

"AwsEc2NetworkAcl": {
  "IsDefault": false,
  "NetworkAclId": "acl-1234567890abcdef0",
  "OwnerId": "123456789012",
  "VpcId": "vpc-1234abcd",
  "Associations": [{
    "NetworkAclAssociationId": "aclassoc-abcd1234",
    "NetworkAclId": "acl-021345abcdef6789",
    "SubnetId": "subnet-abcd1234"
  }],
  "Entries": [{
    "CidrBlock": "10.24.34.0/23",
    "Egress": true,
    "IcmpTypeCode": {
      "Code": 10,
      "Type": 30
    },
    "Ipv6CidrBlock": "2001:DB8::/32",
    "PortRange": {

```

```

        "From": 20,
        "To": 40
    },
    "Protocol": "tcp",
    "RuleAction": "allow",
    "RuleNumber": 100
  ]
}
```

AwsEc2NetworkInterface

AwsEc2NetworkInterface 物件提供有關 Amazon EC2 網路介面的資訊。

下列範例顯示 AwsEc2NetworkInterface 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEc2NetworkInterface屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2NetworkInterfaceDetails](#)。

範例

```

"AwsEc2NetworkInterface": {
  "Attachment": {
    "AttachTime": "2019-01-01T03:03:21Z",
    "AttachmentId": "eni-attach-43348162",
    "DeleteOnTermination": true,
    "DeviceIndex": 123,
    "InstanceId": "i-1234567890abcdef0",
    "InstanceOwnerId": "123456789012",
    "Status": 'ATTACHED'
  },
  "SecurityGroups": [
    {
      "GroupName": "my-security-group",
      "GroupId": "sg-903004f8"
    },
  ],
  "NetworkInterfaceId": 'eni-686ea200',
  "SourceDestCheck": false
}
```

AwsEc2RouteTable

AwsEc2RouteTable 物件提供有關 Amazon EC2 路由表的資訊。

下列範例顯示 `AwsEc2RouteTable` 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 `AwsEc2RouteTable` 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2RouteTableDetails](#)。

範例

```
"AwsEc2RouteTable": {
  "AssociationSet": [{
    "AssociationSet": {
      "State": "associated"
    },
    "Main": true,
    "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
    "RouteTableId": "rtb-0a59bde9cf2548e34",
  }],
  "PropagatingVgwSet": [],
  "RouteTableId": "rtb-0a59bde9cf2548e34",
  "RouteSet": [
    {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
    },
    {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
    }
  ],
  "VpcId": "vpc-0c250a5c33f51d456"
}
```

AwsEc2SecurityGroup

`AwsEc2SecurityGroup` 物件描述 Amazon EC2 安全群組。

下列範例顯示 `AwsEc2SecurityGroup` 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 `AwsEc2SecurityGroup` 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2SecurityGroupDetails](#)。

範例

```

"AwsEc2SecurityGroup": {
  "GroupName": "MySecurityGroup",
  "GroupId": "sg-903004f8",
  "OwnerId": "123456789012",
  "VpcId": "vpc-1a2b3c4d",
  "IpPermissions": [
    {
      "IpProtocol": "-1",
      "IpRanges": [],
      "UserIdGroupPairs": [
        {
          "UserId": "123456789012",
          "GroupId": "sg-903004f8"
        }
      ],
      "PrefixListIds": [
        {"PrefixListId": "pl-63a5400a"}
      ]
    },
    {
      "PrefixListIds": [],
      "FromPort": 22,
      "IpRanges": [
        {
          "CidrIp": "203.0.113.0/24"
        }
      ],
      "ToPort": 22,
      "IpProtocol": "tcp",
      "UserIdGroupPairs": []
    }
  ]
}

```

AwsEc2Subnet

AwsEc2Subnet 物件提供 Amazon EC2 中子網路的相關資訊。

下列範例顯示 AwsEc2Subnet 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEc2Subnet屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2SubnetDetails](#)。

範例

```

AwsEc2Subnet: {
  "AssignIpv6AddressOnCreation": false,
  "AvailabilityZone": "us-west-2c",
  "AvailabilityZoneId": "usw2-az3",
  "AvailableIpAddressCount": 8185,
  "CidrBlock": "10.0.0.0/24",
  "DefaultForAz": false,
  "MapPublicIpOnLaunch": false,
  "OwnerId": "123456789012",
  "State": "available",
  "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
  "SubnetId": "subnet-d5436c93",
  "VpcId": "vpc-153ade70",
  "Ipv6CidrBlockAssociationSet": [{
    "AssociationId": "subnet-cidr-assoc-EXAMPLE",
    "Ipv6CidrBlock": "2001:DB8::/32",
    "CidrBlockState": "associated"
  }]
}

```

AwsEc2TransitGateway

AwsEc2TransitGateway 物件提供 Amazon EC2 傳輸閘道的詳細資訊，可互連您的虛擬私有雲端 (VPCs) 和內部部署網路。

以下是 AWS 安全AwsEc2TransitGateway調查結果格式 (ASFF) 中的範例調查結果。若要檢視AwsEc2TransitGateway屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2TransitGatewayDetails](#)。

範例

```

"AwsEc2TransitGateway": {
  "AmazonSideAsn": 65000,
  "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
  "AutoAcceptSharedAttachments": "disable",
  "DefaultRouteTableAssociation": "enable",
  "DefaultRouteTablePropagation": "enable",
  "Description": "sample transit gateway",
  "DnsSupport": "enable",
  "Id": "tgw-042ae6bf7a5c126c3",
  "MulticastSupport": "disable",
  "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
  "TransitGatewayCidrBlocks": ["10.0.0.0/16"],

```



```
"VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

AwsEc2Volume 物件提供 Amazon EC2 磁碟區的詳細資訊。

下列範例顯示 AwsEc2Volume 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEc2Volume屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2VolumeDetails](#)。

範例

```
"AwsEc2Volume": {
  "Attachments": [
    {
      "AttachTime": "2017-10-17T14:47:11Z",
      "DeleteOnTermination": true,
      "InstanceId": "i-123abc456def789g",
      "Status": "attached"
    }
  ],
  "CreateTime": "2020-02-24T15:54:30Z",
  "Encrypted": true,
  "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJa1rXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
  "Size": 80,
  "SnapshotId": "",
  "Status": "available"
}
```

AwsEc2Vpc

AwsEc2Vpc 物件提供 Amazon EC2 VPC 的詳細資訊。

下列範例顯示 AwsEc2Vpc 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEc2Vpc屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2VpcDetails](#)。

範例

```
"AwsEc2Vpc": {
  "CidrBlockAssociationSet": [
    {
      "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",

```

```

        "CidrBlock": "192.0.2.0/24",
        "CidrBlockState": "associated"
    }
],
"DhcpOptionsId": "dopt-4e42ce28",
"Ipv6CidrBlockAssociationSet": [
    {
        "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
        "CidrBlockState": "associated",
        "Ipv6CidrBlock": "192.0.2.0/24"
    }
],
"State": "available"
}

```

AwsEc2VpcEndpointService

AwsEc2VpcEndpointService 物件包含 VPC 端點服務的服務組態詳細資訊。

下列範例顯示 AwsEc2VpcEndpointService 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEc2VpcEndpointService屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2VpcEndpointServiceDetails](#)。

範例

```

"AwsEc2VpcEndpointService": {
    "ServiceType": [
        {
            "ServiceType": "Interface"
        }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
        "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
        "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-load-balancer/example1"
    ]
}

```

```
],
"GatewayLoadBalancerArns": [],
"BaseEndpointDnsNames": [
  "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
],
"PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

AwsEc2VpcPeeringConnection 物件提供兩個 VPCs之間網路連線的詳細資訊。

下列範例顯示 AwsEc2VpcPeeringConnection 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEc2VpcPeeringConnection屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEc2VpcPeeringConnectionDetails](#)。

範例

```
"AwsEc2VpcPeeringConnection": {
  "AcceptorVpcInfo": {
    "CidrBlock": "10.0.0.0/28",
    "CidrBlockSet": [{
      "CidrBlock": "10.0.0.0/28"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
    }],
    "OwnerId": "012345678910",
    "PeeringOptions": {
      "AllowDnsResolutionFromRemoteVpc": true,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
      "AllowEgressFromLocalVpcToRemoteClassicLink": true
    },
    "Region": "us-west-2",
    "VpcId": "vpc-i123456"
  },
  "ExpirationTime": "2022-02-18T15:31:53.161Z",
  "RequesterVpcInfo": {
    "CidrBlock": "192.168.0.0/28",
    "CidrBlockSet": [{
      "CidrBlock": "192.168.0.0/28"
    }],
    "Ipv6CidrBlockSet": [{
```

```

    "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
  "OwnerId": "012345678910",
  "PeeringOptions": {
    "AllowDnsResolutionFromRemoteVpc": true,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
    "AllowEgressFromLocalVpcToRemoteClassicLink": true
  },
  "Region": "us-west-2",
  "VpcId": "vpc-i123456"
},
"Status": {
  "Code": "initiating-request",
  "Message": "Active"
},
"VpcPeeringConnectionId": "pcx-1a2b3c4d"
}

```

AwsEcr ASFF 中的 資源

以下是 AwsEcr 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsEcrContainerImage

AwsEcrContainerImage 物件提供 Amazon ECR 映像的相關資訊。

下列範例顯示 AwsEcrContainerImage 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEcrContainerImage屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEcrContainerImageDetails](#)。

範例

```

"AwsEcrContainerImage": {
  "RegistryId": "123456789012",
  "RepositoryName": "repository-name",
  "Architecture": "amd64"
  "ImageDigest":
    "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
  "ImageTags": ["00000000-0000-0000-0000-000000000000"],
  "ImagePublishedAt": "2019-10-01T20:06:12Z"
}

```

```
}
```

AwsEcrRepository

AwsEcrRepository 物件提供有關 Amazon Elastic Container Registry 儲存庫的資訊。

下列範例顯示 AwsEcrRepository 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEcrRepository屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEcrRepositoryDetails](#)。

範例

```
"AwsEcrRepository": {
  "LifecyclePolicy": {
    "RegistryId": "123456789012",
  },
  "RepositoryName": "sample-repo",
  "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
  "ImageScanningConfiguration": {
    "ScanOnPush": true
  },
  "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs ASFF 中的 資源

以下是 AwsEcs 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsEcsCluster

AwsEcsCluster 物件提供有關 Amazon Elastic Container Service 叢集的詳細資訊。

下列範例顯示 AwsEcsCluster 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEcsCluster屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEcsClusterDetails](#)。

範例

```
"AwsEcsCluster": {
  "CapacityProviders": [],
  "ClusterSettings": [
```

```

    {
      "Name": "containerInsights",
      "Value": "enabled"
    }
  ],
  "Configuration": {
    "ExecuteCommandConfiguration": {
      "KmsKeyId": "kmsKeyId",
      "LogConfiguration": {
        "CloudWatchEncryptionEnabled": true,
        "CloudWatchLogGroupName": "cloudWatchLogGroupName",
        "S3BucketName": "s3BucketName",
        "S3EncryptionEnabled": true,
        "S3KeyPrefix": "s3KeyPrefix"
      },
      "Logging": "DEFAULT"
    }
  }
  "DefaultCapacityProviderStrategy": [
    {
      "Base": 0,
      "CapacityProvider": "capacityProvider",
      "Weight": 1
    }
  ]
}

```

AwsEcsContainer

AwsEcsContainer 物件包含 Amazon ECS 容器的詳細資訊。

下列範例顯示 AwsEcsContainer 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsEcsContainer 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEcsContainerDetails](#)。

範例

```

"AwsEcsContainer": {
  "Image": "11111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
    "ContainerPath": "/mnt/etc",
    "SourceVolume": "vol-03909e9"
  }
]
}

```

```
    }],  
    "Name": "knote",  
    "Privileged": true  
  }  
}
```

AwsEcsService

AwsEcsService 物件提供 Amazon ECS 叢集內服務的詳細資訊。

下列範例顯示 AwsEcsService 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsEcsService 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEcsServiceDetails](#)。

範例

```
"AwsEcsService": {  
  "CapacityProviderStrategy": [  
    {  
      "Base": 12,  
      "CapacityProvider": "",  
      "Weight": ""  
    }  
  ],  
  "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",  
  "DeploymentConfiguration": {  
    "DeploymentCircuitBreaker": {  
      "Enable": false,  
      "Rollback": false  
    },  
    "MaximumPercent": 200,  
    "MinimumHealthyPercent": 100  
  },  
  "DeploymentController": "",  
  "DesiredCount": 1,  
  "EnableEcsManagedTags": false,  
  "EnableExecuteCommand": false,  
  "HealthCheckGracePeriodSeconds": 1,  
  "LaunchType": "FARGATE",  
  "LoadBalancers": [  
    {  
      "ContainerName": "",  
      "ContainerPort": 23,  
      "LoadBalancerName": "",  
      "TargetGroupArn": ""  
    }  
  ]  
}
```

```

],
"Name": "sample-app-service",
"NetworkConfiguration": {
  "AwsVpcConfiguration": {
    "Subnets": [
      "Subnet-example1",
      "Subnet-example2"
    ],
    "SecurityGroups": [
      "Sg-0ce48e9a6e5b457f5"
    ],
    "AssignPublicIp": "ENABLED"
  }
},
"PlacementConstraints": [
  {
    "Expression": "",
    "Type": ""
  }
],
"PlacementStrategies": [
  {
    "Field": "",
    "Type": ""
  }
],
"PlatformVersion": "LATEST",
"PropagateTags": "",
"Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/ServiceRoleForECS",
"SchedulingStrategy": "REPLICA",
"ServiceName": "sample-app-service",
"ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/sample-app-service",
"ServiceRegistries": [
  {
    "ContainerName": "",
    "ContainerPort": 1212,
    "Port": 1221,
    "RegistryArn": ""
  }
],
"TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-taskdef:1"

```



```
}
```

AwsEcsTask

AwsEcsTask 物件提供 Amazon ECS 任務的詳細資訊。

下列範例顯示 AwsEcsTask 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsEcsTask屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEcsTask](#)。

範例

```
"AwsEcsTask": {
  "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
  "CreatedAt": "1557134011644",
  "Group": "service:fargate-service",
  "StartedAt": "1557134011644",
  "StartedBy": "ecs-svc/1234567890123456789",
  "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-fargate:2",
  "Version": 3,
  "Volumes": [{
    "Name": "string",
    "Host": {
      "SourcePath": "string"
    }
  ]},
  "Containers": {
    "Image": "11111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
      "ContainerPath": "/mnt/etc",
      "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
  }
}
```

AwsEcsTaskDefinition

AwsEcsTaskDefinition 物件包含任務定義的詳細資訊。任務定義說明 Amazon Elastic Container Service 任務的容器和磁碟區定義。

下列範例顯示 `AwsEcsTaskDefinition` 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 `AwsEcsTaskDefinition` 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEcsTaskDefinitionDetails](#)。

範例

```
"AwsEcsTaskDefinition": {
  "ContainerDefinitions": [
    {
      "Command": ['ruby', 'hi.rb'],
      "Cpu": 128,
      "Essential": true,
      "HealthCheck": {
        "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
        "Interval": 10,
        "Retries": 3,
        "StartPeriod": 5,
        "Timeout": 20
      },
      "Image": "tongueroo/sinatra:latest",
      "Interactive": true,
      "Links": [],
      "LogConfiguration": {
        "LogDriver": "awslogs",
        "Options": {
          "awslogs-group": "/ecs/sinatra-hi",
          "awslogs-region": "ap-southeast-1",
          "awslogs-stream-prefix": "ecs"
        },
        "SecretOptions": []
      },
      "MemoryReservation": 128,
      "Name": "web",
      "PortMappings": [
        {
          "ContainerPort": 4567,
          "HostPort": 4567,
          "Protocol": "tcp"
        }
      ],
      "Privileged": true,
      "StartTimeout": 10,
```

```

        "StopTimeout": 100,
      },
    ],
    "Family": "sinatra-hi",
    "NetworkMode": "host",
    "RequiresCompatibilities": ["EC2"],
    "Status": "ACTIVE",
    "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
  }
}

```

AwsEfs ASFF 中的 資源

以下是 AwsEfs 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsEfsAccessPoint

AwsEfsAccessPoint 物件提供存放在 Amazon Elastic File System 中的檔案詳細資訊。

下列範例顯示 AwsEfsAccessPoint 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsEfsAccessPoint 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEfsAccessPointDetails](#)。

範例

```

"AwsEfsAccessPoint": {
  "AccessPointId": "fsap-05c4c0e79ba0b118a",
  "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/fsap-05c4c0e79ba0b118a",
  "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
  "FileSystemId": "fs-0f8137f731cb32146",
  "PosixUser": {
    "Gid": "1000",
    "SecondaryGids": ["0", "4294967295"],
    "Uid": "1234"
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": "1000",
      "OwnerUid": "1234",
      "Permissions": "777"
    },
  },
}

```

```
"Path": "/tmp/example"
}
```

AwsEks ASFF 中的 資源

以下是 AwsEks 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsEksCluster

AwsEksCluster 物件提供 Amazon EKS 叢集的詳細資訊。

下列範例顯示 AwsEksCluster 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsEksCluster 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEksClusterDetails](#)。

範例

```
{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",

```

```

        "audit",
        "authenticator",
        "controllerManager",
        "scheduler"
    ],
    "Enabled": true
  }
],
},
"Status": "CREATING",
"CertificateAuthorityData": {},
}
}

```

AwsElasticBeanstalk ASFF 中的 資源

以下是 AwsElasticBeanstalk 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsElasticBeanstalkEnvironment

AwsElasticBeanstalkEnvironment 物件包含 AWS Elastic Beanstalk 環境的詳細資訊。

下列範例顯示 AwsElasticBeanstalkEnvironment 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsElasticBeanstalkEnvironment屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsElasticBeanstalkEnvironmentDetails](#)。

範例

```

"AwsElasticBeanstalkEnvironment": {
  "ApplicationName": "MyApplication",
  "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
  "DateCreated": "2021-04-30T01:38:01.090Z",
  "DateUpdated": "2021-04-30T01:38:01.090Z",
  "Description": "Example description of my awesome application",
  "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-east-1.elb.amazonaws.com",
  "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/MyApplication/myapplication-env",
  "EnvironmentId": "e-abcd1234",
  "EnvironmentLinks": [
    {

```

```

        "EnvironmentName": "myexampleapp-env",
        "LinkName": "myapplicationLink"
    }
],
"EnvironmentName": "myapplication-env",
"OptionSettings": [
    {
        "Namespace": "aws:elasticbeanstalk:command",
        "OptionName": "BatchSize",
        "Value": "100"
    },
    {
        "Namespace": "aws:elasticbeanstalk:command",
        "OptionName": "Timeout",
        "Value": "600"
    },
    {
        "Namespace": "aws:elasticbeanstalk:command",
        "OptionName": "BatchSizeType",
        "Value": "Percentage"
    },
    {
        "Namespace": "aws:elasticbeanstalk:command",
        "OptionName": "IgnoreHealthCheck",
        "Value": "false"
    },
    {
        "Namespace": "aws:elasticbeanstalk:application",
        "OptionName": "Application Healthcheck URL",
        "Value": "TCP:80"
    }
],
"PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
running on 64bit Amazon Linux/2.7.7",
"SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
"Status": "Ready",
"Tier": {
    "Name": "WebServer"
    "Type": "Standard"
    "Version": "1.0"
},
"VersionLabel": "Sample Application"
}

```

AwsElasticSearch ASFF 中的 資源

以下是 AwsElasticSearch 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsElasticSearchDomain

AwsElasticSearchDomain 物件提供 Amazon OpenSearch Service 網域的詳細資訊。

下列範例顯示 AwsElasticSearchDomain 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsElasticSearchDomain屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsElasticSearchDomainDetails](#)。

範例

```
"AwsElasticSearchDomain": {
  "AccessPolicies": "string",
  "DomainStatus": {
    "DomainId": "string",
    "DomainName": "string",
    "Endpoint": "string",
    "Endpoints": {
      "string": "string"
    }
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "ElasticsearchClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,
    "InstanceType": "string",
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": number
    },
    "ZoneAwarenessEnabled": boolean
  },
  "ElasticsearchVersion": "string",
  "EncryptionAtRestOptions": {
```

```
        "Enabled": boolean,
        "KmsKeyId": "string"
    },
    "LogPublishingOptions": {
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "string",
            "Enabled": boolean
        },
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "string",
            "Enabled": boolean
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "string",
            "Enabled": boolean
        }
    },
    "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
        "Description": "string",
        "NewVersion": "string",
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
    },
    "VPCOptions": {
        "AvailabilityZones": [
            "string"
        ],
        "SecurityGroupIds": [
            "string"
        ],
        "SubnetIds": [
            "string"
        ],
        "VPCId": "string"
    }
}
```


AwsElb ASFF 中的 資源

以下是 AwsElb 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsElbLoadBalancer

AwsElbLoadBalancer 物件包含 Classic Load Balancer 的詳細資訊。

下列範例顯示 AwsElbLoadBalancer 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsElbLoadBalancer 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsElbLoadBalancerDetails](#)。

範例

```
"AwsElbLoadBalancer": {
  "AvailabilityZones": ["us-west-2a"],
  "BackendServerDescriptions": [
    {
      "InstancePort": 80,
      "PolicyNames": ["doc-example-policy"]
    }
  ],
  "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
  "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
  "CreatedTime": "2020-08-03T19:22:44.637Z",
  "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
  "HealthCheck": {
    "HealthyThreshold": 2,
    "Interval": 30,
    "Target": "HTTP:80/png",
    "Timeout": 3,
    "UnhealthyThreshold": 2
  },
  "Instances": [
    {
      "InstanceId": "i-example"
    }
  ],
  "ListenerDescriptions": [
    {
```

```
        "Listener": {
            "InstancePort": 443,
            "InstanceProtocol": "HTTPS",
            "LoadBalancerPort": 443,
            "Protocol": "HTTPS",
            "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
        },
        "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
    }
],
"LoadBalancerAttributes": {
    "AccessLog": {
        "EmitInterval": 60,
        "Enabled": true,
        "S3BucketName": "amzn-s3-demo-bucket",
        "S3BucketPrefix": "doc-example-prefix"
    },
    "ConnectionDraining": {
        "Enabled": false,
        "Timeout": 300
    },
    "ConnectionSettings": {
        "IdleTimeout": 30
    },
    "CrossZoneLoadBalancing": {
        "Enabled": true
    },
    "AdditionalAttributes": [{
        "Key": "elb.http.desyncmitigationmode",
        "Value": "strictest"
    }]
},
"LoadBalancerName": "example-load-balancer",
"Policies": {
    "AppCookieStickinessPolicies": [
        {
            "CookieName": "",
            "PolicyName": ""
        }
    ],
    "LbCookieStickinessPolicies": [
        {
```

```

        "CookieExpirationPeriod": 60,
        "PolicyName": "my-example-cookie-policy"
    },
    ],
    "OtherPolicies": [
        "my-PublicKey-policy",
        "my-authentication-policy",
        "my-SSLNegotiation-policy",
        "my-ProxyProtocol-policy",
        "ELBSecurityPolicy-2015-03"
    ],
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
        "OwnerAlias": "444455556666"
    },
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}

```

AwsElbv2LoadBalancer

AwsElbv2LoadBalancer 物件提供了負載平衡器的資訊。

下列範例顯示 AwsElbv2LoadBalancer 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsElbv2LoadBalancer屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsElbv2LoadBalancerDetails](#)。

範例

```

"AwsElbv2LoadBalancer": {
    "AvailabilityZones": {
        "SubnetId": "string",
        "ZoneName": "string"
    },
    "CanonicalHostedZoneId": "string",
    "CreatedTime": "string",
    "DNSName": "string",
    "IpAddressType": "string",
    "LoadBalancerAttributes": [
        {

```

```

        "Key": "string",
        "Value": "string"
      }
    ],
    "Scheme": "string",
    "SecurityGroups": [ "string" ],
    "State": {
      "Code": "string",
      "Reason": "string"
    },
    "Type": "string",
    "VpcId": "string"
  }
}

```

AwsEventBridge ASFF 中的 資源

以下是 AwsEventBridge 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsEventSchemasRegistry

AwsEventSchemasRegistry 物件提供有關 Amazon EventBridge 結構描述登錄檔的資訊。結構描述會定義傳送至 EventBridge 的事件結構。結構描述登錄檔是收集結構描述並將其邏輯分組的容器。

下列範例顯示 AwsEventSchemasRegistry 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsEventSchemasRegistry 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEventSchemasRegistry](#)。

範例

```

"AwsEventSchemasRegistry": {
  "Description": "This is an example event schema registry.",
  "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
  "RegistryName": "schema-registry"
}

```

AwsEventsEndpoint

AwsEventsEndpoint 物件提供有關 Amazon EventBridge 全域端點的資訊。端點可以透過提高區域容錯能力來改善應用程式的可用性。

下列範例顯示 `AwsEventsEndpoint` 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 `AwsEventsEndpoint` 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEventsEndpointDetails](#)。

範例

```
"AwsEventsEndpoint": {
  "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
  "Description": "This is a sample endpoint.",
  "EndpointId": "04k1exajoy.veo",
  "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
  "EventBuses": [
    {
      "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
    },
    {
      "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
    }
  ],
  "Name": "my-endpoint",
  "ReplicationConfig": {
    "State": "ENABLED"
  },
  "RoleArn": "arn:aws:iam::123456789012:role/service-role/Amazon_EventBridge_Invoke_Event_Bus_1258925394",
  "RoutingConfig": {
    "FailoverConfig": {
      "Primary": {
        "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "Secondary": {
        "Route": "us-east-2"
      }
    }
  },
  "State": "ACTIVE"
}
```

AwsEventsEventbus

`AwsEventsEventbus` 物件提供有關 Amazon EventBridge 全域端點的資訊。端點可以透過提高區域容錯能力來改善應用程式的可用性。

下列範例顯示 `AwsEventsEventbus` 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 `AwsEventsEventbus` 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsEventsEventbusDetails](#)。

範例

```
"AwsEventsEventbus":
  "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
  "Name": "my-event-bus",
  "Policy": "{\n  \"Version\": \"2012-10-17\",
    \"Statement\": [{\n      \"Sid\": \"AllowAllAccountsFromOrganizationToPutEvents\",
      \"Effect\": \"Allow\",
      \"Principal\": \"*\",
      \"Action\": \"events:PutEvents\",
      \"Resource\": \"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",
      \"Condition\": {\n        \"StringEquals\": {\n          \"aws:PrincipalOrgID\": \"o-ki7yjt看5\"
        }\n      },
      \"Sid\": \"AllowAccountToManageRulesTheyCreated\",
      \"Effect\": \"Allow\",
      \"Principal\": {\n        \"AWS\": \"arn:aws:iam::123456789012:root\"
      },
      \"Action\": [\"events:PutRule\", \"events:PutTargets\", \"events:DeleteRule\", \"events:RemoveTargets\", \"events:DisableRule\", \"events:EnableRule\", \"events:TagResource\", \"events:UntagResource\", \"events:DescribeRule\", \"events:ListTargetsByRule\", \"events:ListTagsForResource\"],
      \"Resource\": \"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",
      \"Condition\": {\n        \"StringEqualsIfExists\": {\n          \"events:creatorAccount\": \"123456789012\"
        }\n      }\n    }\n  }"
```

AwsGuardDuty ASFF 中的 資源

以下是 `AwsGuardDuty` 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsGuardDutyDetector

`AwsGuardDutyDetector` 物件提供 Amazon GuardDuty 偵測器的相關資訊。偵測器是一種用來代表 GuardDuty 服務的物件。GuardDuty 需要偵測器才能運作。

下列範例顯示 `AwsGuardDutyDetector` 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 `AwsGuardDutyDetector` 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsGuardDutyDetector](#)。

範例

```
"AwsGuardDutyDetector": {
```

```

    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
            "Status": "ENABLED"
        },
        "Kubernetes": {
            "AuditLogs": {
                "Status": "ENABLED"
            }
        },
        "MalwareProtection": {
            "ScanEc2InstanceWithFindings": {
                "EbsVolumes": {
                    "Status": "ENABLED"
                }
            },
            "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
        }
    }
}

```

AwsIam ASFF 中的 資源

以下是 AwsIam 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsIamAccessKey

AwsIamAccessKey 物件包含與問題清單相關的 IAM 存取金鑰詳細資訊。

下列範例顯示 `AwsIamAccessKey` 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 `AwsIamAccessKey` 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsIamAccessKeyDetails](#)。

範例

```
"AwsIamAccessKey": {
  "AccessKeyId": "string",
  "AccountId": "string",
  "CreatedAt": "string",
  "PrincipalId": "string",
  "PrincipalName": "string",
  "PrincipalType": "string",
  "SessionContext": {
    "Attributes": {
      "CreationDate": "string",
      "MfaAuthenticated": boolean
    },
    "SessionIssuer": {
      "AccountId": "string",
      "Arn": "string",
      "PrincipalId": "string",
      "Type": "string",
      "UserName": "string"
    }
  },
  "Status": "string"
}
```

AwsIamGroup

`AwsIamGroup` 物件包含 IAM 群組的詳細資訊。

下列範例顯示 `AwsIamGroup` 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 `AwsIamGroup` 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsIamGroupDetails](#)。

範例

```
"AwsIamGroup": {
  "AttachedManagedPolicies": [
    {
      "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
    }
  ]
}
```



```

        "PolicyName": "ExampleManagedAccess",
      }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
      {
        "PolicyName": "ExampleGroupPolicy"
      }
    ],
    "Path": "/"
  }
}

```

AwsIamPolicy

AwsIamPolicy 物件代表 IAM 許可政策。

下列範例顯示 AwsIamPolicy 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsIamPolicy屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsIamPolicyDetails](#)。

範例

```

"AwsIamPolicy": {
  "AttachmentCount": 1,
  "CreateDate": "2017-09-14T08:17:29.000Z",
  "DefaultVersionId": "v1",
  "Description": "Example IAM policy",
  "IsAttachable": true,
  "Path": "/",
  "PermissionsBoundaryUsageCount": 5,
  "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
  "PolicyName": "EXAMPLE-MANAGED-POLICY",
  "PolicyVersionList": [
    {
      "VersionId": "v1",
      "IsDefaultVersion": true,
      "CreateDate": "2017-09-14T08:17:29.000Z"
    }
  ],
  "UpdateDate": "2017-09-14T08:17:29.000Z"
}

```

AwsIamRole

AwsIamRole 物件包含 IAM 角色的相關資訊，包括角色的所有政策。

下列範例顯示 AwsIamRole 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsIamRole屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsIamRoleDetails](#)。

範例

```
"AwsIamRole": {
  "AssumeRolePolicyDocument": "{ 'Version': '2012-10-17',          'Statement':
[{'Effect': 'Allow', 'Action': 'sts:AssumeRole'}]}",
  "AttachedManagedPolicies": [
    {
      "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
      "PolicyName": "Example policy 1"
    },
    {
      "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
      "PolicyName": "Example policy 2"
    }
  ],
  "CreateDate": "2020-03-14T07:19:14.000Z",
  "InstanceProfileList": [
    {
      "Arn": "arn:aws:iam::333333333333:ExampleProfile",
      "CreateDate": "2020-03-11T00:02:27Z",
      "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
      "InstanceProfileName": "ExampleInstanceProfile",
      "Path": "/",
      "Roles": [
        {
          "Arn": "arn:aws:iam::444455556666:role/example-role",
          "AssumeRolePolicyDocument": "",
          "CreateDate": "2020-03-11T00:02:27Z",
          "Path": "/",
          "RoleId": "AR0AJ520TH4H7LEXAMPLE",
          "RoleName": "example-role",
        }
      ]
    }
  ],
  "MaxSessionDuration": 3600,
  "Path": "/",
}
```

```

    "PermissionsBoundary": {
      "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
      "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
    },
    "RoleId": "ARO4TPS3VLEXAMPLE",
    "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
    "RolePolicyList": [
      {
        "PolicyName": "Example role policy"
      }
    ]
  }
}

```

AwsIamUser

AwsIamUser 物件提供使用者的相關資訊。

下列範例顯示 **AwsIamUser** 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 **AwsIamUser** 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsIamUserDetails](#)。

範例

```

"AwsIamUser": {
  "AttachedManagedPolicies": [
    {
      "PolicyName": "ExamplePolicy",
      "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
    }
  ],
  "CreateDate": "2018-01-26T23:50:05.000Z",
  "GroupList": [],
  "Path": "/",
  "PermissionsBoundary": {
    "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
    "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
  },
  "UserId": "AIDACKCEVSQ6C2EXAMPLE",
  "UserName": "ExampleUser",
  "UserPolicyList": [
    {
      "PolicyName": "InstancePolicy"
    }
  ]
}

```

```
}
```

AwsKinesis ASFF 中的 資源

以下是 AwsKinesis 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsKinesisStream

AwsKinesisStream 物件提供有關 Amazon Kinesis Data Streams 的詳細資訊。

下列範例顯示 AwsKinesisStream 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsKinesisStream屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsKinesisStreamDetails](#)。

範例

```
"AwsKinesisStream": {
  "Name": "test-vir-kinesis-stream",
  "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
  "RetentionPeriodHours": 24,
  "ShardCount": 2,
  "StreamEncryption": {
    "EncryptionType": "KMS",
    "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
  }
}
```

AwsKms ASFF 中的 資源

以下是 AwsKms 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsKmsKey

AwsKmsKey 物件提供有關 的詳細資訊 AWS KMS key。

下列範例顯示 AwsKmsKey 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsKmsKey屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsKmsKeyDetails](#)。

範例

```
"AwsKmsKey": {
    "AWSAccountId": "string",
    "CreationDate": "string",
    "Description": "string",
    "KeyId": "string",
    "KeyManager": "string",
    "KeyRotationStatus": boolean,
    "KeyState": "string",
    "Origin": "string"
}
```

AwsLambda

以下是 AwsLambda 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsLambdaFunction

AwsLambdaFunction 物件提供 Lambda 函數組態的詳細資訊。

下列範例顯示 AwsLambdaFunction 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsLambdaFunction屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsLambdaFunctionDetails](#)。

範例

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "amzn-s3-demo-bucket",
        "S3Key": "samplekey",
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111111111111111111111111111111111111111111111111111111",
    "DeadLetterConfig": {
```

```

    "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
  },
  "Environment": {
    "Variables": {
      "Stage": "foobar"
    },
    "Error": {
      "ErrorCode": "Sample-error-code",
      "Message": "Caller principal is a manager."
    }
  },
  "FunctionName": "CheckOut",
  "Handler": "main.py:lambda_handler",
  "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
  "LastModified": "2001-09-11T09:00:00Z",
  "Layers": {
    "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
    "CodeSize": 169
  },
  "PackageType": "Zip",
  "RevisionId": "23",
  "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
  "Runtime": "go1.7",
  "Timeout": 15,
  "TracingConfig": {
    "Mode": "Active"
  },
  "Version": "$LATEST",
  "VpcConfig": {
    "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
    "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
  },
  "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
  "MemorySize": 2048
}

```

AwsLambdaLayerVersion

AwsLambdaLayerVersion 物件提供 Lambda layer 版本的詳細資訊。

下列範例顯示 AwsLambdaLayerVersion 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsLambdaLayerVersion屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsLambdaLayerVersionDetails](#)。

範例

```
"AwsLambdaLayerVersion": {
  "Version": 2,
  "CompatibleRuntimes": [
    "java8"
  ],
  "CreateDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk ASFF 中的 資源

以下是 AwsMsk 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsMskCluster

AwsMskCluster 物件提供有關 Amazon Managed Streaming for Apache Kafka (Amazon MSK) 叢集的資訊。

下列範例顯示 AwsMskCluster 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsMskCluster 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsMskClusterDetails](#)。

範例

```
"AwsMskCluster": {
  "ClusterInfo": {
    "ClientAuthentication": {
      "Sasl": {
        "Scram": {
          "Enabled": true
        },
        "Iam": {
          "Enabled": true
        }
      },
      "Tls": {
        "CertificateAuthorityArnList": [],
        "Enabled": false
      },
      "Unauthenticated": {
```

```

        "Enabled": false
      },
      "ClusterName": "my-cluster",
      "CurrentVersion": "K2PWKAKR8XB7XF",
      "EncryptionInfo": {
        "EncryptionAtRest": {
          "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
        },
        "EncryptionInTransit": {
          "ClientBroker": "TLS",
          "InCluster": true
        }
      },
      "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
      "NumberOfBrokerNodes": 3
    }
  }
}

```

AwsNetworkFirewall ASFF 中的 資源

以下是 AwsNetworkFirewall 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsNetworkFirewallFirewall

AwsNetworkFirewallFirewall 物件包含 AWS Network Firewall 防火牆的詳細資訊。

下列範例顯示 AwsNetworkFirewallFirewall 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsNetworkFirewallFirewall 屬性的說明，請參閱 AWS Security Hub API 參考中的 [AwsNetworkFirewallFirewallDetails](#)。

範例

```

"AwsNetworkFirewallFirewall": {
  "DeleteProtection": false,
  "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/testfirewall",
  "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-policy/InitialFirewall",

```



```

    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
      {
        "SubnetId": "subnet-0183481095e588cdc"
      },
      {
        "SubnetId": "subnet-01f518fad1b1c90b0"
      }
    ],
    "VpcId": "vpc-40e83c38"
  }

```

AwsNetworkFirewallFirewallPolicy

AwsNetworkFirewallFirewallPolicy 物件提供防火牆政策的詳細資訊。防火牆政策會定義網路防火牆的行為。

下列範例顯示 AwsNetworkFirewallFirewallPolicy 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsNetworkFirewallFirewallPolicy屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsNetworkFirewallFirewallPolicyDetails](#)。

範例

```

"AwsNetworkFirewallFirewallPolicy": {
  "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
      {
        "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-rulegroup/PatchesOnly"
      }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
      {
        "Priority": 1,
        "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-rulegroup/Stateless-1"
      }
    ]
  }
}

```

```
},
  "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-policy/InitialFirewall",
  "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
  "FirewallPolicyName": "InitialFirewall",
  "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

AwsNetworkFirewallRuleGroup 物件提供 AWS Network Firewall 規則群組的詳細資訊。規則群組用於檢查和控制網路流量。無狀態規則群組適用於個別封包。狀態規則群組會套用到流量流程中的封包。

防火牆政策中會參考規則群組。

下列範例顯示 AwsNetworkFirewallRuleGroup 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsNetworkFirewallRuleGroup屬性的說明，請參閱 AWS Security Hub API 參考中的 [AwsNetworkFirewallRuleGroupDetails](#)。

範例 – 無狀態規則群組

```
"AwsNetworkFirewallRuleGroup": {
  "Capacity": 600,
  "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-rulegroup/Stateless-1",
  "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
  "RuleGroupName": "Stateless-1"
  "Description": "Example of a stateless rule group",
  "Type": "STATELESS",
  "RuleGroup": {
    "RulesSource": {
      "StatelessRulesAndCustomActions": {
        "CustomActions": [],
        "StatelessRules": [
          {
            "Priority": 1,
            "RuleDefinition": {
              "Actions": [
                "aws:pass"
              ],
              "MatchAttributes": {
                "DestinationPorts": [
```

```
{
    {
        "FromPort": 443,
        "ToPort": 443
    },
    "Destinations": [
        {
            "AddressDefinition": "192.0.2.0/24"
        }
    ],
    "Protocols": [
        6
    ],
    "SourcePorts": [
        {
            "FromPort": 0,
            "ToPort": 65535
        }
    ],
    "Sources": [
        {
            "AddressDefinition": "198.51.100.0/24"
        }
    ]
}
}
```

範例－狀態規則群組

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",

```

```

    "RuleGroup": {
      "RuleSource": {
        "StatefulRules": [
          {
            "Action": "PASS",
            "Header": {
              "Destination": "Any",
              "DestinationPort": "443",
              "Direction": "ANY",
              "Protocol": "TCP",
              "Source": "Any",
              "SourcePort": "Any"
            },
            "RuleOptions": [
              {
                "Keyword": "sid:1"
              }
            ]
          }
        ]
      }
    }
  }
}

```

以下是AwsNetworkFirewallRuleGroup屬性的有效值範例清單：

- Action

有效值：PASS | DROP | ALERT

- Protocol

有效值：IP | TCP | UDP | ICMP HTTP | FTP | | TLS | SMB | DNS | DCERPC | SSH | SMTP IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP DHCP

- Flags

有效值：FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

- Masks

有效值：FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

AwsOpenSearchService ASFF 中的 資源

以下是 AwsOpenSearchService 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsOpenSearchServiceDomain

AwsOpenSearchServiceDomain 物件包含 Amazon OpenSearch Service 網域的相關資訊。

下列範例顯示 AwsOpenSearchServiceDomain 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsOpenSearchServiceDomain屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsOpenSearchServiceDomainDetails](#)。

範例

```
"AwsOpenSearchServiceDomain": {
  "AccessPolicies": "IAM_Id",
  "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
      "MasterUserName": "third-master-use",
      "MasterUserPassword": "some-password"
    }
  },
  "Arn": "arn:aws:opensearch:us-east-1:111122223333:somedomain",
  "ClusterConfig": {
    "InstanceType": "c5.large.search",
    "InstanceCount": 1,
    "DedicatedMasterEnabled": true,
    "ZoneAwarenessEnabled": false,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 2
    },
    "DedicatedMasterType": "c5.large.search",
    "DedicatedMasterCount": 3,
    "WarmEnabled": true,
    "WarmCount": 3,
    "WarmType": "ultrawarm1.large.search"
  },
}
```

```

    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
    "DomainEndpoints": {
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
    },
    "NodeToNodeEncryptionOptions": {
        "Enabled": true
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",

```

```

    "Description": "There is no software update available for this domain.",
    "NewVersion": "OpenSearch_1.0",
    "UpdateAvailable": false,
    "UpdateStatus": "COMPLETED",
    "OptionalDeployment": false
  },
  "VpcOptions": {
    "SecurityGroupIds": [
      "sg-2a3a4a5a"
    ],
    "SubnetIds": [
      "subnet-1a2a3a4a"
    ],
  }
}

```

AwsRds ASFF 中的 資源

以下是 AwsRds 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsRdsDbCluster

AwsRdsDbCluster 物件提供 Amazon RDS 資料庫叢集的詳細資訊。

下列範例顯示 AwsRdsDbCluster 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsRdsDbCluster 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsRdsDbClusterDetails](#)。

範例

```

"AwsRdsDbCluster": {
  "ActivityStreamStatus": "stopped",
  "AllocatedStorage": 1,
  "AssociatedRoles": [
    {
      "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/AWSServiceRoleForRDS",
      "Status": "PENDING"
    }
  ],
  "AutoMinorVersionUpgrade": true,

```

```
"AvailabilityZones": [
    "us-east-1a",
    "us-east-1c",
    "us-east-1e"
],
"BackupRetentionPeriod": 1,
"ClusterCreateTime": "2020-06-22T17:40:12.322Z",
"CopyTagsToSnapshot": true,
"CrossAccountClone": false,
"CustomEndpoints": [],
"DatabaseName": "Sample name",
"DbClusterIdentifier": "database-3",
"DbClusterMembers": [
    {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
    }
],
"DbClusterOptionGroupMemberships": [],
"DbClusterParameterGroup": "cluster-parameter-group",
"DbClusterResourceId": "cluster-example",
"DbSubnetGroup": "subnet-group",
"DeletionProtection": false,
"DomainMemberships": [],
"Status": "modifying",
"EnabledCloudwatchLogsExports": [
    "audit",
    "error",
    "general",
    "slowquery"
],
"Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
"Engine": "aurora-mysql",
"EngineMode": "provisioned",
"EngineVersion": "5.7.mysql_aurora.2.03.4",
"HostedZoneId": "ZONE1",
"HttpEndpointEnabled": false,
"IamDatabaseAuthenticationEnabled": false,
"KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
"MasterUsername": "admin",
"MultiAz": false,
"Port": 3306,
```



```

    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
      {
        "Status": "active",
        "VpcSecurityGroupId": "sg-example-1"
      }
    ],
  }
}

```

AwsRdsDbClusterSnapshot

AwsRdsDbClusterSnapshot 物件包含 Amazon RDS 資料庫叢集快照的相關資訊。

下列範例顯示 AwsRdsDbClusterSnapshot 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsRdsDbClusterSnapshot屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsRdsDbClusterSnapshotDetails](#)。

範例

```

"AwsRdsDbClusterSnapshot": {
  "AllocatedStorage": 0,
  "AvailabilityZones": [
    "us-east-1a",
    "us-east-1d",
    "us-east-1e"
  ],
  "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
  "DbClusterIdentifier": "database-2",
  "DbClusterSnapshotAttributes": [{
    "AttributeName": "restore",
    "AttributeValues": ["123456789012"]
  }],
  "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
  "Engine": "aurora",
  "EngineVersion": "5.6.10a",
  "IamDatabaseAuthenticationEnabled": false,
  "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
  "LicenseModel": "aurora",

```

```
"MasterUsername": "admin",
"PercentProgress": 100,
"Port": 0,
"SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
"SnapshotType": "automated",
"Status": "available",
"StorageEncrypted": true,
"VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

AwsRdsDbInstance 物件提供 Amazon RDS 資料庫執行個體的詳細資訊。

下列範例顯示 AwsRdsDbInstance 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsRdsDbInstance屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsRdsDbInstanceDetails](#)。

範例

```
"AwsRdsDbInstance": {
  "AllocatedStorage": 20,
  "AssociatedRoles": [],
  "AutoMinorVersionUpgrade": true,
  "AvailabilityZone": "us-east-1d",
  "BackupRetentionPeriod": 7,
  "CaCertificateIdentifier": "certificate1",
  "CharacterSetName": "",
  "CopyTagsToSnapshot": true,
  "DbClusterIdentifier": "",
  "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
  "DbInstanceClass": "db.t2.micro",
  "DbInstanceIdentifier": "database-1",
  "DbInstancePort": 0,
  "DbInstanceStatus": "available",
  "DbiResourceId": "db-EXAMPLE123",
  "DbName": "",
  "DbParameterGroups": [
    {
      "DbParameterGroupName": "default.mysql5.7",
      "ParameterApplyStatus": "in-sync"
    }
  ],
}
```

```

"DbSecurityGroups": [],

"DbSubnetGroup": {
  "DbSubnetGroupName": "my-group-123abc",
  "DbSubnetGroupDescription": "My subnet group",
  "VpcId": "vpc-example1",
  "SubnetGroupStatus": "Complete",
  "Subnets": [
    {
      "SubnetIdentifier": "subnet-123abc",
      "SubnetAvailabilityZone": {
        "Name": "us-east-1d"
      },
      "SubnetStatus": "Active"
    },
    {
      "SubnetIdentifier": "subnet-456def",
      "SubnetAvailabilityZone": {
        "Name": "us-east-1c"
      },
      "SubnetStatus": "Active"
    }
  ],
  "DbSubnetGroupArn": ""
},
"DeletionProtection": false,
"DomainMemberships": [],
"EnabledCloudWatchLogsExports": [],
"Endpoint": {
  "address": "database-1.example.us-east-1.rds.amazonaws.com",
  "port": 3306,
  "hostedZoneId": "ZONEID1"
},
"Engine": "mysql",
"EngineVersion": "5.7.22",
"EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-group:Example:log-stream:db-EXAMPLE1",
"IamDatabaseAuthenticationEnabled": false,
"InstanceCreateTime": "2020-06-22T17:40:12.322Z",
"Iops": "",
"KmsKeyId": "",
"LatestRestorableTime": "2020-06-24T05:50:00.000Z",
"LicenseModel": "general-public-license",

```

```
"ListenerEndpoint": "",
"MasterUsername": "admin",
"MaxAllocatedStorage": 1000,
"MonitoringInterval": 60,
"MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
"MultiAz": false,
"OptionGroupMemberships": [
  {
    "OptionGroupName": "default:mysql-5-7",
    "Status": "in-sync"
  }
],
"PreferredBackupWindow": "03:57-04:27",
"PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
"PendingModifiedValues": {
  "DbInstanceClass": "",
  "AllocatedStorage": "",
  "MasterUserPassword": "",
  "Port": "",
  "BackupRetentionPeriod": "",
  "MultiAZ": "",
  "EngineVersion": "",
  "LicenseModel": "",
  "Iops": "",
  "DbInstanceIdentifier": "",
  "StorageType": "",
  "CaCertificateIdentifier": "",
  "DbSubnetGroupName": "",
  "PendingCloudWatchLogsExports": "",
  "ProcessorFeatures": []
},
"PerformanceInsightsEnabled": false,
"PerformanceInsightsKmsKeyId": "",
"PerformanceInsightsRetentionPeriod": "",
"ProcessorFeatures": [],
"PromotionTier": "",
"PubliclyAccessible": false,
"ReadReplicaDBClusterIdentifiers": [],
"ReadReplicaDBInstanceIdentifiers": [],
"ReadReplicaSourceDBInstanceIdentifier": "",
"SecondaryAvailabilityZone": "",
"StatusInfos": [],
"StorageEncrypted": false,
"StorageType": "gp2",
```

```
"TdeCredentialArn": "",
"Timezone": "",
"VpcSecurityGroups": [
  {
    "VpcSecurityGroupId": "sg-example1",
    "Status": "active"
  }
]
}
```

AwsRdsDbSecurityGroup

AwsRdsDbSecurityGroup 物件包含 Amazon Relational Database Service 的相關資訊

下列範例顯示 AwsRdsDbSecurityGroup 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsRdsDbSecurityGroup屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsRdsDbSecurityGroupDetails](#)。

範例

```
"AwsRdsDbSecurityGroup": {
  "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
  "DbSecurityGroupDescription": "default",
  "DbSecurityGroupName": "mysecgroup",
  "Ec2SecurityGroups": [
    {
      "Ec2SecurityGrouppuId": "myec2group",
      "Ec2SecurityGroupName": "default",
      "Ec2SecurityGroupOwnerId": "987654321021",
      "Status": "authorizing"
    }
  ],
  "IpRanges": [
    {
      "Cidrip": "0.0.0.0/0",
      "Status": "authorizing"
    }
  ],
  "OwnerId": "123456789012",
  "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

AwsRdsDbSnapshot 物件包含 Amazon RDS 資料庫叢集快照的詳細資訊。

下列範例顯示 AwsRdsDbSnapshot 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsRdsDbSnapshot屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsRdsDbSnapshotDetails](#)。

範例

```
"AwsRdsDbSnapshot": {
  "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
  "DbInstanceIdentifier": "database-1",
  "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
  "Engine": "mysql",
  "AllocatedStorage": 20,
  "Status": "available",
  "Port": 3306,
  "AvailabilityZone": "us-east-1d",
  "VpcId": "vpc-example1",
  "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
  "MasterUsername": "admin",
  "EngineVersion": "5.7.22",
  "LicenseModel": "general-public-license",
  "SnapshotType": "automated",
  "Iops": null,
  "OptionGroupName": "default:mysql-5-7",
  "PercentProgress": 100,
  "SourceRegion": null,
  "SourceDbSnapshotIdentifier": "",
  "StorageType": "gp2",
  "TdeCredentialArn": "",
  "Encrypted": false,
  "KmsKeyId": "",
  "Timezone": "",
  "IamDatabaseAuthenticationEnabled": false,
  "ProcessorFeatures": [],
  "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

AwsRdsEventSubscription 包含 RDS 事件通知訂閱的詳細資訊。訂閱可讓 RDS 將事件發佈至 SNS 主題。

下列範例顯示 AwsRdsEventSubscription 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsRdsEventSubscription屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsRdsEventSubscriptionDetails](#)。

範例

```
"AwsRdsEventSubscription": {
  "CustSubscriptionId": "myawsuser-secgrp",
  "CustomerAwsId": "111111111111",
  "Enabled": true,
  "EventCategoriesList": [
    "configuration change",
    "failure"
  ],
  "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
  "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
  "SourceIdsList": [
    "si-sample",
    "mysqlldb-rr"
  ],
  "SourceType": "db-security-group",
  "Status": "creating",
  "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift ASFF 中的 資源

以下是 AwsRedshift 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsRedshiftCluster

AwsRedshiftCluster 物件包含 Amazon Redshift 叢集的詳細資訊。

下列範例顯示 `AwsRedshiftCluster` 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 `AwsRedshiftCluster` 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsRedshiftClusterDetails](#)。

範例

```
"AwsRedshiftCluster": {
  "AllowVersionUpgrade": true,
  "AutomatedSnapshotRetentionPeriod": 1,
  "AvailabilityZone": "us-west-2d",
  "ClusterAvailabilityStatus": "Unavailable",
  "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
  "ClusterIdentifier": "redshift-cluster-1",
  "ClusterNodes": [
    {
      "NodeRole": "LEADER",
      "PrivateIPAddress": "192.0.2.108",
      "PublicIPAddress": "198.51.100.29"
    },
    {
      "NodeRole": "COMPUTE-0",
      "PrivateIPAddress": "192.0.2.22",
      "PublicIPAddress": "198.51.100.63"
    },
    {
      "NodeRole": "COMPUTE-1",
      "PrivateIPAddress": "192.0.2.224",
      "PublicIPAddress": "198.51.100.226"
    }
  ],
  "ClusterParameterGroups": [
    {
      "ClusterParameterStatusList": [
        {
          "ParameterName": "max_concurrency_scaling_clusters",
          "ParameterApplyStatus": "in-sync",
          "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
        },
        {
          "ParameterName": "enable_user_activity_logging",
          "ParameterApplyStatus": "in-sync",
          "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
        }
      ]
    }
  ]
}
```



```
{
  "ParameterName": "auto_analyze",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "query_group",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "datestyle",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "extra_float_digits",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "search_path",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "statement_timeout",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "wlm_json_configuration",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "require_ssl",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
},
{
  "ParameterName": "use_fips_ssl",
  "ParameterApplyStatus": "in-sync",
  "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
}
```

```

        }
    ],
    "ParameterApplyStatus": "in-sync",
    "ParameterGroupName": "temp"
}
],
"ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
"ClusterRevisionNumber": 17498,
"ClusterSecurityGroups": [
    {
        "ClusterSecurityGroupName": "default",
        "Status": "active"
    }
],
"ClusterSnapshotCopyStatus": {
    "DestinationRegion": "us-west-2",
    "ManualSnapshotRetentionPeriod": -1,
    "RetentionPeriod": 1,
    "SnapshotCopyGrantName": "snapshotCopyGrantName"
},
"ClusterStatus": "available",
"ClusterSubnetGroupName": "default",
"ClusterVersion": "1.0",
"DBName": "dev",
"DeferredMaintenanceWindows": [
    {
        "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
        "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
        "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
    }
],
"ElasticIpStatus": {
    "ElasticIp": "203.0.113.29",
    "Status": "active"
},
"ElasticResizeNumberOfNodeOptions": "4",
"Encrypted": false,
"Endpoint": {
    "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
    "Port": 5439
},
"EnhancedVpcRouting": false,
"ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
"ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",

```

```

"HsmStatus": {
  "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
  "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
  "Status": "applying"
},
"IamRoles": [
  {
    "ApplyStatus": "in-sync",
    "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
  }
],
"KmsKeyId": "kmsKeyId",
"LoggingStatus": {
  "BucketName": "amzn-s3-demo-bucket",
  "LastFailureMessage": "test message",
  "LastFailureTime": "2020-08-09T13:00:00.000Z",
  "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
  "LoggingEnabled": true,
  "S3KeyPrefix": "/"
},
"MaintenanceTrackName": "current",
"ManualSnapshotRetentionPeriod": -1,
"MasterUsername": "awsuser",
"NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
"NodeType": "dc2.large",
"NumberOfNodes": 2,
"PendingActions": [],
"PendingModifiedValues": {
  "AutomatedSnapshotRetentionPeriod": 0,
  "ClusterIdentifier": "clusterIdentifier",
  "ClusterType": "clusterType",
  "ClusterVersion": "clusterVersion",
  "EncryptionType": "None",
  "EnhancedVpcRouting": false,
  "MaintenanceTrackName": "maintenanceTrackName",
  "MasterUserPassword": "masterUserPassword",
  "NodeType": "dc2.large",
  "NumberOfNodes": 1,
  "PubliclyAccessible": true
},
"PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
"PubliclyAccessible": true,
"ResizeInfo": {
  "AllowCancelResize": true,

```

```

    "ResizeType": "ClassicResize"
  },
  "RestoreStatus": {
    "CurrentRestoreRateInMegaBytesPerSecond": 15,
    "ElapsedTimeInSeconds": 120,
    "EstimatedTimeToCompletionInSeconds": 100,
    "ProgressInMegaBytes": 10,
    "SnapshotSizeInMegaBytes": 1500,
    "Status": "restoring"
  },
  "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
  "SnapshotScheduleState": "ACTIVE",
  "VpcId": "vpc-example",
  "VpcSecurityGroups": [
    {
      "Status": "active",
      "VpcSecurityGroupId": "sg-example"
    }
  ]
}

```

AwsRoute53 ASFF 中的 資源

以下是 AwsRoute53 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsRoute53HostedZone

AwsRoute53HostedZone 物件提供有關 Amazon Route 53 託管區域的資訊，包括指派給託管區域的四個名稱伺服器。託管區域代表可一起管理的記錄集合，屬於單一父系網域名稱。

下列範例顯示 AwsRoute53HostedZone 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsRoute53HostedZone屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsRoute53HostedZoneDetails](#)。

範例

```

"AwsRoute53HostedZone": {
  "HostedZone": {
    "Id": "Z06419652JEMG09TA2XKL",
    "Name": "asff.testing",

```

```
    "Config": {
      "Comment": "This is an example comment."
    },
    "NameServers": [
      "ns-470.awsdns-32.net",
      "ns-1220.awsdns-12.org",
      "ns-205.awsdns-13.com",
      "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
      "CloudWatchLogsLogGroupArn": {
        "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-group:asfftesting:*",
        "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "HostedZoneId": "Z00932193AF5H180PPNZD"
      }
    },
    "Vpcs": [
      {
        "Id": "vpc-05d7c6e36bc03ea76",
        "Region": "us-east-1"
      }
    ]
  }
}
```

AwsS3 ASFF 中的 資源

以下是 AwsS3 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsS3AccessPoint

AwsS3AccessPoint 提供 Amazon S3 存取點的相關資訊。S3 存取點是連接至 S3 儲存貯體的具名網路端點，可用來執行 S3 物件操作。

下列範例顯示 AwsS3AccessPoint 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsS3AccessPoint屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsS3AccessPointDetails](#)。

範例

```
"AwsS3AccessPoint": {
  "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-point",
  "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
  "Bucket": "amzn-s3-demo-bucket",
  "BucketAccountId": "123456789012",
  "Name": "asff-access-point",
  "NetworkOrigin": "VPC",
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": true,
    "RestrictPublicBuckets": true
  },
  "VpcConfiguration": {
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
  }
}
```

AwsS3AccountPublicAccessBlock

AwsS3AccountPublicAccessBlock 提供帳戶 Amazon S3 公有存取區塊組態的相關資訊。

下列範例顯示 AwsS3AccountPublicAccessBlock 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsS3AccountPublicAccessBlock屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsS3AccountPublicAccessBlockDetails](#)。

範例

```
"AwsS3AccountPublicAccessBlock": {
  "BlockPublicAcls": true,
  "BlockPublicPolicy": true,
  "IgnorePublicAcls": false,
  "RestrictPublicBuckets": true
}
```

AwsS3Bucket

AwsS3Bucket 物件提供 Amazon S3 儲存貯體的詳細資訊。

下列範例顯示 AwsS3Bucket 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsS3Bucket屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsS3BucketDetails](#)。

範例

```

"AwsS3Bucket": {
  "AccessControlList": "{ \"grantSet\": null, \"grantList\": [ { \"grantee\": { \"id\": \"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\", \"displayName\": null }, \"permission\": \"FullControl\" }, { \"grantee\": \"AllUsers\", \"permission\": \"ReadAcp\" }, { \"grantee\": \"AuthenticatedUsers\", \"permission\": \"ReadAcp\" } ], ,
  \"BucketLifecycleConfiguration\": {
    \"Rules\": [
      {
        \"AbortIncompleteMultipartUpload\": {
          \"DaysAfterInitiation\": 5
        },
        \"ExpirationDate\": \"2021-11-10T00:00:00.000Z\",
        \"ExpirationInDays\": 365,
        \"ExpiredObjectDeleteMarker\": false,
        \"Filter\": {
          \"Predicate\": {
            \"Operands\": [
              {
                \"Prefix\": \"tmp/\",
                \"Type\": \"LifecyclePrefixPredicate\"
              },
              {
                \"Tag\": {
                  \"Key\": \"ArchiveAge\",
                  \"Value\": \"9m\"
                },
                \"Type\": \"LifecycleTagPredicate\"
              }
            ],
            \"Type\": \"LifecycleAndOperator\"
          }
        },
        \"ID\": \"Move rotated logs to Glacier\",
        \"NoncurrentVersionExpirationInDays\": -1,
        \"NoncurrentVersionTransitions\": [
          {
            \"Days\": 2,
            \"StorageClass\": \"GLACIER\"
          }
        ],
        \"Prefix\": \"rotated/\",
        \"Status\": \"Enabled\",

```

```

        "Transitions": [
            {
                "Date": "2020-11-10T00:00:00.000Z",
                "Days": 100,
                "StorageClass": "GLACIER"
            }
        ]
    },
    ],
    "BucketLoggingConfiguration": {
        "DestinationBucketName": "s3serversideloggingbucket-123456789012",
        "LogFilePrefix": "buckettestreadwrite23435/"
    },
    "BucketName": "amzn-s3-demo-bucket",
    "BucketNotificationConfiguration": {
        "Configurations": [{
            "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
            "Events": [
                "s3:ObjectCreated:Put"
            ],
            "Filter": {
                "S3KeyFilter": {
                    "FilterRules": [
                        {
                            "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
                            "Value": "pre"
                        },
                        {
                            "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
                            "Value": "suf"
                        }
                    ]
                }
            },
            "Type": "LambdaConfiguration"
        }]
    },
    "BucketVersioningConfiguration": {
        "IsMfaDeleteEnabled": true,
        "Status": "Off"
    },
    "BucketWebsiteConfiguration": {
        "ErrorDocument": "error.html",

```



```
"IndexDocumentSuffix": "index.html",
"RedirectAllRequestsTo": {
  "HostName": "example.com",
  "Protocol": "http"
},
"RoutingRules": [{
  "Condition": {
    "HttpErrorCodeReturnedEquals": "Redirected",
    "KeyPrefixEquals": "index"
  },
  "Redirect": {
    "HostName": "example.com",
    "HttpRedirectCode": "401",
    "Protocol": "HTTP",
    "ReplaceKeyPrefixWith": "string",
    "ReplaceKeyWith": "string"
  }
}]
},
"CreatedAt": "2007-11-30T01:46:56.000Z",
"ObjectLockConfiguration": {
  "ObjectLockEnabled": "Enabled",
  "Rule": {
    "DefaultRetention": {
      "Days": null,
      "Mode": "GOVERNANCE",
      "Years": 12
    }
  },
},
},
"OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
"OwnerName": "s3bucketowner",
"PublicAccessBlockConfiguration": {
  "BlockPublicAcls": true,
  "BlockPublicPolicy": true,
  "IgnorePublicAcls": true,
  "RestrictPublicBuckets": true,
},
"ServerSideEncryptionConfiguration": {
  "Rules": [
    {
      "ApplyServerSideEncryptionByDefault": {
        "SSEAlgorithm": "AES256",
        "KMSEMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
```

```

    }
  }
}
}
}

```

AwsS3Object

AwsS3Object 物件提供 Amazon S3 物件的相關資訊。

下列範例顯示 AwsS3Object 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsS3Object屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsS3ObjectDetails](#)。

範例

```

"AwsS3Object": {
  "ContentType": "text/html",
  "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
  "LastModified": "2012-04-23T18:25:43.511Z",
  "ServerSideEncryption": "aws:kms",
  "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-a9a0-608ec069e5a7",
  "VersionId": "ws310urg00jH_HH1lIxPE35P.MELYaYh"
}

```

AwsSageMaker ASFF 中的 資源

以下是 AwsSageMaker 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsSageMakerNotebookInstance

AwsSageMakerNotebookInstance 物件提供有關 Amazon SageMaker AI 筆記本執行個體的資訊，這是執行 Jupyter 筆記本應用程式的機器學習運算執行個體。

下列範例顯示 AwsSageMakerNotebookInstance 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsSageMakerNotebookInstance屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsSageMakerNotebookInstanceDetails](#)。

範例

```

"AwsSageMakerNotebookInstance": {
  "DirectInternetAccess": "Disabled",
  "InstanceMetadataServiceConfiguration": {
    "MinimumInstanceMetadataServiceVersion": "1",
  },
  "InstanceType": "ml.t2.medium",
  "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
  "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
  "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
  "NotebookInstanceName":
  "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
  "NotebookInstanceStatus": "InService",
  "PlatformIdentifier": "notebook-all-v1",
  "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-SageMakerCustomExecution-1R0X32HGC38IW",
  "RootAccess": "Disabled",
  "SecurityGroups": [
    "sg-06b347359ab068745"
  ],
  "SubnetId": "subnet-02c0deea5fa64578e",
  "Url":
  "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-east-1.sagemaker.aws",
  "VolumeSizeInGB": 5
}

```

AwsSecretsManager ASFF 中的 資源

以下是 AwsSecretsManager 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsSecretsManagerSecret

AwsSecretsManagerSecret 物件提供 Secrets Manager 秘密的詳細資訊。

下列範例顯示 AwsSecretsManagerSecret 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 AwsSecretsManagerSecret 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsSecretsManagerSecretDetails](#)。

範例

```
"AwsSecretsManagerSecret": {
  "RotationRules": {
    "AutomaticallyAfterDays": 30
  },
  "RotationOccurredWithinFrequency": true,
  "KmsKeyId": "kmsKeyId",
  "RotationEnabled": true,
  "RotationLambdaArn": "arn:aws:lambda:us-west-2:777788889999:function:MyTestRotationLambda",
  "Deleted": false,
  "Name": "MyTestDatabaseSecret",
  "Description": "My test database secret"
}
```

AwsSns ASFF 中的 資源

以下是 AwsSns 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsSnsTopic

AwsSnsTopic 物件包含 Amazon Simple Notification Service 主題的詳細資訊。

下列範例顯示 AwsSnsTopic 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsSnsTopic屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsSnsTopicDetails](#)。

範例

```
"AwsSnsTopic": {
  "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/ApplicationSuccessFeedbackRoleArn",
  "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/FirehoseFailureFeedbackRoleArn",
  "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/FirehoseSuccessFeedbackRoleArn",
  "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/HttpFailureFeedbackRoleArn",
  "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/HttpSuccessFeedbackRoleArn",
  "KmsMasterKeyId": "alias/ExampleAlias",
```

```
"Owner": "123456789012",
"SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
"SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
"Subscription": {
  "Endpoint": "http://sampleendpoint.com",
  "Protocol": "http"
},
"TopicName": "SampleTopic"
}
```

AwsSqs ASFF 中的 資源

以下是 AwsSqs 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsSqsQueue

AwsSqsQueue 物件包含 Amazon Simple Queue Service 佇列的相關資訊。

下列範例顯示 AwsSqsQueue 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsSqsQueue屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsSqsQueueDetails](#)。

範例

```
"AwsSqsQueue": {
  "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
  "KmsDataKeyReusePeriodSeconds": 60,,
  "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "QueueName": "sample-queue"
}
```

AwsSsm ASFF 中的 資源

以下是 AwsSsm 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsSsmPatchCompliance

AwsSsmPatchCompliance 物件會根據用來修補執行個體的修補程式基準，提供執行個體上修補程式狀態的相關資訊。

下列範例顯示 AwsSsmPatchCompliance 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsSsmPatchCompliance屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsSsmPatchComplianceDetails](#)。

範例

```
"AwsSsmPatchCompliance": {
  "Patch": {
    "ComplianceSummary": {
      "ComplianceType": "Patch",
      "CompliantCriticalCount": 0,
      "CompliantHighCount": 0,
      "CompliantInformationalCount": 0,
      "CompliantLowCount": 0,
      "CompliantMediumCount": 0,
      "CompliantUnspecifiedCount": 461,
      "ExecutionType": "Command",
      "NonCompliantCriticalCount": 0,
      "NonCompliantHighCount": 0,
      "NonCompliantInformationalCount": 0,
      "NonCompliantLowCount": 0,
      "NonCompliantMediumCount": 0,
      "NonCompliantUnspecifiedCount": 0,
      "OverallSeverity": "UNSPECIFIED",
      "PatchBaselineId": "pb-0c5b2769ef7cbe587",
      "PatchGroup": "ExamplePatchGroup",
      "Status": "COMPLIANT"
    }
  }
}
```

AwsStepFunctions ASFF 中的 資源

以下是 AwsStepFunctions 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsStepFunctionStateMachine

AwsStepFunctionStateMachine 物件提供有關 AWS Step Functions 狀態機器的資訊，這是由一系列事件驅動步驟組成的工作流程。

下列範例顯示 AwsStepFunctionStateMachine 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsStepFunctionStateMachine屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsStepFunctionStateMachine](#)。

範例

```
"AwsStepFunctionStateMachine": {
  "StateMachineArn": "arn:aws:states:us-east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
  "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
  "Status": "ACTIVE",
  "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-StatesExecutionRole-1PNM71RV01UKT",
  "Type": "STANDARD",
  "LoggingConfiguration": {
    "Level": "OFF",
    "IncludeExecutionData": false
  },
  "TracingConfiguration": {
    "Enabled": false
  }
}
```

AwsWaf ASFF 中的 資源

以下是 AwsWaf 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsWafRateBasedRule

AwsWafRateBasedRule 物件包含全域 AWS WAF 資源的速率型規則詳細資訊。以 AWS WAF 速率為基礎的規則提供設定，指出何時允許、封鎖或計數請求。以速率為基礎的規則包括在指定期間內到達的請求數量。

下列範例顯示 `AwsWafRateBasedRule` 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 `AwsWafRateBasedRule` 屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsWafRateBasedRuleDetails](#)。

範例

```
"AwsWafRateBasedRule":{
  "MatchPredicates" : [{
    "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
    "Negated" : "True",
    "Type" : "IPMatch" ,
  }],
  "MetricName" : "MetricName",
  "Name" : "Test",
  "RateKey" : "IP",
  "RateLimit" : 235000,
  "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRateBasedRule

`AwsWafRegionalRateBasedRule` 物件包含區域資源的速率型規則詳細資訊。以速率為基礎的規則提供設定，指出何時允許、封鎖或計數請求。以速率為基礎的規則包括在指定期間內到達的請求數量。

下列範例顯示 `AwsWafRegionalRateBasedRule` 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視 `AwsWafRegionalRateBasedRule` 屬性的說明，請參閱 AWS Security Hub API 參考中的 [AwsWafRegionalRateBasedRuleDetails](#)。

範例

```
"AwsWafRegionalRateBasedRule":{
  "MatchPredicates" : [{
    "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
    "Negated" : "True",
    "Type" : "IPMatch" ,
  }],
  "MetricName" : "MetricName",
  "Name" : "Test",
  "RateKey" : "IP",
  "RateLimit" : 235000,
  "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```


AwsWafRegionalRule

AwsWafRegionalRule 物件提供有關 AWS WAF 區域性規則 的詳細資訊。此規則會識別您要允許、封鎖或計數的 Web 請求。

下列範例顯示 AwsWafRegionalRule 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsWafRegionalRule屬性的說明，請參閱 AWS Security Hub API 參考中的 [AwsWafRegionalRuleDetails](#)。

範例

```
"AwsWafRegionalRule": {
  "MetricName": "SampleWAF_Rule__Metric_1",
  "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
  "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
  "PredicateList": [{
    "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
    "Negated": false,
    "Type": "GeoMatch"
  }]
}
```

AwsWafRegionalRuleGroup

AwsWafRegionalRuleGroup 物件提供區域性規則群組的詳細資訊 AWS WAF 。規則群組是您新增至 Web 存取控制清單 (Web ACL) 的預先定義規則集合。

下列範例顯示 AwsWafRegionalRuleGroup 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsWafRegionalRuleGroup屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsWafRegionalRuleGroupDetails](#)。

範例

```
"AwsWafRegionalRuleGroup": {
  "MetricName": "SampleWAF_Metric_1",
  "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
  "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
  "Rules": [{
    "Action": {
      "Type": "ALLOW"
    }
  ]},
}
```

```

    "Priority": 1,
    "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
    "Type": "REGULAR"
}

```

AwsWafRegionalWebAcl

AwsWafRegionalWebAcl 提供有關 AWS WAF 區域 Web 存取控制清單 (Web ACL) 的詳細資訊。Web ACL 包含規則，可識別您要允許、封鎖或計數的請求。

以下是安全AwsWafRegionalWebAcl調查結果格式 AWS (ASFF) 中的範例調查結果。若要檢視AwsApiGatewayV2Stage屬性的說明，請參閱 AWS Security Hub API 參考中的 [AwsWafRegionalWebAclDetails](#)。

範例

```

"AwsWafRegionalWebAcl": {
  "DefaultAction": "ALLOW",
  "MetricName" : "web-regional-webacl-metric-1",
  "Name": "WebACL_123",
  "RulesList": [
    {
      "Action": {
        "Type": "Block"
      },
      "Priority": 3,
      "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
      "Type": "REGULAR",
      "ExcludedRules": [
        {
          "ExclusionType": "Exclusion",
          "RuleId": "Rule_id_1"
        }
      ],
      "OverrideAction": {
        "Type": "OVERRIDE"
      }
    }
  ],
  "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}

```

AwsWafRule

AwsWafRule 提供 AWS WAF 規則的相關資訊。AWS WAF 規則會識別您要允許、封鎖或計數的 Web 請求。

以下是 AWS 安全AwsWafRule調查結果格式 (ASFF) 中的範例調查結果。若要檢視AwsApiGatewayV2Stage屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsWafRuleDetails](#)。

範例

```
"AwsWafRule": {
  "MetricName": "AwsWafRule_Metric_1",
  "Name": "AwsWafRule_Name_1",
  "PredicateList": [{
    "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
    "Negated": false,
    "Type": "GeoMatch"
  }],
  "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

AwsWafRuleGroup 提供 AWS WAF 規則群組的相關資訊。規則群組是您新增至 Web AWS WAF 存取控制清單 (Web ACL) 的預先定義規則集合。

以下是 AWS 安全AwsWafRuleGroup調查結果格式 (ASFF) 中的範例調查結果。若要檢視AwsApiGatewayV2Stage屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsWafRuleGroupDetails](#)。

範例

```
"AwsWafRuleGroup": {
  "MetricName": "SampleWAF_Metric_1",
  "Name": "bb-WAFRuleGroupWithRuleCompliant",
  "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
  "Rules": [{
    "Action": {
      "Type": "ALLOW",
    },
  ]
}
```

```
    "Priority": 1,  
    "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",  
    "Type": "REGULAR"  
  }]  
}
```

AwsWafv2RuleGroup

AwsWafv2RuleGroup 物件提供有關 an AWS WAF V2 規則群組的詳細資訊。

下列範例顯示 AwsWafv2RuleGroup 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsWafv2RuleGroup屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsWafv2RuleGroupDetails](#)。

範例

```
"AwsWafv2RuleGroup": {  
  "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",  
  "Capacity": 1000,  
  "Description": "Resource for ASFF",  
  "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",  
  "Name": "wafv2rulegroupasff",  
  "Rules": [{  
    "Action": {  
      "Allow": {  
        "CustomRequestHandling": {  
          "InsertHeaders": [  
            {  
              "Name": "AllowActionHeader1Name",  
              "Value": "AllowActionHeader1Value"  
            },  
            {  
              "Name": "AllowActionHeader2Name",  
              "Value": "AllowActionHeader2Value"  
            }  
          ]  
        }  
      }  
    },  
    "Name": "RuleOne",  
    "Priority": 1,  
    "VisibilityConfig": {  
      "CloudWatchMetricsEnabled": true,  

```

```
    "MetricName": "rulegroupasff",
    "SampledRequestsEnabled": false
  }
}],
"VisibilityConfig": {
  "CloudWatchMetricsEnabled": true,
  "MetricName": "rulegroupasff",
  "SampledRequestsEnabled": false
}
}
```

AwsWafWebAcl

AwsWafWebAcl 物件提供 AWS WAF Web ACL 的詳細資訊。

下列範例顯示 AwsWafWebAcl 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsWafWebAcl屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsWafWebAclDetails](#)。

範例

```
"AwsWafWebAcl": {
  "DefaultAction": "ALLOW",
  "Name": "MyWafAcl",
  "Rules": [
    {
      "Action": {
        "Type": "ALLOW"
      },
      "ExcludedRules": [
        {
          "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
        }
      ],
      "OverrideAction": {
        "Type": "NONE"
      },
      "Priority": 1,
      "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
      "Type": "REGULAR"
    }
  ],
  "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

AwsWafv2WebAcl 物件提供 an AWS WAF V2 Web ACL 的詳細資訊。

下列範例顯示 AwsWafv2WebAcl 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsWafv2WebAcl屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsWafv2WebAclDetails](#)。

範例

```
"AwsWafv2WebAcl": {
  "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Capacity": 1326,
  "CaptchaConfig": {
    "ImmunityTimeProperty": {
      "ImmunityTime": 500
    }
  },
  "DefaultAction": {
    "Block": {}
  },
  "Description": "Web ACL for JsonBody testing",
  "ManagedbyFirewallManager": false,
  "Name": "WebACL-RoaD4QexqSxG",
  "Rules": [{
    "Action": {
      "RuleAction": {
        "Block": {}
      }
    },
    "Name": "TestJsonBodyRule",
    "Priority": 1,
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
    }
  }],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "TestingJsonBodyMetric"
  }
}
```

```
}
```

AwsXray ASFF 中的 資源

以下是 AwsXray 資源 AWS 的安全調查結果格式 (ASFF) 語法範例。

AWS Security Hub CSPM 將各種來源的問題清單標準化為 ASFF。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

AwsXrayEncryptionConfig

AwsXrayEncryptionConfig 物件包含 加密組態的相關資訊 AWS X-Ray。

下列範例顯示 AwsXrayEncryptionConfig 物件 AWS 的安全調查結果格式 (ASFF)。若要檢視AwsXrayEncryptionConfig屬性的描述，請參閱 AWS Security Hub API 參考中的 [AwsXrayEncryptionConfigDetails](#)。

範例

```
"AwsXRayEncryptionConfig": {
  "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
  "Status": "UPDATING",
  "Type": "KMS"
}
```

CodeRepository ASFF 中的 物件

CodeRepository 物件提供連線至 AWS 資源的外部程式碼儲存庫相關資訊，並設定 Amazon Inspector 掃描漏洞。

下列範例顯示 CodeRepository 物件 AWS 的安全調查結果格式 (ASFF) 語法。若要檢視CodeRepository屬性的描述，請參閱 AWS Security Hub API 參考中的 [CodeRepositoryDetails](#)。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

範例

```
"CodeRepository": {
  "ProviderType": "GITLAB_SELF_MANAGED",
  "ProjectName": "projectName",
  "CodeSecurityIntegrationArn": "arn:aws:inspector2:us-east-1:123456789012:codesecurity-integration/00000000-0000-0000-0000-000000000000"
}
```

Container ASFF 中的 物件

下列範例顯示 Container 物件 AWS 的安全調查結果格式 (ASFF) 語法。若要檢視 Container 屬性的描述，請參閱 AWS Security Hub API 參考中的 [ContainerDetails](#)。如需 ASFF 的背景資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

範例

```
"Container": {
  "ContainerRuntime": "docker",
  "ImageId": "image12",
  "ImageName": "11111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "Name": "knote",
  "Privileged": true,
  "VolumeMounts": [{
    "Name": "vol-03909e9",
    "MountPath": "/mnt/etc"
  }]
}
```

Other ASFF 中的 物件

在 AWS 安全調查結果格式 (ASFF) 中，Other 物件會指定自訂欄位和值。如需 ASFF 的詳細資訊，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

透過使用 Other 物件，您可以指定資源的自訂欄位和值。您可以針對下列案例使用 Other 物件：

- 資源類型沒有對應的 Details 物件。若要指定資源的詳細資訊，請使用 Other 物件。
- 資源類型的 Details 物件不包含您要指定的所有屬性。在此情況下，請使用資源類型的 Details 物件來指定可用的屬性。使用 Other 物件來指定不在類型特定 Details 物件中的屬性。
- 資源類型不是提供的類型之一。在此情況下，將 Resource.Type 設定為 Other 並使用 Other 物件來指定詳細資訊。

類型：最多 50 個鍵值對的映射

每個鍵/值對必須符合下列需求。

- 金鑰必須包含少於 128 個字元。

- 此值必須包含少於 1,024 個字元。

在 Security Hub CSPM 中檢視洞見

在 AWS Security Hub CSPM 中，洞見是相關調查結果的集合。洞見可以識別需要注意和介入的特定安全區域。舉例來說，洞見可能會指出 EC2 執行個體是偵測到不良安全實務的問題清單主體。洞見結合了各問題清單提供者的問題清單。

每個洞見都會根據 group by 陳述式和選用篩選條件定義。group by 陳述式會指出如何將相符的問題清單分組，並識別套用洞見的項目類型。舉例來說，如果洞見根據資源識別符分組，則洞見會產生資源識別符的清單。選用篩選條件會識別洞見的相符調查結果。例如，您可能只想查看特定提供者的問題清單或與特定類型資源相關聯的問題清單。

Security Hub CSPM 提供數個內建的受管洞察。您無法修改或刪除受管洞察。若要追蹤您 AWS 環境和用量特有的安全問題，您可以建立自訂洞見。

AWS Security Hub CSPM 主控台上的 Insights 頁面會顯示可用的洞見清單。

根據預設，清單會顯示受管和自訂洞見。若要根據洞見類型篩選洞見清單，請從篩選欄位旁的下拉式功能表中選擇洞見類型。

- 若要顯示所有可用的洞見，請選擇所有洞見。此為預設選項。
- 若要僅顯示受管洞見，請選擇 Security Hub CSPM 受管洞見。
- 若要僅顯示自訂洞見，請選擇自訂洞見。

您也可以根據洞見的名稱來篩選洞見清單。若要這樣做，請在篩選欄位中，輸入用來篩選清單的文字。篩選條件不區分大小寫。篩選條件會尋找洞見，其中包含洞見名稱中任何位置的文字。

只有當您已啟用產生相符調查結果的整合或標準時，洞見才會傳回結果。例如，受管洞見 29。如果啟用網際網路安全中心 (CIS) AWS Foundations Benchmark 標準的版本，則依失敗 CIS 檢查計數排序的熱門資源只會傳回結果。

在 Security Hub CSPM 中檢閱洞見並採取行動

對於每個洞見，AWS Security Hub CSPM 會先決定符合篩選條件的問題清單，然後使用分組屬性將相符的問題清單分組。

在主控台的 Insights 頁面中，您可以檢視結果和調查結果並對其採取動作。

如果您啟用跨區域彙總，受管洞察的結果（當您登入彙總區域時）會包含來自彙總區域和連結區域的調查結果。如果洞見未依區域篩選，則自訂洞見的結果也會包含來自彙總區域和連結區域的調查結果（當您登入彙總區域時）。在其他區域中，洞見結果僅適用於該區域。

如需設定跨區域彙總的資訊，請參閱 [the section called “跨區域彙總資料”](#)。

檢視洞見結果並採取行動

洞見結果由洞見結果的分組清單組成。例如，如果洞見依資源識別符分組，洞見結果即為資源識別符的清單。結果清單中的每個項目都會指出該項目符合的問題清單數。

如果問題清單依資源識別符或資源類型分組，則結果會包含相符問題清單中的所有資源。這包括與篩選條件中指定的資源類型具有不同類型的資源。例如，洞見可識別與 S3 儲存貯體相關聯的調查結果。如果相符的調查結果同時包含 S3 儲存貯體資源和 IAM 存取金鑰資源，則洞見結果會同時包含這兩個資源。

在 Security Hub CSPM 主控台上，結果清單會從最相符的調查結果排序到最少。Security Hub CSPM 只能顯示 100 個結果。如果超過 100 個分組值，您只會看到前 100 個。

除了結果清單之外，洞見結果還會顯示一組圖表，摘要下列屬性的相符問題清單數。

- 嚴重性標籤 – 每個嚴重性標籤的問題清單數量
- AWS 帳戶 ID – 相符問題清單的前五個帳戶 IDs
- 資源類型 – 比對問題清單的前五個資源類型
- 資源 ID – 相符問題清單的前五個資源 IDs
- 產品名稱 - 相符調查結果的前五個調查結果提供者

若您已設定自訂動作，即可將選取的結果傳送到自訂動作。動作必須與 Security Hub Insight Results 事件類型的 Amazon CloudWatch 規則相關聯。如需詳細資訊，請參閱 [the section called “自動化回應和修復”](#)。如果您尚未設定自訂動作，則會停用動作功能表。

Security Hub CSPM console

檢視洞見結果並採取動作（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇 Insights。
3. 若要顯示洞見結果的清單，請選擇洞見名稱。

4. 選取各個結果的核取方塊，並傳送到自訂動作。
5. 從 Actions (動作) 選單選擇自訂動作。

Security Hub CSPM API, AWS CLI

檢視洞見結果並採取動作 (API) AWS CLI

若要檢視洞見結果，請使用 Security Hub CSPM API [GetInsightResults](#) 的操作。如果您使用 AWS CLI，請執行 [get-insight-results](#) 命令。

若要識別要傳回結果的洞見，您需要洞見 ARN。若要取得自訂洞見 ARNs，請使用 [GetInsights](#) API 操作或 [get-insight-results](#) 命令。

下列範例會擷取指定洞見的結果。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

如需如何以程式設計方式建立自訂動作的詳細資訊，請參閱 [使用自訂動作將問題清單和洞見結果傳送至 EventBridge](#)。

檢視洞見結果調查結果並對其採取行動 (主控台)

從 Security Hub CSPM 主控台上的洞見結果清單中，您可以顯示每個結果的調查結果清單。

顯示洞見調查結果並對其採取動作 (主控台)

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇 Insights。
3. 若要顯示洞見結果的清單，請選擇洞見名稱。
4. 若要顯示洞見結果的問題清單，請從結果清單選擇項目。問題清單會顯示工作流程狀態為 NEW 或 NOTIFIED 選取洞見結果的作用中問題清單。

從調查結果清單中，您可以執行下列動作：

- [在 Security Hub CSPM 中篩選問題清單](#)
- [檢閱問題清單詳細資訊和歷史記錄](#)
- [在 Security Hub CSPM 中設定問題清單的工作流程狀態](#)
- [將問題清單傳送至自訂 Security Hub CSPM 動作](#)

Security Hub CSPM 中的受管洞察

AWS Security Hub CSPM 提供數個受管洞察。

您無法編輯或刪除 Security Hub CSPM 受管洞察。您可以[檢視並對洞見結果和問題清單採取動作](#)。您也可以[使用受管洞見做為新自訂洞見的基礎](#)。

如同所有洞見，如果您有啟用的產品整合或可產生相符問題清單的安全標準，則受管洞見只會傳回結果。

對於依資源識別符分組的洞見，結果會包含相符調查結果中所有資源的識別符。這包括與篩選條件中的資源類型具有不同類型的資源。例如，以下清單中的洞見 2 可識別與 Amazon S3 儲存貯體相關聯的調查結果。如果相符的調查結果同時包含 S3 儲存貯體資源和 IAM 存取金鑰資源，則洞見結果會同時包含這兩個資源。

Security Hub CSPM 目前提供下列受管洞察：

問題清單最多的 1. AWS resources

ARN : `arn:aws:securityhub:::insight/securityhub/default/1`

分組依據：資源識別符

尋找篩選條件：

- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

2. 具有公有寫入或讀取許可的 S3 儲存貯體

ARN : `arn:aws:securityhub:::insight/securityhub/default/10`

分組依據：資源識別符

尋找篩選條件：

- 類型開頭為 Effects/Data Exposure

- 資源類型為 `AwsS3Bucket`
- 記錄狀態為 `ACTIVE`
- 工作流程狀態為 `NEW` 或 `NOTIFIED`

3. 產生最多問題清單的 AMI

ARN : `arn:aws:securityhub:::insight/securityhub/default/3`

分組依據：EC2 執行個體映像 ID

尋找篩選條件：

- 資源類型為 `AwsEc2Instance`
- 記錄狀態為 `ACTIVE`
- 工作流程狀態為 `NEW` 或 `NOTIFIED`

4. 有關已知戰術、技術和程序 (TTP) 的 EC2 執行個體

ARN : `arn:aws:securityhub:::insight/securityhub/default/14`

分組依據：資源 ID

尋找篩選條件：

- 類型開頭為 `TTPs`
- 資源類型為 `AwsEc2Instance`
- 記錄狀態為 `ACTIVE`
- 工作流程狀態為 `NEW` 或 `NOTIFIED`

具有可疑存取金鑰活動的 5. AWS principals

ARN : `arn:aws:securityhub:::insight/securityhub/default/9`

分組依據：IAM 存取金鑰主體名稱

尋找篩選條件：

- 資源類型為 `AwsIamAccessKey`
- 記錄狀態為 `ACTIVE`
- 工作流程狀態為 `NEW` 或 `NOTIFIED`

6. AWS 資源不符合安全標準/最佳實務的執行個體

ARN : `arn:aws:securityhub:::insight/securityhub/default/6`

分組依據：資源 ID

尋找篩選條件：

- 類型為 Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

7. 與潛在資料外洩相關聯的 AWS 資源

ARN : `arn:aws:securityhub:::insight/securityhub/default/7`

分組依據：資源 ID

尋找篩選條件：

- 類型開頭為 Effects/Data Exfiltration/
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

8. 與未經授權資源耗用 AWS 相關聯的資源

ARN : `arn:aws:securityhub:::insight/securityhub/default/8`

分組依據：資源 ID

尋找篩選條件：

- 類型開頭為 Effects/Resource Consumption
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

9. 不符合安全標準/最佳實務的 S3 儲存貯體

ARN : `arn:aws:securityhub:::insight/securityhub/default/11`

分組依據：資源 ID

尋找篩選條件：

- 資源類型為 AwsS3Bucket
- 類型為 Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices

- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

10. 具有敏感資料的 S3 儲存貯體

ARN : `arn:aws:securityhub:::insight/securityhub/default/12`

分組依據：資源 ID

尋找篩選條件：

- 資源類型為 `AwsS3Bucket`
- 類型開頭為 `Sensitive Data Identifications/`
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

11. 登入資料可能已洩漏

ARN : `arn:aws:securityhub:::insight/securityhub/default/13`

分組依據：資源 ID

尋找篩選條件：

- 類型開頭為 `Sensitive Data Identifications/Passwords/`
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

12. 缺少重要漏洞安全性修補程式的 EC2 執行個體

ARN : `arn:aws:securityhub:::insight/securityhub/default/16`

分組依據：資源 ID

尋找篩選條件：

- 類型開頭為 `Software and Configuration Checks/Vulnerabilities/CVE`
- 資源類型為 `AwsEc2Instance`
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

13. 具有一般異常行為的 EC2 執行個體

ARN : `arn:aws:securityhub:::insight/securityhub/default/17`

分組依據：資源 ID

尋找篩選條件：

- 類型開頭為 Unusual Behaviors
- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

14. 具有可從網際網路存取連接埠的 EC2 執行個體

ARN : `arn:aws:securityhub:::insight/securityhub/default/18`

分組依據：資源 ID

尋找篩選條件：

- 類型開頭為 Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

15. 不符合安全標準或最佳實務的 EC2 執行個體

ARN : `arn:aws:securityhub:::insight/securityhub/default/19`

分組依據：資源 ID

尋找篩選條件：

- 類型以下列其中一個項目開頭：
 - Software and Configuration Checks/Industry and Regulatory Standards/
 - Software and Configuration Checks/AWS Security Best Practices
- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

16. 向網際網路開放的 EC2 執行個體

ARN : `arn:aws:securityhub:::insight/securityhub/default/21`

分組依據：資源 ID

尋找篩選條件：

- 類型開頭為 Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

17. 與對手偵察相關聯的 EC2 執行個體

ARN : arn:aws:securityhub:::insight/securityhub/default/22

分組依據：資源 ID

尋找篩選條件：

- 類型以 TTPs/Discovery/Recon 開頭
- 資源類型為 AwsEc2Instance
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

與惡意軟體相關聯的 18. AWS resources

ARN : arn:aws:securityhub:::insight/securityhub/default/23

分組依據：資源 ID

尋找篩選條件：

- 類型以下列其中一個項目開頭：
 - Effects/Data Exfiltration/Trojan
 - TTPs/Initial Access/Trojan
 - TTPs/Command and Control/Backdoor
 - TTPs/Command and Control/Trojan
 - Software and Configuration Checks/Backdoor
 - Unusual Behaviors/VM/Backdoor
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

19. AWS 與加密貨幣問題相關聯的資源

ARN : `arn:aws:securityhub:::insight/securityhub/default/24`

分組依據：資源 ID

尋找篩選條件：

- 類型以下列其中一個項目開頭：
 - `Effects/Resource Consumption/Cryptocurrency`
 - `TTPs/Command and Control/CryptoCurrency`
- 記錄狀態為 `ACTIVE`
- 工作流程狀態為 `NEW` 或 `NOTIFIED`

具有未經授權存取嘗試的 20. AWS resources

ARN : `arn:aws:securityhub:::insight/securityhub/default/25`

分組依據：資源 ID

尋找篩選條件：

- 類型以下列其中一個項目開頭：
 - `TTPs/Command and Control/UnauthorizedAccess`
 - `TTPs/Initial Access/UnauthorizedAccess`
 - `Effects/Data Exfiltration/UnauthorizedAccess`
 - `Unusual Behaviors/User/UnauthorizedAccess`
 - `Effects/Resource Consumption/UnauthorizedAccess`
- 記錄狀態為 `ACTIVE`
- 工作流程狀態為 `NEW` 或 `NOTIFIED`

21. 過去一週最多命中的威脅 intel 指標

ARN : `arn:aws:securityhub:::insight/securityhub/default/26`

尋找篩選條件：

- 最近 7 天內建立

22. 按問題清單計數排列的熱門帳戶

ARN : `arn:aws:securityhub:::insight/securityhub/default/27`

依：ID 分組 AWS 帳戶

尋找篩選條件：

- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

23. 按問題清單計數排列的熱門產品

ARN : `arn:aws:securityhub:::insight/securityhub/default/28`

分組依據：產品名稱

尋找篩選條件：

- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

24. 按問題清單計數排列的嚴重性

ARN : `arn:aws:securityhub:::insight/securityhub/default/29`

分組依據：嚴重性標籤

尋找篩選條件：

- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

25. 按問題清單計數排列的熱門 S3 儲存貯體

ARN : `arn:aws:securityhub:::insight/securityhub/default/30`

分組依據：資源 ID

尋找篩選條件：

- 資源類型為 `AwsS3Bucket`
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

26. 按問題清單計數排列的熱門 EC2 執行個體

ARN : `arn:aws:securityhub:::insight/securityhub/default/31`

分組依據：資源 ID

尋找篩選條件：

- 資源類型為 `AwsEc2Instance`
- 記錄狀態為 `ACTIVE`
- 工作流程狀態為 `NEW` 或 `NOTIFIED`

27. 按問題清單計數排列的熱門 AMI

ARN : `arn:aws:securityhub:::insight/securityhub/default/32`

分組依據：EC2 執行個體映像 ID

尋找篩選條件：

- 資源類型為 `AwsEc2Instance`
- 記錄狀態為 `ACTIVE`
- 工作流程狀態為 `NEW` 或 `NOTIFIED`

28. 按問題清單計數排列的熱門 IAM 使用者

ARN : `arn:aws:securityhub:::insight/securityhub/default/33`

分組依據：IAM 存取金鑰 ID

尋找篩選條件：

- 資源類型為 `AwsIamAccessKey`
- 記錄狀態為 `ACTIVE`
- 工作流程狀態為 `NEW` 或 `NOTIFIED`

29. 按失敗 CIS 檢查計數排列的熱門資源

ARN : `arn:aws:securityhub:::insight/securityhub/default/34`

分組依據：資源 ID

尋找篩選條件：

- 產生器 ID 開頭為 `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
- 最後一天更新
- 合規狀態為 `FAILED`
- 記錄狀態為 `ACTIVE`

- 工作流程狀態為 NEW 或 NOTIFIED

30. 按問題清單計數排列的熱門整合

ARN : `arn:aws:securityhub:::insight/securityhub/default/35`

分組依據：產品 ARN

尋找篩選條件：

- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

31. 安全檢查失敗次數最多的資源

ARN : `arn:aws:securityhub:::insight/securityhub/default/36`

分組依據：資源 ID

尋找篩選條件：

- 最後一天更新
- 合規狀態為 FAILED
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

32. 具有可疑活動的 IAM 使用者

ARN : `arn:aws:securityhub:::insight/securityhub/default/37`

分組依據：IAM 使用者

尋找篩選條件：

- 資源類型為 `AwsIamUser`
- 記錄狀態為 ACTIVE
- 工作流程狀態為 NEW 或 NOTIFIED

33. 問題 AWS Health 清單最多的資源

ARN : `arn:aws:securityhub:::insight/securityhub/default/38`

分組依據：資源 ID

尋找篩選條件：

- ProductName 等於 Health

34. 問題 AWS Config 清單最多的資源

ARN : arn:aws:securityhub:::insight/securityhub/default/39

分組依據：資源 ID

尋找篩選條件：

- ProductName 等於 Config

35. 問題清單最多的應用程式

ARN : arn:aws:securityhub:::insight/securityhub/default/40

分組依據：ResourceApplicationArn

尋找篩選條件：

- RecordState 等於 ACTIVE
- Workflow.Status 等於 NEW或 NOTIFIED

了解 Security Hub CSPM 中的自訂洞見

除了 AWS Security Hub CSPM 受管洞察之外，您還可以在 Security Hub CSPM 中建立自訂洞察，以追蹤您環境特有的問題。自訂洞見可協助您追蹤精選的問題子集。

以下是一些自訂洞見的範例，可能有助於設定：

- 如果您擁有管理員帳戶，您可以設定自訂洞見來追蹤影響成員帳戶的關鍵和高嚴重性問題清單。
- 如果您依賴特定的[整合 AWS 服務](#)，您可以設定自訂洞見，以追蹤該服務的關鍵和高嚴重性問題清單。
- 如果您依賴[第三方整合](#)，您可以設定自訂洞見，以追蹤該整合產品的關鍵和高嚴重性問題清單。

您可以建立全新的自訂洞見，或從現有的自訂或受管洞見開始。

您可以使用下列選項設定每個洞見：

- 分組屬性 – 分組屬性會決定洞見結果清單中顯示的項目。例如，如果分組屬性是產品名稱，洞見結果會顯示與每個調查結果提供者相關聯的調查結果數量。
- 選用篩選條件 – 篩選條件縮小了洞見的相符調查結果範圍。

只有當問題清單符合所有提供的篩選條件時，問題清單才會包含在洞見結果中。例如，如果篩選條件為「產品名稱為 GuardDuty」且「資源類型為AwsS3Bucket」，則相符的問題清單必須符合這兩個條件。

不過，Security Hub CSPM 會將布林值 OR 邏輯套用至使用相同屬性但不同值的篩選條件。例如，如果篩選條件是「產品名稱為 GuardDuty」和「產品名稱為 Amazon Inspector」，則如果問題清單是由 Amazon GuardDuty 或 Amazon Inspector 產生，則會相符。

如果您使用資源識別符或資源類型做為分組屬性，洞見結果會包含相符調查結果中的所有資源。清單不限於符合資源類型篩選條件的資源。例如，洞見會識別與 S3 儲存貯體相關聯的調查結果，並根據資源識別符將這些調查結果分組。相符的調查結果同時包含 S3 儲存貯體資源和 IAM 存取金鑰資源。洞見結果包含兩個資源。

如果您啟用[跨區域彙總](#)，然後建立自訂洞見，洞見會套用至彙總區域和連結區域中相符的調查結果。例外情況是，如果您的洞見包含區域篩選條件。

建立自訂洞見

在 AWS Security Hub CSPM 中，自訂洞見可用來收集一組特定的問題清單，並追蹤您環境特有的問題。如需自訂洞見的背景資訊，請參閱 [了解 Security Hub CSPM 中的自訂洞見](#)。

選擇您偏好的方法，並依照步驟在 Security Hub CSPM 中建立自訂洞見

Security Hub CSPM console

建立自訂洞見（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇 Insights。
3. 選擇 Create insight (建立洞見)。
4. 選取洞見的分組屬性：
 - a. 選擇搜尋方塊以顯示篩選條件選項。
 - b. 選擇 Group by (分組依據)。
 - c. 選取要用於將與此洞見相關聯的調查結果分組的屬性。
 - d. 選擇套用。

5. 或者，選擇要用於此洞見的任何其他篩選條件。對於每個篩選條件，定義篩選條件，然後選擇套用。
6. 選擇 Create insight (建立洞見)。
7. 輸入 Insight 名稱，然後選擇建立 Insight。

Security Hub CSPM API

建立自訂洞見 (API)

1. 若要建立自訂洞見，請使用 Security Hub CSPM API [CreateInsight](#) 的操作。如果您使用 AWS CLI，請執行 [create-insight](#) 命令。
2. 使用自訂洞見的名稱填入 Name 參數。
3. 填入 Filters 參數以指定要包含在洞見中的調查結果。
4. 填入 GroupByAttribute 參數以指定用於將洞見中包含的問題清單分組的屬性。
5. 或者，填入 SortCriteria 參數，依特定欄位排序問題清單。

下列範例會建立自訂洞見，其中包含具有 `AwsIamRole` 資源類型的關鍵調查結果。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub create-insight --name "Critical role findings" --filters
'{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole" }],
"SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

建立自訂洞見 (PowerShell)

1. 使用 `New-SHUBInsight` cmdlet。
2. 使用自訂洞見的名稱填入 Name 參數。
3. 填入 Filter 參數以指定要包含在洞見中的調查結果。
4. 填入 GroupByAttribute 參數以指定用於將洞見中包含的問題清單分組的屬性。

如果您已啟用 [跨區域彙總](#)，並從彙總區域使用此 cmdlet，則洞見會套用至來自彙總和連結區域的相符問題清單。

範例

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

從受管洞見建立自訂洞見（僅限主控台）

您無法儲存變更或刪除受管洞見。不過，您可以使用受管洞見作為自訂洞見的基礎。此選項僅適用於 Security Hub CSPM 主控台。

從受管洞見建立自訂洞見（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇 Insights。
3. 選擇要使用的受管洞見。
4. 視需要編輯洞見組態。
 - 變更在洞見中用於將問題清單分組的屬性：
 - a. 若要移除現有的群組，請透過設定選擇群組旁的 X。
 - b. 選取搜尋方塊。
 - c. 選取要用於分組的屬性。
 - d. 選擇套用。
 - 若要從洞見中移除篩選條件，請選擇篩選條件旁的圓圈 X。
 - 新增篩選條件到洞見：
 - a. 選取搜尋方塊。
 - b. 選取要用做篩選條件的屬性和值。
 - c. 選擇套用。

5. 更新完成時，請選擇 Create insight (建立洞見)。
6. 出現提示時，輸入 Insight 名稱，然後選擇建立洞見。

編輯自訂洞見

您可以編輯現有的自訂洞見，以變更分組值和篩選條件。進行變更後，您可以將更新儲存到原始洞見，或另存更新的版本為新的洞見。

在 AWS Security Hub CSPM 中，自訂洞見可用來收集一組特定的問題清單，並追蹤您環境特有的問題。如需自訂洞見的背景資訊，請參閱 [了解 Security Hub CSPM 中的自訂洞見](#)。

若要編輯自訂洞見，請選擇您偏好的方法，然後遵循指示。

Security Hub CSPM console

編輯自訂洞見（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇 Insights。
3. 選擇要修改的自訂洞見
4. 視需要編輯洞見組態。
 - 變更在洞見中用於將問題清單分組的屬性：
 - a. 若要移除現有的群組，請透過設定選擇群組旁的 X。
 - b. 選取搜尋方塊。
 - c. 選取要用於分組的屬性。
 - d. 選擇套用。
 - 若要從洞見中移除篩選條件，請選擇篩選條件旁的圓圈 X。
 - 新增篩選條件到洞見：
 - a. 選取搜尋方塊。
 - b. 選取要用做篩選條件的屬性和值。
 - c. 選擇套用。
5. 完成更新時，請選擇 Save insight (儲存洞見)。
6. 出現提示時，請執行以下其中一項作業：

- 若要更新現有的洞見以反映您的變更，請選擇更新 **<Insight_Name>**，然後選擇儲存洞見。
- 如果要以更新建立新的洞見，請選擇 Save new insight (儲存新的洞見)。輸入 Insight name (洞見名稱)，然後選擇 Save insight (儲存洞見)。

Security Hub CSPM API

編輯自訂洞見 (API)

1. 使用 Security Hub CSPM API [UpdateInsight](#) 的操作。如果您使用 AWS CLI 執行 [update-insight](#) 命令。
2. 若要識別您要更新的自訂洞見，請提供洞見的 Amazon Resource Name (ARN)。若要取得自訂洞見的 ARN，請使用 [GetInsights](#) 操作或 [get-insights](#) 命令。
3. 視需要更新 Filters、Name 和 GroupByAttribute 參數。

下列範例會更新指定的洞見。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}], "SeverityLabel": [{ "Comparison": "EQUALS", "Value": "HIGH"}]}' --name "High severity role findings"
```

PowerShell

編輯自訂洞見 (PowerShell)

1. 使用 Update-SHUBInsight cmdlet。
2. 若要識別自訂洞見，請提供洞見的 Amazon Resource Name (ARN)。若要取得自訂洞見的 ARN，請使用 Get-SHUBInsight cmdlet。
3. 視需要更新 Name、Filter 和 GroupByAttribute 參數。

範例

```
$Filter = @{  
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
```

```
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

刪除自訂洞見

在 AWS Security Hub CSPM 中，自訂洞見可用來收集一組特定的問題清單，並追蹤您環境特有的問題。如需自訂洞見的背景資訊，請參閱 [了解 Security Hub CSPM 中的自訂洞見](#)。

若要刪除自訂洞見，請選擇您偏好的方法，然後遵循指示。您無法刪除受管洞見。

Security Hub CSPM console

刪除自訂洞見（主控台）

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇 Insights。
3. 找到要刪除的自訂洞見。
4. 針對該洞見，請選擇更多選項圖示（卡片右上角的三個點）。
5. 選擇 刪除。

Security Hub CSPM API

刪除自訂洞見 (API)

1. 使用 Security Hub CSPM API [DeleteInsight](#) 的操作。如果您使用 AWS CLI 執行 [delete-insight](#) 命令。
2. 若要識別要刪除的自訂洞見，請提供洞見的 ARN。若要取得自訂洞見的 ARN，請使用 [GetInsights](#) 操作或 [get-insights](#) 命令。

下列範例會刪除指定的洞見。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

PowerShell

刪除自訂洞見 (PowerShell)

1. 使用 Remove-SHUBInsight cmdlet。
2. 若要識別自訂洞見，請提供洞見的 ARN。若要取得自訂洞見的 ARN，請使用 Get-SHUBInsight cmdlet。

範例

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

自動修改 Security Hub CSPM 中的調查結果並對其採取行動

AWS Security Hub CSPM 具有可根據您的規格自動修改問題清單並對其採取動作的功能。

Security Hub CSPM 目前支援兩種類型的自動化：

- 自動化規則 – 根據您定義的條件，以近乎即時的方式自動更新和隱藏問題清單。
- 自動化回應和修復 – 建立自訂 Amazon EventBridge 規則，以定義針對特定調查結果和洞見採取的自動動作。

當您想要自動更新 AWS 安全調查結果格式 (ASFF) 中的調查結果欄位時，自動化規則很有幫助。例如，您可以使用自動化規則來更新特定第三方整合問題清單的嚴重性等級或工作流程狀態。使用自動化規則不需要手動更新此第三方產品中每個調查結果的嚴重性等級或工作流程狀態。

當您想要在 Security Hub CSPM 之外對特定調查結果採取動作，或將特定調查結果傳送至第三方工具以進行修復或其他調查時，EventBridge 規則很有用。這些規則可用來觸發支援的動作，例如叫用 AWS Lambda 函數或將特定問題清單通知 Amazon Simple Notification Service (Amazon SNS) 主題。

自動化規則會在套用 EventBridge 規則之前生效。也就是說，自動化規則會在 EventBridge 收到問題清單之前觸發並更新問題清單。然後 EventBridge 規則會套用至更新的調查結果。

為安全控制設定自動化時，我們建議根據控制 ID 進行篩選，而不是根據標題或描述進行篩選。雖然 Security Hub CSPM 偶爾會更新控制項標題和描述，但控制項 IDs 保持不變。

主題

- [了解 Security Hub CSPM 中的自動化規則](#)
- [使用 EventBridge 進行自動回應和修復](#)

了解 Security Hub CSPM 中的自動化規則

您可以使用自動化規則自動更新 AWS Security Hub CSPM 中的問題清單。擷取問題清單時，Security Hub CSPM 可以套用各種規則動作，例如隱藏問題清單、變更問題清單的嚴重性以及新增備註。這類規則動作會修改符合您指定條件的問題清單。

自動化規則的使用案例範例包括下列項目：

- CRITICAL 如果問題清單的資源 ID 參考關鍵業務資源，請將問題清單的嚴重性提升為。
- CRITICAL 如果問題清單影響特定生產帳戶中的資源，請將問題清單的嚴重性從 提升HIGH為。
- 指派具有INFORMATIONALSUPPRESSED工作流程狀態嚴重性的特定問題清單。

您只能從 Security Hub CSPM 管理員帳戶建立和管理自動化規則。

規則同時適用於新的調查結果和更新的調查結果。您可以從頭開始建立自訂規則，或使用 Security Hub CSPM 提供的規則範本。您也可以從範本開始，並視需要修改。

定義規則條件和規則動作

從 Security Hub CSPM 管理員帳戶，您可以透過定義一或多個規則條件和一或多個規則動作來建立自動化規則。當問題清單符合定義的條件時，Security Hub CSPM 會將規則動作套用到其中。如需可用條件和動作的詳細資訊，請參閱 [可用的規則條件和規則動作](#)。

Security Hub CSPM 目前支援每個管理員帳戶最多 100 個自動化規則。

Security Hub CSPM 管理員帳戶也可以編輯、檢視和刪除自動化規則。規則適用於管理員帳戶及其所有成員帳戶中相符的問題清單。透過提供成員帳戶 IDs 做為規則條件，Security Hub CSPM 管理員也可以使用自動化規則來更新或隱藏特定成員帳戶中的問題清單。

自動化規則僅適用於建立自動化規則 AWS 區域 的。若要在多個區域中套用規則，管理員必須在每個區域中建立規則。這可以透過 Security Hub CSPM 主控台、Security Hub CSPM API 或 來完成[AWS CloudFormation](#)。您也可以使用[多區域部署指令碼](#)。

可用的規則條件和規則動作

目前支援下列 AWS 安全調查結果格式 (ASFF) 欄位做為自動化規則的條件：

規則條件	篩選條件運算子	欄位類型
AwsAccountId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
AwsAccountName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
CompanyName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ComplianceStatus	Is, Is Not	選取： 【FAILED、NOT_AVAILABLE、PASSED、WARNING】

規則條件	篩選條件運算子	欄位類型
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
CreatedAt	Start, End, DateRange	日期 (格式為 2022-12-01T21 : 47 : 39.269Z)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
FirstObservedAt	Start, End, DateRange	日期 (格式為 2022-12-01T21 : 47 : 39.269Z)
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
LastObservedAt	Start, End, DateRange	日期 (格式為 2022-12-01T21 : 47 : 39.269Z)

規則條件	篩選條件運算子	欄位類型
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
NoteUpdatedAt	Start, End, DateRange	日期 (格式為 2022-12-01T21:47:39.269Z)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串

規則條件	篩選條件運算子	欄位類型
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

規則條件	篩選條件運算子	欄位類型
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map
ResourceType	Is, Is Not	選取 (請參閱 ASFF 支援 的資源)
SeverityLabel	Is, Is Not	選取 : 【CRITICAL、HIGH、MEDIUMLOW、 ONAL 】
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	字串
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
UpdatedAt	Start, End, DateRange	日期 (格式為 2022-12-01T21 : 47 : 39.269Z)
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Map

規則條件	篩選條件運算子	欄位類型
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
WorkflowStatus	Is, Is Not	選取： 【NEW、NOTIFIED、RESOLVED、SUCCEEDED】

對於標記為字串欄位的條件，在相同欄位上使用不同的篩選條件運算子會影響評估邏輯。如需詳細資訊，請參閱 AWS Security Hub CSPM API 參考[StringFilter](#)中的。

每個條件都支援可用於篩選相符問題清單的最大值。如需每個條件的限制，請參閱 AWS Security Hub CSPM API 參考[AutomationRulesFindingFilters](#)中的。

下列 ASFF 欄位目前支援做為自動化規則的動作：

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

如需特定 ASFF 欄位的詳細資訊，請參閱[AWS 安全調查結果格式 \(ASFF\) 語法](#)。

Tip

如果您希望 Security Hub CSPM 停止產生特定控制項的問題清單，建議您停用控制項，而不是使用自動化規則。當您停用控制項時，Security Hub CSPM 會停止對其執行安全檢查，並

停止為其產生問題清單，因此您不需要為該控制項支付費用。我們建議您使用自動化規則，為符合定義條件的問題清單變更特定 ASFF 欄位的值。如需停用控制項的詳細資訊，請參閱 [在 Security Hub CSPM 中停用控制項](#)。

自動化規則評估的問題清單

自動化規則會評估 Security Hub CSPM 在您建立規則後透過 [BatchImportFindings](#) 操作產生或擷取的新問題清單和更新的問題清單。Security Hub CSPM 每 12-24 小時或關聯資源變更狀態時更新控制問題清單。如需詳細資訊，請參閱 [執行安全檢查的排程](#)。

自動化規則會評估原始供應商提供的調查結果。供應商可以使用 Security Hub CSPM API `BatchImportFindings` 的操作，提供新的問題清單並更新現有的問題清單。如果原始調查結果中不存在下列欄位，Security Hub CSPM 會自動填入欄位，然後在自動化規則的評估中使用填入的值：

- `AwsAccountName`
- `CompanyName`
- `ProductName`
- `Resource.Tags`
- `Workflow.Status`

建立一或多個自動化規則之後，如果您使用 [BatchUpdateFindings](#) 操作更新問題清單欄位，則不會觸發規則。如果您建立自動化規則並進行會影響相同調查結果欄位的 `BatchUpdateFindings` 更新，則上次更新會設定該欄位的值。採用下列範例：

1. 您可以使用 `BatchUpdateFindings` 操作，將調查結果 `Workflow.Status` 欄位的值從 變更為 `NEW NOTIFIED`。
2. 如果您呼叫 `GetFindings`，`Workflow.Status` 欄位現在的值為 `NOTIFIED`。
3. 您可以建立自動化規則，將調查結果 `Workflow.Status` 的欄位從 變更為 `NEW SUPPRESSED`。（請記住，規則會忽略使用 `BatchUpdateFindings` 操作所做的更新。）
4. 調查結果提供者使用 `BatchImportFindings` 操作來更新調查結果，並將調查結果 `Workflow.Status` 欄位的值變更為 `NEW`。
5. 如果您呼叫 `GetFindings`，`Workflow.Status` 欄位現在的值為 `SUPPRESSED`。這是因為已套用自動化規則，且規則是對調查結果採取的最後一個動作。

當您在 Security Hub CSPM 主控台上建立或編輯規則時，主控台會顯示符合規則條件的調查結果測試版。雖然自動化規則會評估問題清單提供者傳送的原始問題清單，但主控台 Beta 版會反映問題清單的最終狀態，如同回應[GetFindings](#)操作時所示（也就是套用規則動作或其他更新至問題清單之後）。

規則順序的運作方式

建立自動化規則時，您會為每個規則指派一個順序。這將決定 Security Hub CSPM 套用自動化規則的順序，並在多個規則與相同的調查結果或調查結果欄位相關時變得重要。

當多個規則動作與相同的調查結果或調查結果欄位相關時，具有規則順序最高數值的規則會最後套用，並具有最終效果。

當您在 Security Hub CSPM 主控台中建立規則時，Security Hub CSPM 會根據規則建立的順序自動指派規則順序。最近建立的規則具有最低的規則順序數值，因此會先套用。Security Hub CSPM 會以遞增順序套用後續規則。

當您透過 Security Hub CSPM API 或 建立規則時 AWS CLI，Security Hub CSPM 會先套用具有最低數值的規則RuleOrder。然後，它會以遞增順序套用後續規則。如果多個問題清單具有相同的RuleOrder，Security Hub CSPM 會先為 UpdatedAt 欄位套用具有較早值的規則（也就是說，最近編輯的規則會套用最後）。

您可以隨時修改規則順序。

規則順序範例：

規則 A（規則順序為 1）：

- 規則 A 條件
 - ProductName = Security Hub CSPM
 - Resources.Type 是 S3 Bucket
 - Compliance.Status = FAILED
 - RecordState 是 NEW
 - Workflow.Status = ACTIVE
- 規則 A 動作
 - 更新Confidence至 95
 - 更新Severity至 CRITICAL

規則 B（規則順序為 2）：

- 規則 B 條件
 - `AwsAccountId = 123456789012`
- 規則 B 動作
 - 更新Severity至 INFORMATIONAL

規則 動作會先套用至符合規則 A 條件的 Security Hub CSPM 調查結果。接下來，規則 B 動作適用於具有指定帳戶 ID 的 Security Hub CSPM 調查結果。在此範例中，由於規則 B 最後套用，因此來自指定帳戶 ID 之調查結果Severity中的 結束值為 INFORMATIONAL。根據規則 A 動作，相符調查結果Confidence中的 結束值為 95。

建立自動化規則

自動化規則可用來自動更新 AWS Security Hub CSPM 中的調查結果。您可以從頭開始建立自訂自動化規則，或在 Security Hub CSPM 主控台上使用預先填入的規則範本。如需自動化規則運作方式的背景資訊，請參閱 [了解 Security Hub CSPM 中的自動化規則](#)。

您一次只能建立一個自動化規則。若要建立多個自動化規則，請遵循主控台程序多次，或使用所需的參數多次呼叫 API 或命令。

您必須在您希望規則套用至問題清單的每個區域和帳戶中建立自動化規則。

當您在 Security Hub CSPM 主控台中建立自動化規則時，Security Hub CSPM 會顯示規則適用的調查結果測試版。如果您的規則條件包含 CONTAINS 或 NOT_CONTAINS 篩選條件，目前不支援 Beta。您可以針對映射和字串欄位類型選擇這些篩選條件。

Important

AWS 建議您不要在規則名稱、描述或其他欄位中包含個人識別、機密或敏感資訊。

建立自訂自動化規則

選擇您偏好的方法，並完成下列步驟以建立自訂自動化規則。

Console

建立自訂自動化規則（主控台）

1. 使用 Security Hub CSPM 管理員的登入資料，開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。

2. 在導覽窗格中，選擇自動化。
3. 選擇建立規則。針對規則類型，選擇建立自訂規則。
4. 在規則區段中，提供規則的唯一規則名稱和描述。
5. 針對條件，請使用金鑰、運算子和值下拉式選單來指定您的規則條件。您必須指定至少一個規則條件。

如果所選條件支援，主控台會顯示符合您條件的調查結果測試版。

6. 對於自動化動作，使用下拉式選單指定當問題清單符合您的規則條件時要更新哪些問題清單欄位。您必須指定至少一個規則動作。
7. 針對規則狀態，選擇您希望規則在建立之後啟用或停用。
8. （選用）展開其他設定區段。如果您希望此規則是套用到符合規則條件之調查結果的最後一個規則，請選取忽略符合這些條件之調查結果的後續規則。
9. （選用）對於標籤，將標籤新增為鍵/值對，以協助您輕鬆識別規則。
10. 選擇建立規則。

API

建立自訂自動化規則 (API)

1. [CreateAutomationRule](#) 從 Security Hub CSPM 管理員帳戶執行。此 API 會建立具有特定 Amazon Resource Name (ARN) 的規則。
2. 提供規則的名稱和描述。
3. `true` 如果您希望此規則是套用至符合規則條件之問題清單的最後一個規則，請將 `IsTerminal` 參數設定為。
4. 針對 `RuleOrder` 參數，提供規則的順序。Security Hub CSPM 會先套用此參數數值較低的規則。
5. 針對 `RuleStatus` 參數，指定您是否希望 Security Hub CSPM 在建立後啟用並開始將規則套用到問題清單。如未指定任何值，則預設值為 `ENABLED`。的值 `DISABLED` 表示規則會在建立後暫停。
6. 針對 `Criteria` 參數，提供您希望 Security Hub CSPM 用來篩選問題清單的條件。規則動作將套用到符合條件的問題清單。如需支援的條件清單，請參閱 [可用的規則條件和規則動作](#)。
7. 針對 `Actions` 參數，提供您希望 Security Hub CSPM 在問題清單與您定義的條件相符時所採取的動作。如需支援的動作清單，請參閱 [可用的規則條件和規則動作](#)。

下列範例 AWS CLI 命令會建立自動化規則，更新工作流程狀態和相符問題清單的備註。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub create-automation-rule \
--actions '[{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Severity": {
      "Label": "HIGH"
    },
    "Note": {
      "Text": "Known issue that is a risk. Updated by automation rules",
      "UpdatedBy": "sechub-automation"
    }
  }
}]' \
--criteria '{
  "SeverityLabel": [{
    "Value": "INFORMATIONAL",
    "Comparison": "EQUALS"
  }]
}' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

從範本建立自動化規則（僅限主控台）

規則範本反映自動化規則的常見使用案例。目前，只有 Security Hub CSPM 主控台支援規則範本。完成下列步驟，從主控台內的範本建立自動化規則。

從範本建立自動化規則（主控台）

1. 使用 Security Hub CSPM 管理員的登入資料，開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇自動化。
3. 選擇建立規則。針對規則類型，選擇從範本建立規則。

4. 從下拉式選單中選取規則範本。
5. (選用) 如果您的使用案例需要，請修改規則、條件和自動化動作區段。您必須指定至少一個規則條件和一個規則動作。

如果所選條件支援，主控台會顯示符合您條件的調查結果測試版。

6. 針對規則狀態，選擇您希望規則在建立之後啟用或停用。
7. (選用) 展開其他設定區段。如果您希望此規則是套用到符合規則條件之調查結果的最後一個規則，請選取忽略符合這些條件之調查結果的後續規則。
8. (選用) 對於標籤，將標籤新增為鍵值對，以協助您輕鬆識別規則。
9. 選擇建立規則。

檢視自動化規則

自動化規則可用來自動更新 AWS Security Hub CSPM 中的調查結果。如需自動化規則運作方式的背景資訊，請參閱 [了解 Security Hub CSPM 中的自動化規則](#)。

選擇您偏好的方法，並依照步驟檢視現有的自動化規則和每個規則的詳細資訊。

若要檢視自動化規則如何變更問題清單的歷史記錄，請參閱 [在 Security Hub CSPM 中檢閱問題清單詳細資訊和歷史記錄](#)。

Console

檢視自動化規則 (主控台)

1. 使用 Security Hub CSPM 管理員的登入資料，開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇自動化。
3. 選擇規則名稱。或者，選取規則。
4. 選擇動作和檢視。

API

檢視自動化規則 (API)

1. 若要檢視帳戶的自動化規則，[ListAutomationRules](#) 請從 Security Hub CSPM 管理員帳戶執行。此 API 會傳回規則 ARNs 和其他中繼資料。此 API 不需要輸入參數，但您可以

選擇提供 MaxResults 來限制結果數量，並以分頁參數 NextToken 的形式提供。的初始值 NextToken 應為 NULL。

2. 如需其他規則詳細資訊，包括規則的條件和動作，[BatchGetAutomationRules](#) 請從 Security Hub CSPM 管理員帳戶執行。提供您想要其詳細資訊之自動化規則的 ARNs。

下列範例會擷取指定自動化規則的詳細資訊。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

編輯自動化規則

自動化規則可用來自動更新 AWS Security Hub CSPM 中的調查結果。如需自動化規則運作方式的背景資訊，請參閱 [了解 Security Hub CSPM 中的自動化規則](#)。

建立自動化規則後，委派的 Security Hub CSPM 管理員可以編輯規則。當您編輯自動化規則時，變更會套用至 Security Hub CSPM 在規則編輯後產生或擷取的新問題清單和更新的問題清單。

選擇您偏好的方法，然後依照步驟編輯自動化規則的內容。您可以使用單一請求編輯一或多個規則。如需編輯規則順序的指示，請參閱 [編輯自動化規則順序](#)。

Console

編輯自動化規則（主控台）

1. 使用 Security Hub CSPM 管理員的登入資料，開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇自動化。
3. 選取您要編輯的規則。選擇動作和編輯。
4. 視需要變更規則，然後選擇儲存變更。

API

編輯自動化規則 (API)

1. [BatchUpdateAutomationRules](#) 從 Security Hub CSPM 管理員帳戶執行。
2. 針對 RuleArn 參數，提供您要編輯之規則的 ARN (ARN)。
3. 為您要編輯的參數提供新值。您可以編輯 以外的任何參數RuleArn。

下列 範例會更新指定的自動化規則。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
  {
    "Actions": [{
      "Type": "FINDING_FIELDS_UPDATE",
      "FindingFieldsUpdate": {
        "Note": {
          "Text": "Known issue that is a risk",
          "UpdatedBy": "sechub-automation"
        },
        "Workflow": {
          "Status": "NEW"
        }
      }
    }],
    "Criteria": {
      "SeverityLabel": [{
        "Value": "LOW",
        "Comparison": "EQUALS"
      }]
    },
    "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "RuleOrder": 14,
    "RuleStatus": "DISABLED",
  }
]' \
--region us-east-1
```

編輯自動化規則順序

自動化規則可用來自動更新 AWS Security Hub CSPM 中的調查結果。如需自動化規則運作方式的背景資訊，請參閱 [了解 Security Hub CSPM 中的自動化規則](#)。

建立自動化規則後，委派的 Security Hub CSPM 管理員可以編輯規則。

如果您想要保持規則條件和動作相同，但變更 Security Hub CSPM 套用自動化規則的順序，您可以只編輯規則順序。選擇您偏好的方法，然後依照步驟編輯規則順序。

如需編輯自動化規則的條件或動作的說明，請參閱 [編輯自動化規則](#)。

Console

編輯自動化規則順序（主控台）

1. 使用 Security Hub CSPM 管理員的登入資料，開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇自動化。
3. 選取您要變更其順序的規則。選擇編輯優先順序。
4. 選擇向上移動，將規則的優先順序增加一個單位。選擇向下移動，將規則優先順序降低一個單位。選擇移至頂端，將規則的順序指派為 1（這會讓規則優先於其他現有規則）。

Note

當您在 Security Hub CSPM 主控台中建立規則時，Security Hub CSPM 會根據規則建立的順序自動指派規則順序。最近建立的規則具有最低的規則順序數值，因此會先套用。

API

編輯自動化規則順序 (API)

1. 使用 Security Hub CSPM 管理員帳戶中的 [BatchUpdateAutomationRules](#) 操作。
2. 針對 RuleArn 參數，提供您要編輯其順序之規則的 ARN (ARN)。
3. 修改 RuleOrder 欄位的值。

 Note

如果多個規則具有相同的 RuleOrder，Security Hub CSPM 會先為 UpdatedAt 欄位套用具有較早值的規則（也就是最近編輯的規則最後套用）。

刪除或停用自動化規則

自動化規則可用來自動更新 AWS Security Hub CSPM 中的調查結果。如需自動化規則運作方式的背景資訊，請參閱 [了解 Security Hub CSPM 中的自動化規則](#)。

當您刪除自動化規則時，Security Hub CSPM 會從您的帳戶中移除它，不再將規則套用至問題清單。除了刪除之外，您也可以停用規則。這將保留規則以供日後使用，但 Security Hub CSPM 不會將規則套用到任何相符的問題清單，直到您啟用為止。

選擇您偏好的方法，然後依照步驟刪除自動化規則。您可以在單一請求中刪除一或多個規則。

Console

刪除或停用自動化規則（主控台）

1. 使用 Security Hub CSPM 管理員的登入資料，開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇自動化。
3. 選取您要刪除的規則（多個）。選擇動作和刪除（若要保留規則，但暫時停用，請選擇停用）。
4. 確認您的選擇，然後選擇 Delete (刪除)。

API

刪除或停用自動化規則 (API)

1. 使用 Security Hub CSPM 管理員帳戶中的 [BatchDeleteAutomationRules](#) 操作。
2. 對於 AutomationRulesArns 參數，請提供您要刪除之規則的 ARN（若要保留規則，但暫時停用它），DISABLED 請為 RuleStatus 參數提供）。

以下範例會刪除指定的自動化規則。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE1111"]' \
--region us-east-1
```

自動化規則的範例

本節提供常見 Security Hub CSPM 使用案例的自動化規則範例。這些範例對應至 Security Hub CSPM 主控台上可用的規則範本。

當 S3 儲存貯體等特定資源面臨風險時，將嚴重性提升為「關鍵」

在此範例中，當調查結果ResourceId中的 是特定的 Amazon Simple Storage Service (Amazon S3) 儲存貯體時，規則條件會相符。規則動作是將相符問題清單的嚴重性變更為 CRITICAL。您可以修改此範本以套用至其他資源。

範例 API 請求：

```
{
  "IsTerminal": true,
  "RuleName": "Elevate severity of findings that relate to important resources",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Elevate finding severity to CRITICAL when specific resource such as
an S3 bucket is at risk",
  "Criteria": {
    "ProductName": [{
      "Value": "Security Hub CSPM",
      "Comparison": "EQUALS"
    }],
    "ComplianceStatus": [{
      "Value": "FAILED",
      "Comparison": "EQUALS"
    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }]
  }
}
```

```

    ]],
    "ResourceId": [{
        "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
        "Comparison": "EQUALS"
    }]
},
"Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
        "Severity": {
            "Label": "CRITICAL"
        },
        "Note": {
            "Text": "This is a critical resource. Please review ASAP.",
            "UpdatedBy": "sechub-automation"
        }
    }
}]
}

```

範例 CLI 命令：

```

$
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
S3 bucket is at risk" \
--criteria '{
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}
}

```



```

    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
    "ResourceId": [{
      "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
      "Comparison": "EQUALS"
    }]
  }' \
  --actions '[{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
      "Severity": {
        "Label": "CRITICAL"
      },
      "Note": {
        "Text": "This is a critical resource. Please review ASAP.",
        "UpdatedBy": "sechub-automation"
      }
    }
  }]' \
  --region us-east-1

```

提高與生產帳戶中資源相關的問題清單嚴重性

在此範例中，當在特定生產帳戶中產生HIGH嚴重性調查結果時，規則條件會相符。規則動作是將相符問題清單的嚴重性變更為 CRITICAL。

範例 API 請求：

```

{
  "IsTerminal": false,
  "RuleName": "Elevate severity for production accounts",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Elevate finding severity from HIGH to CRITICAL for findings that relate to resources in specific production accounts",
  "Criteria": {
    "ProductName": [{
      "Value": "Security Hub CSPM",
      "Comparison": "EQUALS"
    }],

```

```

    "ComplianceStatus": [{
      "Value": "FAILED",
      "Comparison": "EQUALS"
    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
    "SeverityLabel": [{
      "Value": "HIGH",
      "Comparison": "EQUALS"
    }],
    "AwsAccountId": [
      {
        "Value": "111122223333",
        "Comparison": "EQUALS"
      },
      {
        "Value": "123456789012",
        "Comparison": "EQUALS"
      }
    ],
  },
  "Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
      "Severity": {
        "Label": "CRITICAL"
      },
      "Note": {
        "Text": "A resource in production accounts is at risk. Please review
ASAP.",
        "UpdatedBy": "sechub-automation"
      }
    }
  ]
}

```

範例 CLI 命令：

```
aws securityhub create-automation-rule \  
--no-is-terminal \  
--rule-name "Elevate severity of findings that relate to resources in production  
accounts" \  
--rule-order 1 \  
--rule-status "ENABLED" \  
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate  
to resources in specific production accounts" \  
--criteria '{  
  "ProductName": [{  
    "Value": "Security Hub CSPM",  
    "Comparison": "EQUALS"  
  }],  
  "ComplianceStatus": [{  
    "Value": "FAILED",  
    "Comparison": "EQUALS"  
  }],  
  "RecordState": [{  
    "Value": "ACTIVE",  
    "Comparison": "EQUALS"  
  }],  
  "SeverityLabel": [{  
    "Value": "HIGH",  
    "Comparison": "EQUALS"  
  }],  
  "AwsAccountId": [  
    {  
      "Value": "111122223333",  
      "Comparison": "EQUALS"  
    },  
    {  
      "Value": "123456789012",  
      "Comparison": "EQUALS"  
    }  
  ]  
' \  
--actions '[{  
  "Type": "FINDING_FIELDS_UPDATE",  
  "FindingFieldsUpdate": {  
    "Severity": {  
      "Label": "CRITICAL"  
    },  
    "Note": {
```

```

"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1

```

隱藏資訊性問題清單

在此範例中，從 Amazon GuardDuty 傳送至 Security Hub CSPM 的 INFORMATIONAL 嚴重性調查結果符合規則條件。規則動作是將相符問題清單的工作流程狀態變更為 SUPPRESSED。

範例 API 請求：

```

{
  "IsTerminal": false,
  "RuleName": "Suppress informational findings",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
  "Criteria": {
    "ProductName": [{
      "Value": "GuardDuty",
      "Comparison": "EQUALS"
    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
    "SeverityLabel": [{
      "Value": "INFORMATIONAL",
      "Comparison": "EQUALS"
    }]
  },
  "Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
      "Workflow": {
        "Status": "SUPPRESSED"
      }
    }
  ]
}

```

```

    },
    "Note": {
      "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
severity",
      "UpdatedBy": "sechub-automation"
    }
  }
}]
}

```

CLI 命令範例：

```

aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",

```

```
"FindingFieldsUpdate": {  
  "Workflow": {  
    "Status": "SUPPRESSED"  
  },  
  "Note": {  
    "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",  
    "UpdatedBy": "sechub-automation"  
  }  
}  
}]' \  
--region us-east-1
```

使用 EventBridge 進行自動回應和修復

透過在 Amazon EventBridge 中建立規則，您可以自動回應 AWS Security Hub CSPM 問題清單。Security Hub CSPM 會以近乎即時的方式將調查結果作為事件傳送至 EventBridge。您可以撰寫簡單的規則來指出您感興趣的事件，以及在事件符合規則時要採取哪些自動化動作。可以自動觸發的動作如下：

- 叫用 AWS Lambda 函數
- 叫用 Amazon EC2 執行命令
- 將事件轉傳至 Amazon Kinesis Data Streams
- 啟用 AWS Step Functions 狀態機器
- 通知 Amazon SNS 主題或 Amazon SQS 佇列
- 將問題清單傳送至第三方票證系統、聊天、SIEM 或事件反應及管理工具

Security Hub CSPM 會自動將所有新調查結果和現有調查結果的所有更新作為 EventBridge 事件傳送至 EventBridge。您也可以建立自訂動作，讓您將選取的調查結果和洞見結果傳送至 EventBridge。

然後，您可以設定 EventBridge 規則來回應每種類型的事件。

如需使用 EventBridge 的詳細資訊，請參閱 [《Amazon EventBridge 使用者指南》](#)。

Note

根據最佳實務，請確定授予您使用者存取 EventBridge 的許可，使用僅授予必要許可的 least-privilege AWS Identity and Access Management (IAM) 政策。

如需詳細資訊，請參閱 [Amazon EventBridge 中的身分和存取管理](#)。

AWS 解決方案也提供一組跨帳戶自動回應和修復的範本。範本會利用 EventBridge 事件規則和 Lambda 函數。您可以使用 CloudFormation 和 部署解決方案 AWS Systems Manager。解決方案可以建立完全自動化的回應和修補動作。它也可以使用 Security Hub CSPM 自訂動作來建立使用者觸發的回應和修補動作。如需如何設定和使用解決方案的詳細資訊，請參閱解決方案[上的自動安全回應 AWS](#)頁面。

主題

- [EventBridge 中的 Security Hub CSPM 事件類型](#)
- [Security Hub CSPM 的 EventBridge 事件格式](#)
- [為 Security Hub CSPM 調查結果設定 EventBridge 規則](#)
- [使用自訂動作將問題清單和洞見結果傳送至 EventBridge](#)

EventBridge 中的 Security Hub CSPM 事件類型

Security Hub CSPM 使用以下 Amazon EventBridge 事件類型與 EventBridge 整合。

在 Security Hub CSPM 的 EventBridge 儀表板上，所有事件都包含所有這些事件類型。

所有問題清單 (Security Hub Findings - Imported)

Security Hub CSPM 會自動將所有新調查結果和現有調查結果的所有更新作為 Security Hub Findings - Imported 事件傳送至 EventBridge。每個 Security Hub Findings - Imported 事件都包含單一調查結果。

每個 [BatchImportFindings](#) 和 [BatchUpdateFindings](#) 請求都會觸發 Security Hub Findings - Imported 事件。

對於管理員帳戶，EventBridge 中的事件饋送包含來自其帳戶及其成員帳戶的問題清單事件。

在彙總區域中，事件饋送包含來自彙總區域和連結區域的問題清單事件。跨區域調查結果會近乎即時地包含在事件饋送中。如需如何設定問題清單彙總的資訊，請參閱 [the section called “跨區域彙總資料”](#)。

您可以在 EventBridge 中定義規則，自動將問題清單路由至修復工作流程、第三方工具或[其他支援的 EventBridge 目標](#)。這些規則可以包含篩選條件，只有在問題清單具有特定屬性值時才會套用規則。

您可以使用此方法自動將所有問題清單或具有特定特性的所有問題清單傳送至回應或修復工作流程。

請參閱 [the section called “設定 EventBridge 規則”](#)。

自訂動作問題清單 (Security Hub Findings - Custom Action)

Security Hub CSPM 也會將與自訂動作相關聯的調查結果作為 Security Hub Findings - Custom Action 事件傳送至 EventBridge。

這對於使用 Security Hub CSPM 主控台的分析師來說非常有用，他們想要將特定調查結果或一小組調查結果傳送到回應或修復工作流程。您一次最多可以為 20 個問題清單選取自訂動作。每個調查結果都會以個別的 EventBridge 事件的形式傳送至 EventBridge。

當您建立自訂動作時，您會為其指派自訂動作 ID。您可以使用此 ID 來建立 EventBridge 規則，該規則會在收到與該自訂動作 ID 相關聯的問題清單後採取指定的動作。

請參閱 [the section called “設定和使用自訂動作”](#)。

例如，您可以在 Security Hub CSPM 中建立名為 `send_to_ticketing` 的自訂動作。然後在 EventBridge 中，建立當 EventBridge 收到包含 `send_to_ticketing` 自訂動作 ID 的問題清單時觸發的規則。規則包含了將問題清單傳送至您票證系統的邏輯。然後，您可以在 Security Hub CSPM 中選取問題清單，並使用 Security Hub CSPM 中的自訂動作，手動將問題清單傳送至您的票證系統。

如需如何將 Security Hub CSPM 調查結果傳送至 EventBridge 以進行進一步處理的範例，請參閱 AWS 合作夥伴網路 (APN) 部落格上的 [如何將 AWS Security Hub CSPM 自訂動作與 PagerDuty 整合，以及如何在 AWS Security Hub CSPM 中啟用自訂動作](#)。

自訂動作的洞見結果 (Security Hub Insight Results)

您也可以使用自訂動作，將洞察結果集以 Security Hub Insight Results 事件形式傳送至 EventBridge。Insight 結果是符合洞見的資源。請注意，當您將洞見結果傳送至 EventBridge 時，不會將調查結果傳送至 EventBridge。您只會傳送與洞見結果相關聯的資源識別符。您一次最多可以傳送 100 個資源識別符。

與問題清單的自訂動作類似，您會先在 Security Hub CSPM 中建立自訂動作，然後在 EventBridge 中建立規則。

請參閱 [the section called “設定和使用自訂動作”](#)。

例如，假設您看到想要與同事分享的特定感興趣的洞見結果。在這種情況下，您可以使用自訂動作，透過聊天或票證系統將該洞見結果傳送給同事。

Security Hub CSPM 的 EventBridge 事件格式

Security Hub Findings - Imported、Security Findings - Custom Action 和 Security Hub Insight Results 事件類型使用以下事件格式。

事件格式是 Security Hub CSPM 將事件傳送至 EventBridge 時所使用的格式。

Security Hub Findings - Imported

Security Hub Findings - Imported 從 Security Hub CSPM 傳送至 EventBridge 的事件使用以下格式。

```
{
  "version": "0",
  "id": "CWE-event-id",
  "detail-type": "Security Hub Findings - Imported",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T21:52:17Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:securityhub:us-west-2::product/aws/maciek/arn:aws:maciek:us-west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/f2893b211841"
  ],
  "detail": {
    "findings": [
      <finding content>
    ]
  }
}
```

<finding content> 是事件所傳送問題清單的內容，採用 JSON 格式。每個事件都會傳送單一問題清單。

如需問題清單屬性的完整清單，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

如需如何設定由這些事件觸發的 EventBridge 規則的詳細資訊，請參閱 [the section called “設定 EventBridge 規則”](#)。

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action 從 Security Hub CSPM 傳送至 EventBridge 的事件使用以下格式。每個問題清單都會以個別的事件傳送。

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
```

```

"source": "aws.securityhub",
"account": "111122223333",
"time": "2019-04-11T18:43:48Z",
"region": "us-west-1",
"resources": [
  "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
],
"detail": {
  "actionName": "custom-action-name",
  "actionDescription": "description of the action",
  "findings": [
    {
      <finding content>
    }
  ]
}
}

```

<finding content> 是事件所傳送問題清單的內容，採用 JSON 格式。每個事件都會傳送單一問題清單。

如需問題清單屬性的完整清單，請參閱 [AWS 安全調查結果格式 \(ASFF\)](#)。

如需如何設定由這些事件觸發的 EventBridge 規則的詳細資訊，請參閱 [the section called “設定和使用自訂動作”](#)。

Security Hub Insight Results

Security Hub Insight Results 從 Security Hub CSPM 傳送至 EventBridge 的事件使用以下格式。

```

{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333::product/aws/maciek:us-west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName": "name of the action",

```

```
{
  "actionDescription": "description of the action",
  "insightArn": "ARN of the insight",
  "insightName": "Name of the insight",
  "resultType": "ResourceAwsIamAccessKeyUserName",
  "number of results": "number of results, max of 100",
  "insightResults": [
    {"result 1": 5},
    {"result 2": 6}
  ]
}
```

如需如何建立由這些事件觸發的 EventBridge 規則的詳細資訊，請參閱 [the section called “設定和使用自訂動作”](#)。

為 Security Hub CSPM 調查結果設定 EventBridge 規則

您可以在 Amazon EventBridge 中建立規則，定義收到 Security Hub Findings - Imported 事件時要採取的動作。Security Hub Findings - Imported 事件是由 [BatchImportFindings](#) 和 [BatchUpdateFindings](#) 操作的更新所觸發。

每個規則都包含事件模式，可識別觸發規則的事件。事件模式一律包含事件來源 (aws.securityhub) 和事件類型 (Security Hub 調查結果 - 匯入)。事件模式也可以指定篩選條件，以識別規則套用的調查結果。

事件規則接著會識別規則目標。當 EventBridge 收到 Security Hub 調查結果 - 匯入的事件，且調查結果符合篩選條件時，目標為要採取的動作。

此處提供的指示使用 EventBridge 主控台。當您使用主控台時，EventBridge 會自動建立必要的資源型政策，讓 EventBridge 能夠寫入 Amazon CloudWatch Logs。

您也可以使用 EventBridge API [PutRule](#) 的操作。不過，如果您使用 EventBridge API，則必須建立以資源為基礎的政策。如需必要政策的相關資訊，請參閱《Amazon EventBridge 使用者指南》中的 [CloudWatch Logs 許可](#)。

事件模式的格式

Security Hub 調查結果 - 匯入事件的事件模式格式如下：

```
{
  "source": [
    "aws.securityhub"
  ],
```

```

"detail-type": [
  "Security Hub Findings - Imported"
],
"detail": {
  "findings": {
    <attribute filter values>
  }
}
}

```

- `source` 會將 Security Hub CSPM 識別為產生事件的服務。
- `detail-type` 會識別事件的類型。
- `detail` 是選用的，並提供事件模式的篩選條件值。如果事件模式不包含 `detail` 欄位，則所有調查結果都會觸發規則。

您可以根據任何問題清單屬性來篩選問題清單。對於每個屬性，您提供一或多個值的逗號分隔陣列。

```

"<attribute name>": [ "<value1>", "<value2>" ]

```

如果您為屬性提供多個值，則這些值會由 聯結OR。如果問題清單具有任何列出的值，則問題清單會比對個別屬性的篩選條件。例如，如果您同時提供 `INFORMATIONAL` 和 `LOW` 作為 的 `Severity.Label`，則如果問題清單的嚴重性標籤為 `INFORMATIONAL` 或 `LOW`，則問題清單會相符。

屬性由 聯結AND。如果問題清單符合所有提供屬性的篩選條件，則問題清單會相符。

當您提供屬性值時，它必須在 AWS 安全調查結果格式 (ASFF) 結構中反映該屬性的位置。

Tip

篩選控制項調查結果時，建議您使用 `SecurityControlId` 或 `SecurityControlArn` [ASFF 欄位](#) 做為篩選條件，而非 `Title` 或 `Description`。後者欄位可能會偶爾變更，而控制項 ID 和 ARN 是靜態識別符。

在下列範例中，事件模式提供 `ProductArn` 和 的篩選條件值 `Severity.Label`，因此如果問題清單是由 Amazon Inspector 產生且嚴重性標籤為 `INFORMATIONAL` 或 `LOW`，則問題清單會相符。

```

{

```

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
      "Severity": {
        "Label": ["INFORMATIONAL", "LOW"]
      }
    }
  }
}
```

建立事件規則

您可以使用預先定義的事件模式或自訂事件模式，在 EventBridge 中建立規則。如果您選擇預先定義的模式，EventBridge 會自動填入 source 和 detail-type。EventBridge 也提供欄位，以指定下列調查結果屬性的篩選條件值：

- AwsAccountId
- Compliance.Status
- Criticality
- ProductArn
- RecordState
- ResourceId
- ResourceType
- Severity.Label
- Types
- Workflow.Status

建立 EventBridge 規則（主控台）

1. 前往 <https://console.aws.amazon.com/events/> 開啟 Amazon EventBridge 主控台。
2. 使用下列值，建立 EventBridge 規則來監控調查結果事件：

- 針對規則類型，選擇具有事件模式的規則。
- 選擇如何建置事件模式。

若要使用 建置事件模式...	執行此作業...	
範本	在事件模式區段中，選擇下列選項： • 在事件來源欄位中，選擇 AWS 服務。 • 針對AWS 服務，選擇 Security Hub。 • 針對事件類型，選擇 Security Hub 調查結果 - 已匯入。 • (選用) 若要使規則更具體，請新增篩選條件值。例如，若要將規則限制為具有作用中記錄狀態的問題清單（若為特定記錄狀態），請選擇作用中。	

若要使用 建置事件模式...	執行此作業...	
自訂事件模式 (如果您想要根據 EventBridge 主控台中未顯示的屬性來篩選問題清單，請使用自訂模式。)	- 在事件模式區段中，選擇自訂模式 (JSON 編輯器)，然後將下列事件模式貼入文字區域： <pre data-bbox="690 441 1063 1228"> { "source": ["aws.secu rityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "<attribut e name> ": ["<value1>", "<value2>"] } } } </pre> - 更新事件模式，以包含您要用作篩選條件的屬性和屬性值。 例如，若要將規則套用至驗證狀態為 的調查結果 TRUE_POSITIVE，請使用下列模式範例： <pre data-bbox="690 1648 1063 1848"> { "source": ["aws.secu rityhub"], </pre>	

若要使用 建置事件模式...	執行此作業...	
	<pre> "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "Verifica tionState": ["TRUE_POSITIVE"] } } </pre>	

- 對於目標類型，請選擇AWS 服務，對於選取目標，選擇目標，例如 Amazon SNS 主題或 AWS Lambda 函數。當接收到符合規則中定義之事件模式的事件時，就會觸發目標。

如需建立規則的詳細資訊，請參閱 [《Amazon EventBridge 使用者指南》](#) 中的 [建立對事件做出反應的 Amazon EventBridge 規則](#)。

使用自訂動作將問題清單和洞見結果傳送至 EventBridge

若要使用 AWS Security Hub CSPM 自訂動作將問題清單或洞見結果傳送至 Amazon EventBridge，您必須先在 Security Hub CSPM 中建立自訂動作。然後，您可以在 EventBridge 中定義套用至自訂動作的規則。

您最多可以建立 50 個自訂動作。

如果您啟用跨區域彙總，並從彙總區域管理調查結果，請在彙總區域中建立自訂動作。

EventBridge 中的規則使用自訂動作中的 Amazon Resource Name (ARN)。

建立自訂動作

當您在 AWS Security Hub CSPM 中建立自訂動作時，您可以指定其名稱、描述和唯一識別符。

自訂動作會指定 EventBridge 事件符合 EventBridge 規則時要採取的動作。Security Hub CSPM 會將每個問題清單做為事件傳送至 EventBridge。

選擇您偏好的方法，然後依照步驟建立自訂動作。

Console

在 Security Hub CSPM 中建立自訂動作（主控台）

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇 Settings (設定)，然後選擇 Custom actions (自訂動作)。
3. 選擇 Create custom action (建立自訂動作)。
4. 為動作提供 Name (名稱)、Description (描述) 和 Custom action ID (自訂動作 ID)。

Name (名稱) 必須小於 20 個字元。

每個 AWS 帳戶的自訂動作 ID 必須是唯一的。

5. 選擇 Create custom action (建立自訂動作)。
6. 記下 Custom action ARN (自訂動作 ARN)。在 EventBridge 中建立與此動作建立關聯的規則時，您需要使用 ARN。

API

建立自訂動作 (API)

使用 [CreateActionTarget](#) 操作。如果您使用的是 AWS CLI，請執行 [create-action-target](#) 命令。

下列範例會建立自訂動作，將問題清單傳送至修復工具。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

```
$ aws securityhub create-action-target --name "Send to remediation" --description  
"Action to send the finding for remediation tracking" --id "Remediation"
```

在 EventBridge 中定義規則

若要在 Amazon EventBridge 中觸發自訂動作，您必須在 EventBridge 中建立對應的規則。規則定義包含自訂動作的 Amazon Resource Name (ARN)。

Security Hub 調查結果 - 自訂動作事件的事件模式格式如下：

```
{  
  "source": [  

```

```
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Security Hub Insight 結果事件的事件模式格式如下：

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

在這兩種模式中，<custom action ARN>都是自訂動作的 ARN。您可以設定套用至多個自訂動作的規則。

此處提供的指示適用於 EventBridge 主控台。當您使用主控台時，EventBridge 會自動建立必要的資源型政策，讓 EventBridge 能夠寫入 CloudWatch Logs。

您也可以使用 EventBridge [PutRule](#) API 的 API 操作。不過，如果您使用 EventBridge API，則必須建立以資源為基礎的政策。如需所需政策的詳細資訊，請參閱《Amazon EventBridge 使用者指南》中的 [CloudWatch Logs 許可](#)。

在 EventBridge (EventBridge 主控台) 中定義規則

1. 前往 <https://console.aws.amazon.com/events/> 開啟 Amazon EventBridge 主控台。
2. 在導覽窗格中，選擇規則。
3. 選擇建立規則。
4. 輸入規則的名稱和描述。
5. 針對事件匯流排，選擇要與此規則建立關聯的事件匯流排。如果您想要此規則匹配來自您的帳戶的事件，請選取預設值。當您帳戶中的 AWS 服務發出事件時，一律會前往您帳戶的預設事件匯流排。

6. 針對規則類型，選擇具有事件模式的規則。
7. 選擇下一步。
8. 在事件來源，選擇 AWS 事件。
9. 針對事件模式，選擇事件模式表單。
10. 在事件來源欄位中，選擇 AWS 服務。
11. 針對 AWS 服務，選擇 Security Hub。
12. 針對 Event type (事件類型)，執行下列其中一項操作：
 - 若要在將問題清單傳送到自訂動作時建立要套用的規則，請選擇 Security Hub 問題清單 - 自訂動作。
 - 若要在將洞見結果傳送到自訂動作時建立要套用的規則，請選擇 Security Hub Insight 結果。
13. 選擇特定自訂動作 ARNs，新增自訂動作 ARN。

如果規則適用於多個自訂動作，請選擇新增以新增更多自訂動作 ARNs。
14. 選擇下一步。
15. 在選取目標下，選擇並設定符合此規則時要叫用的目標。
16. 選擇下一步。
17. (選用) 為規則輸入一或多個標籤。如需詳細資訊，請參閱《Amazon EventBridge 使用者指南》中的 [Amazon EventBridge 標籤](#)。
18. 選擇下一步。
19. 檢閱規則的詳細資訊，然後選擇建立規則。

當您對帳戶中的問題清單或洞見結果執行自訂動作時，事件會在 EventBridge 中產生。

選取問題清單和洞見結果的自訂動作

建立 AWS Security Hub CSPM 自訂動作和 Amazon EventBridge 規則之後，您可以將問題清單和洞見結果傳送至 EventBridge 以進行自動管理和處理。

事件只會在檢視事件的帳戶中傳送至 EventBridge。如果您使用管理員帳戶檢視問題清單，事件會傳送至管理員帳戶中的 EventBridge。

若要讓 AWS API 呼叫有效，目標程式碼的實作必須將角色切換為成員帳戶。這也表示您切換到的角色必須部署到需要採取動作的每個成員。

將問題清單傳送至 EventBridge (主控台)

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 顯示問題清單：
 - 從問題清單，您可以檢視所有已啟用產品整合和控制項的問題清單。
 - 從安全標準中，您可以導覽至從特定控制項產生的問題清單。如需詳細資訊，請參閱[檢閱 Security Hub CSPM 中控制項的詳細資訊](#)。
 - 從整合中，您可以導覽至已啟用整合所產生的問題清單。如需詳細資訊，請參閱[從 Security Hub CSPM 整合檢視問題清單](#)。
 - 在 Insights 中，您可以導覽至調查結果清單以取得洞見結果。如需詳細資訊，請參閱[在 Security Hub CSPM 中檢閱洞見並採取行動](#)。
3. 選取要傳送至 EventBridge 的調查結果。您一次最多可以選取 20 個問題清單。
4. 從動作中，選擇與要套用的 EventBridge 規則相符的自訂動作。

Security Hub CSPM 會為每個問題清單傳送個別的 Security Hub 問題清單 - 自訂動作事件。

將洞見結果傳送至 EventBridge (主控台)

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇 Insights。
3. 在洞見頁面上，選擇包含要傳送至 EventBridge 之結果的洞見。
4. 選取要傳送至 EventBridge 的洞見結果。您一次最多可以選取 20 個結果。
5. 從動作中，選擇與要套用的 EventBridge 規則相符的自訂動作。

在 Security Hub CSPM 中使用儀表板

在 Security Hub CSPM 主控台上，摘要儀表板會顯示您的風險、攻擊序列和安全性涵蓋範圍摘要。此儀表板可協助您根據不同安全功能的嚴重性和帳戶涵蓋範圍來識別風險和攻擊序列。每次開啟儀表板時，它都會自動重新整理。不過請注意，安全分數和控制狀態會每 24 小時重新整理一次。

您可以透過新增和移除不同的安全小工具來自訂摘要儀表板。您也可以指定篩選條件來擷取和顯示特定類型的資料。如果您自訂儀表板，Security Hub 會儲存您的自訂設定。如果您帳戶的其他使用者自訂儀表板，其變更會與您的自訂設定獨立儲存。

如果您在 Security Hub CSPM 中設定了跨區域彙總，摘要儀表板會顯示您的彙總資料。如果您的帳戶是組織的委派管理員帳戶，則資料會包含您帳戶和成員帳戶的調查結果。如果您的帳戶是成員帳戶或獨立帳戶，資料只會包含您帳戶的調查結果。

主題

- [摘要儀表板的可用小工具](#)
- [在 Security Hub CSPM 中篩選摘要儀表板](#)
- [在 Security Hub CSPM 中自訂摘要儀表板](#)

摘要儀表板的可用小工具

摘要儀表板包含小工具，以 AWS 客戶的安全操作和體驗為指引，反映現代雲端安全威脅環境。有些小工具預設會顯示，有些則不會顯示。您可以新增或移除小工具來自訂儀表板的檢視。

若要新增小工具，請選擇儀表板頂端的新增小工具。然後，您可以瀏覽可用的小工具清單，或在搜尋列中輸入小工具的標題。當您找到要新增的小工具時，請將其拖曳到要在儀表板上顯示的位置。如需詳細資訊，請參閱[自訂儀表板](#)。

預設顯示的小工具

根據預設，摘要儀表板包含下列小工具。

最高威脅序列

顯示最高嚴重性的威脅序列。威脅序列調查結果稱為 Amazon GuardDuty 中的攻擊序列調查結果，可關聯多個事件以識別對您 AWS 環境的潛在威脅。威脅序列可能包括您環境中正在進行或最近的攻擊行為（在 24 小時內），進而導致進一步入侵。您必須啟用 GuardDuty 和 GuardDuty S3 保護，才能在 Security Hub CSPM 中接收威脅序列調查結果。

最高風險

顯示您環境中最高風險的摘要。小工具頂端會顯示每個嚴重性層級的風險計數。您可以選擇嚴重性等級，以前往風險頁面，並將風險篩選為選取的嚴重性等級。環境中出現次數最多的風險會先出現。此小工具可協助您排定要減輕哪些風險的優先順序。

安全涵蓋範圍

根據涵蓋範圍控制調查結果，摘要說明您的安全涵蓋範圍範圍。涵蓋範圍控制會檢查特定 AWS 服務及其功能是否已啟用（例如，[【Macie.1】應啟用 Amazon Macie](#)）。此小工具可協助您確保您有涵蓋範圍控制的 PASSED 調查結果。Security Hub CSPM 主控台提供此小工具的連結，協助您啟

用缺少的安全功能。我們建議您使用中央組態，以跨多個 AWS 帳戶 和 啟用缺少的安全功能 AWS 區域。如需詳細資訊，請參閱[了解 Security Hub CSPM 中的中央組態](#)。

安全標準

顯示您最近的摘要安全分數，以及每個 Security Hub CSPM 標準的安全分數。安全分數範圍介於 0-100% 之間，代表相對於所有已啟用控制項的通過控制項比例。如需這些分數的詳細資訊，請參閱[計算安全分數的方法](#)。此小工具可協助您了解整體安全狀態。

調查結果最多的資產

提供具有最多調查結果的資源、帳戶和應用程式的概觀。清單會依問題清單數量以遞減順序排序。在小工具中，每個索引標籤都會顯示該類別中前六個項目，依嚴重性和資源類型分組。如果您在總調查結果欄中選擇號碼，Security Hub CSPM 會開啟顯示資產調查結果的頁面。此小工具可協助您快速識別哪些核心資產具有潛在的安全威脅。

依區域分類的問題清單

在啟用 Security Hub CSPM 的每個 AWS 區域 中，顯示依嚴重性分組的問題清單總數。此小工具可協助您識別可能影響特定區域的安全問題。如果您在彙總區域中開啟儀表板，此小工具可協助您監控每個連結區域中的潛在安全問題。

最常見的威脅類型

提供 AWS 環境中 10 種最常見威脅類型的明細。這包括威脅，例如權限提升、使用公開的登入資料，或與惡意 IP 地址通訊。

若要檢視此資料，必須啟用[Amazon GuardDuty](#)。如果是，請在此小工具中選擇威脅類型，以開啟 GuardDuty 主控台並檢閱與此威脅相關的調查結果。此小工具可協助您在其他安全問題的環境中評估潛在威脅。

含有漏洞的軟體漏洞

提供存在於您 AWS 環境中且具有已知漏洞的軟體漏洞摘要。您也可以檢閱已完成且沒有可用修正的漏洞明細。

若要檢視此資料，必須啟用[Amazon Inspector](#)。如果是，在此小工具中選擇統計資料以開啟 Amazon Inspector 主控台，並檢閱有關漏洞的更多詳細資訊。此小工具可協助您在發生其他安全問題的情況下評估軟體漏洞。

隨時間變化的新問題清單

顯示過去 90 天內新每日調查結果數量的趨勢。您可以依嚴重性或供應商細分資料，以取得其他內容。此小工具可協助您了解在過去 90 天內，是否在特定時間發現磁碟區峰值或下降。

問題清單最多的資源

提供產生最多調查結果的資源摘要，依下列資源類型細分：Amazon Simple Storage Service (Amazon S3) 儲存貯體、Amazon Elastic Compute Cloud (Amazon EC2) 執行個體和 AWS Lambda 函數。

在小工具中，每個索引標籤都著重於上述其中一個資源類型，列出產生最多問題清單的 10 個資源執行個體。若要檢閱特定資源的問題清單，請選擇資源執行個體。此小工具可協助您分類與常見 AWS 資源相關聯的安全調查結果。

預設隱藏的小工具

下列小工具也可用於摘要儀表板，但預設為隱藏。

調查結果最多的 AMIs

提供產生最多問題清單的 10 個 Amazon Machine Image (AMIs) 的清單。只有在您的帳戶啟用 Amazon EC2 時，才能使用此資料。它可協助您識別哪些 AMIs 構成潛在的安全風險。

問題清單最多的 IAM 主體

提供產生最多問題清單的 10 個 AWS Identity and Access Management (IAM) 使用者清單。此小工具可協助您執行管理和計費任務。它會顯示哪些使用者對 Security Hub CSPM 用量的貢獻最大。

調查結果最多的帳戶（依嚴重性）

顯示已產生最多調查結果的 10 個帳戶的圖表，依嚴重性分組。此小工具可協助您判斷要專注於哪些帳戶分析和修復工作。

調查結果最多的帳戶（依資源類型）

顯示已產生最多問題清單的 10 個帳戶的圖表，依資源類型分組。此小工具可協助您判斷要優先分析和修復哪些帳戶和資源類型。

洞見

列出五個 [Security Hub CSPM 受管洞察](#) 及其產生的調查結果數量。Insights 會識別需要注意的特定安全區域。

AWS 整合的最新調查結果

顯示您在 Security Hub CSPM 中從 [整合 AWS 服務](#) 收到的調查結果數量。它也會顯示您最近從每個整合服務收到問題清單的時間。此小工具提供來自多個的合併調查結果資料 AWS 服務。若要向下切入，請選擇整合式服務。Security Hub CSPM 接著會開啟該服務的主控台。

在 Security Hub CSPM 中篩選摘要儀表板

您可以在 Security Hub CSPM 主控台上策劃摘要儀表板，使其僅包含與您最相關的安全資料。例如，如果您是應用程式團隊的成員，您可以在生產環境中為關鍵應用程式建立專用檢視。如果您是安全團隊的成員，您可以建立專用檢視，協助您專注於高嚴重性的問題清單。

若要建立這些精選檢視，請在儀表板上方的篩選條件方塊中輸入篩選條件。如果您套用篩選條件，則這些條件適用於儀表板上的所有資料和小工具，但 Insights 和安全標準小工具中的資料除外。如需儀表板上可用小工具的清單，請參閱 [摘要儀表板的可用小工具](#)。

您可以使用下列欄位來篩選資料：

- 帳戶名稱
- 帳戶 ID
- 應用程式 ARN
- Application name (應用程式名稱)
- 產品名稱（適用於將問題清單傳送至 Security Hub CSPM 的 AWS 服務 或第三方產品）
- 記錄狀態
- 區域
- 資源標籤
- 嚴重性
- 工作流程狀態

根據預設，儀表板資料會使用下列條件進行篩選：Workflow.Status 為 NOTIFIED 或 NEW，RecordState 為 ACTIVE。這些條件會顯示在儀表板上，篩選條件方塊下方。若要移除這些條件，請在篩選條件字符中選擇 X，以用於您要移除的條件。

如果您套用要再次使用的篩選條件，您可以將其儲存為篩選條件集。篩選條件集是您建立並儲存的一組篩選條件，可在檢閱摘要儀表板上的資料時重新套用。您可以建立和儲存使用下列欄位以外任何可用欄位的篩選條件集：應用程式 ARN、應用程式名稱和資源標籤。

建立和儲存篩選條件集

請依照下列步驟建立和儲存篩選條件集。

建立和儲存篩選條件集

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇摘要。
3. 在摘要儀表板上方的篩選條件方塊中，輸入篩選條件集的篩選條件條件。
4. 在清除篩選條件功能表中，選擇儲存新的篩選條件集。
5. 在儲存篩選條件集對話方塊中，輸入篩選條件集的名稱。
6. （選用）若要在每次開啟摘要頁面時使用預設篩選條件集，請選取 選項將其設定為預設檢視。
7. 選擇儲存。

若要在已建立和儲存的篩選條件集之間切換，請使用摘要儀表板上方的選擇篩選條件集功能表。當您選取篩選條件集時，Security Hub CSPM 會將篩選條件集的條件套用至儀表板上的資料。

更新或刪除篩選條件集

請依照下列步驟更新或刪除現有的篩選條件集。如果您刪除目前設定為摘要儀表板預設檢視的篩選條件集，您的預設檢視會重設為預設 Security Hub CSPM 檢視。

更新或刪除篩選條件集

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇摘要。
3. 在摘要頁面上方的選擇篩選條件集選單中，選擇篩選條件集。
4. 在清除篩選條件功能表中，執行下列其中一項操作：
 - 若要更新篩選條件集，請選擇更新目前的篩選條件集。然後，在出現的對話方塊中輸入您的變更。
 - 若要刪除篩選條件集，請選擇刪除目前的篩選條件集。然後，在出現的對話方塊中選擇刪除。

在 Security Hub CSPM 中自訂摘要儀表板

您可以在 Security Hub CSPM 主控台上以多種方式自訂摘要儀表板。例如，您可以從儀表板新增和移除小工具。您也可以儀表板上重新排列和調整小工具的大小。如需可用小工具的清單和每個小工具的描述，請參閱 [摘要儀表板的可用小工具](#)。

如果您自訂儀表板，Security Hub CSPM 會立即套用您的變更，並儲存新的儀表板設定。您的變更會套用至所有 AWS 區域 和瀏覽器中儀表板的檢視。

自訂摘要儀表板

1. 開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，選擇摘要。
3. 執行下列任何一項：
 - 若要新增小工具，請選擇頁面右上角的新增小工具。在搜尋列中，輸入要新增的小工具標題。然後，將小工具拖曳到您想要的位置。
 - 若要移除小工具，請選擇小工具右上角的三個點。
 - 若要移動小工具，請選擇小工具左上角的控點，然後將小工具拖曳至您想要的位置。
 - 若要變更小工具的大小，請選擇小工具右下角的調整大小控制代碼。拖曳小工具的邊緣，直到小工具是您偏好的大小。

若要後續還原原始設定，請選擇頁面頂端的重設為預設配置。

Security Hub CSPM 的區域限制

某些 AWS Security Hub CSPM 功能僅適用於特定 AWS 區域。下列各節指定這些區域限制。如需 Security Hub CSPM 目前可用的所有區域的完整清單，請參閱《》中的 [AWS Security Hub 端點和配額](#) AWS 一般參考。

跨區域彙總限制

在 中 AWS GovCloud (US) Regions，[跨區域彙總](#) AWS GovCloud (US) Regions 僅適用於跨 的問題清單、問題清單更新和洞見。具體而言，您只能在 AWS GovCloud（美國東部）和 AWS GovCloud（美國西部）區域之間彙總問題清單、問題清單更新和洞見。

在中國區域中，跨區域彙總僅適用於整個中國區域的調查結果、調查結果更新和洞見。具體而言，您只能在中國（北京）和中國（寧夏）區域之間彙總問題清單、問題清單更新和洞見。

您無法使用預設停用的區域做為彙總區域。如需預設停用的區域清單，請參閱《AWS 帳戶管理 參考指南》[AWS 區域 中的在您的帳戶中啟用或停用](#)。

依區域的整合可用性

有些整合無法全部使用 AWS 區域。在 Security Hub CSPM 主控台上，如果您目前登入的區域中無法使用整合，整合就不會出現在整合頁面上。

中國（北京）和中國（寧夏）區域支援的整合

在中國（北京）和中國（寧夏）區域中，Security Hub CSPM 僅支援與 [的下列整合 AWS 服務](#)：

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager 修補程式管理員

在中國（北京）和中國（寧夏）區域中，Security Hub CSPM 僅支援下列 [第三方整合](#)：

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 區域中支援的整合

在 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 區域中，Security Hub CSPM 僅支援與 [下列整合 AWS 服務](#)：

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- IAM Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender

在 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 區域中，Security Hub CSPM 僅支援下列 [第三方整合](#)：

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator

- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series (僅適用於 AWS GovCloud (美國西部))
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

區域標準可用性

[AWS Control Tower 服務受管標準](#)僅適用於 AWS 區域 AWS Control Tower 支援的。如需 AWS Control Tower 目前支援的區域清單，請參閱AWS Control Tower 《使用者指南》中的[AWS 區域 如何使用 AWS Control Tower](#)。

[AWS 資源標記標準](#)不適用於亞太區域 (台北) 區域。

其他安全標準可在目前提供 Security Hub CSPM 的所有區域中使用。

依區域的控制項可用性

有些 Security Hub CSPM 控制項無法全部使用 AWS 區域。如需每個區域中無法使用的控制項清單，請參閱 [Security Hub CSPM 控制項的區域限制](#)。

在 Security Hub CSPM 主控台上，如果控制項無法在您目前登入的區域中使用，則控制項不會出現在控制項清單中。例外狀況是彙總區域。如果您設定彙總區域並登入該區域，主控台會顯示彙總區域或一個或多個連結區域中可用的控制項。

Security Hub CSPM 控制項的區域限制

有些 AWS Security Hub CSPM 控制項無法全部使用 AWS 區域。此頁面指定在特定區域中無法使用哪些控制項。

在 Security Hub CSPM 主控台上，如果控制項無法在您目前登入的區域中使用，則控制項不會出現在控制項清單中。例外是彙總區域。如果您設定彙總區域並登入該區域，主控台會顯示彙總區域或一或多個連結區域中可用的控制項。

AWS 區域

- [美國東部 \(維吉尼亞北部\)](#)
- [美國東部 \(俄亥俄\)](#)
- [美國西部 \(加利佛尼亞北部\)](#)
- [美國西部 \(奧勒岡\)](#)
- [非洲 \(開普敦\)](#)
- [亞太地區 \(香港\)](#)
- [亞太地區 \(海德拉巴\)](#)
- [亞太地區 \(雅加達\)](#)
- [亞太地區 \(馬來西亞\)](#)
- [亞太地區 \(墨爾本\)](#)
- [亞太地區 \(孟買\)](#)
- [亞太區域 \(紐西蘭\)](#)
- [亞太地區 \(大阪\)](#)
- [亞太地區 \(首爾\)](#)
- [亞太地區 \(新加坡\)](#)
- [亞太地區 \(悉尼\)](#)
- [亞太區域 \(台北\)](#)
- [亞太區域 \(泰國\)](#)
- [亞太地區 \(東京\)](#)
- [加拿大 \(中部\)](#)
- [加拿大西部 \(卡加利\)](#)
- [中國 \(北京\)](#)
- [中國 \(寧夏\)](#)
- [歐洲 \(法蘭克福\)](#)
- [歐洲 \(愛爾蘭\)](#)

- [歐洲 \(倫敦\)](#)
- [歐洲 \(米蘭\)](#)
- [Europe \(Paris\)](#)
- [歐洲 \(西班牙\)](#)
- [歐洲 \(斯德哥爾摩\)](#)
- [歐洲 \(蘇黎世\)](#)
- [以色列 \(特拉維夫\)](#)
- [墨西哥 \(中部\)](#)
- [Middle East \(Bahrain\)](#)
- [中東 \(阿拉伯聯合大公國\)](#)
- [南美洲 \(聖保羅\)](#)
- [AWS GovCloud \(美國東部\)](#)
- [AWS GovCloud \(美國西部\)](#)

美國東部 (維吉尼亞北部)

美國東部 (維吉尼亞北部) 區域不支援下列控制項。

- [【ElastiCache.4】ElastiCache 複寫群組應靜態加密](#)
- [【ElastiCache.5】ElastiCache 複寫群組應在傳輸中加密](#)
- [【ElastiCache.6】舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】ElastiCache 叢集不應使用預設子網路群組](#)
- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【S3.24】S3 多區域存取點應啟用封鎖公開存取設定](#)

美國東部 (俄亥俄)

美國東部 (俄亥俄) 區域不支援下列控制項。

- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)

- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IoT TwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoT TwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoT TwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoT TwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoT Wireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoT Wireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoT Wireless.3】 AWS IoT FUOTA 任務應加上標籤](#)

- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

美國西部 (加利佛尼亞北部)

美國西部（加利佛尼亞北部）區域不支援下列控制項。

- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)
- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)

- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Connect.1】Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DocumentDB.1】Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【EC2.173】具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】ECR 公有儲存庫應加上標籤](#)
- [【FraudDetector.1】Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】Amazon Fraud Detector 標籤應加上標籤](#)

- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.47】 RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.48】 RDS for MySQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)

- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

美國西部 (奧勒岡)

美國西部（奧勒岡）區域不支援下列控制項。

- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)

- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

非洲 (開普敦)

非洲（開普敦）區域不支援下列控制項。

- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)
- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)

- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【DMS.10】Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DocumentDB.1】Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.14】安全群組不應允許從 0.0.0.0/0 或 :::/0 傳入連接埠 3389](#)

- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【ES.3】 Elasticsearch 網域應該加密節點之間傳送的資料](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】 AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】 AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】 AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)

- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtTwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtTwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtTwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtTwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【RDS.1】 RDS 快照應為私有](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)
- [【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)

- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應該啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

亞太地區 (香港)

亞太區域 (香港) 區域不支援下列控制項。

- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)
- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)

- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Connect.1】Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DynamoDB.3】DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.24】不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.58】VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.173】具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】ECR 公有儲存庫應加上標籤](#)
- [【EventBridge.4】EventBridge 全域端點應啟用事件複寫](#)

- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtTwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtTwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtTwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtTwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)

- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SES.1】 SES 聯絡人清單應加上標籤](#)
- [【SES.2】 SES 組態集應加上標籤](#)
- [【SES.3】 SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

亞太地區 (海德拉巴)

亞太區域（海德拉巴）區域不支援下列控制項。

- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppConfig.1】 AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】 AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】 AWS AppConfig 環境應加上標籤](#)
- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)

- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【Backup.1】AWS Backup 復原點應靜態加密](#)
- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.3】CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)

- [【CloudTrail.6】 確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)
- [【CloudTrail.7】 確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】 Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】 Cognito 身分集區不應允許未驗證的身分](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【Detective.1】 應標記 Detective 行為圖表](#)
- [【DMS.2】 DMS 憑證應加上標籤](#)
- [【DMS.3】 DMS 事件訂閱應加上標籤](#)
- [【DMS.4】 DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】 DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】 DMS 端點應使用 SSL](#)
- [【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】 DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.14】 安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】 Amazon EC2 啟動範本不應將公IPs 指派給網路介面](#)

- [【EC2.34】 EC2 傳輸閘道路由表應加上標籤](#)
- [【EC2.40】 EC2 NAT 閘道應加上標籤](#)
- [【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【EC2.180】 EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.181】 EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.6】 舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】 ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)

- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.2】 GuardDuty 篩選條件應加上標籤](#)
- [【IAM.1】 IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】 IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.5】 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】 IAM 身分不應連接 AWSCloudShellFullAccess 政策](#)
- [【Inspector.1】 應啟用 Amazon Inspector EC2 掃描](#)
- [【Inspector.2】 應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】 應啟用 Amazon Inspector Lambda 標準掃描](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】 AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】 AWS IoT Core 角色別名應加上標籤](#)

- [【IoT.6】 AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MQ.4】 Amazon MQ 代理程式應加上標籤](#)
- [【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式](#)

- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.4】 MSK 叢集應停用公有存取](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【MSK.6】 MSK 叢集應停用未驗證的存取](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.9】 應標記 OpenSearch 網域](#)
- [【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)

- [【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)
- [【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】 應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】 應標記 SageMaker 映像](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.17】 SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)

- [【SageMaker.18】 使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.3】 SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【SQS.1】 Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】 SQS 佇列應加上標籤](#)
- [【SQS.3】 SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.6】 SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)
- [【Transfer.3】 Transfer Family 連接器應該已啟用記錄](#)
- [【Transfer.4】 Transfer Family 協議應加上標籤](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

亞太地區 (雅加達)

亞太區域 (雅加達) 區域不支援下列控制項。

- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】 App Runner 服務應加上標籤](#)

- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【Backup.1】AWS Backup 復原點應靜態加密](#)
- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.3】CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)

- [【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料](#)
- [【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料](#)
- [【CodeBuild.3】CodeBuild S3 日誌應加密](#)
- [【CodeBuild.4】CodeBuild AWS Config專案環境應具有記錄 URL](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Connect.1】Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【Detective.1】應標記 Detective 行為圖表](#)
- [【DMS.2】DMS 憑證應加上標籤](#)
- [【DMS.3】DMS 事件訂閱應加上標籤](#)
- [【DMS.4】DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】DMS 端點應使用 SSL](#)
- [【DMS.10】Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DocumentDB.1】Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】Amazon DocumentDB 叢集應在傳輸中加密](#)

- [【DynamoDB.3】DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.14】安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389](#)
- [【EC2.22】應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.24】不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.51】EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.58】VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.173】具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.177】應標記 EC2 流量鏡像工作階段](#)
- [【EC2.179】應標記 EC2 流量鏡像目標](#)
- [【ECR.4】ECR 公有儲存庫應加上標籤](#)
- [【EFS.1】彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】Amazon EFS 磁碟區應位於備份計劃中](#)
- [【ELB.17】具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ElastiCache.1】ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.6】舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【EventBridge.4】EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【GuardDuty.2】GuardDuty 篩選條件應加上標籤](#)
- [【IAM.18】確保已建立支援角色來使用 管理事件 AWS 支援](#)

- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】 AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】 AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】 AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)

- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.11】 S3 一般用途儲存貯體應啟用事件通知](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)

- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【ServiceCatalog.1】 Service Catalog 產品組合只能在 AWS 組織內共用](#)
- [【SQS.1】 Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】 SQS 佇列應加上標籤](#)
- [【SQS.3】 SQS 佇列存取政策不應允許公開存取](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

亞太地區 (馬來西亞)

亞太區域 (馬來西亞) 區域不支援下列控制項。

- [【ACM.1】 匯入和 ACM 發行的憑證應在指定的期間之後續約](#)
- [【ACM.2】 由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)
- [【Account.1】 應針對 提供安全性聯絡資訊 AWS 帳戶](#)
- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppConfig.1】 AWS AppConfig 應用程式應加上標籤](#)

- [【AppConfig.2】AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】AWS AppConfig 環境應加上標籤](#)
- [【AppConfig.4】AWS AppConfig 應標記延伸關聯](#)
- [【AppFlow.1】Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.2】AWS AppSync 應該啟用欄位層級記錄](#)
- [【AppSync.5】AWS AppSync GraphQL APIs不應使用 API 金鑰進行身分驗證](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【Athena.4】Athena 工作群組應該已啟用記錄](#)
- [【AutoScaling.2】Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域](#)
- [【AutoScaling.3】Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【AutoScaling.6】Auto Scaling 群組應在多個可用區域中使用多個執行個體類型](#)
- [【AutoScaling.9】Amazon EC2 Auto Scaling 群組應使用 Amazon EC2 啟動範本](#)
- [【Backup.1】AWS Backup 復原點應靜態加密](#)
- [【Backup.2】AWS Backup 復原點應加上標籤](#)
- [【Backup.4】應標記 AWS Backup 報告計劃](#)
- [【Batch.1】批次任務佇列應加上標籤](#)
- [【Batch.2】批次排程政策應加上標籤](#)
- [【Batch.3】批次運算環境應加上標籤](#)
- [【Batch.4】應標記受管批次運算環境中的運算資源屬性](#)
- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)

- [【CloudFormation.3】CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)
- [【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)
- [【CloudTrail.10】CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys](#)
- [【CloudWatch.17】應啟用 CloudWatch 警示動作](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料](#)
- [【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料](#)
- [【CodeBuild.3】CodeBuild S3 日誌應加密](#)
- [【CodeBuild.4】CodeBuild AWS Config專案環境應具有記錄 URL](#)
- [【CodeBuild.7】CodeBuild 報告群組匯出應靜態加密](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)

- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】Cognito 身分集區不應允許未驗證的身分](#)
- [【Cognito.3】Cognito 使用者集區的密碼政策應具有強大的組態](#)
- [【Cognito.4】Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證](#)
- [【Cognito.5】應為 Cognito 使用者集區啟用 MFA](#)
- [【Cognito.6】Cognito 使用者集區應啟用刪除保護](#)
- [【Connect.1】Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DataFirehose.1】Firehose 交付串流應靜態加密](#)
- [【DataSync.1】DataSync 任務應該已啟用記錄](#)
- [【DataSync.2】應標記 DataSync 任務](#)
- [【Detective.1】應標記 Detective 行為圖表](#)
- [【DMS.2】DMS 憑證應加上標籤](#)
- [【DMS.3】DMS 事件訂閱應加上標籤](#)
- [【DMS.4】DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】DMS 端點應使用 SSL](#)
- [【DMS.10】Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DocumentDB.1】Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】Amazon DocumentDB 手動叢集快照不應公開](#)

- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】 Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.4】 DynamoDB 資料表應存在於備份計畫中](#)
- [【DynamoDB.6】 DynamoDB 資料表應該已啟用刪除保護](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】 已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】 Amazon EC2 啟動範本不應將公IPs 指派給網路介面](#)
- [【EC2.28】 備份計畫應涵蓋 EBS 磁碟區](#)
- [【EC2.34】 EC2 傳輸閘道路由表應加上標籤](#)
- [【EC2.40】 EC2 NAT 閘道應加上標籤](#)
- [【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.53】 EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.54】 EC2 安全群組不應允許從 :::/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.55】 VPCs應使用 ECR API 的介面端點進行設定](#)
- [【EC2.56】 VPCs應使用 Docker 登錄檔的介面端點進行設定](#)
- [【EC2.57】 VPCs應使用 Systems Manager 的介面端點進行設定](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.171】 EC2 VPN 連線應該已啟用記錄](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.174】 EC2 DHCP 選項集應加上標籤](#)

- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.176】 EC2 字首清單應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.178】 應標記 EC2 流量鏡像篩選條件](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【EC2.180】 EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.181】 EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定](#)
- [【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)
- [【ECR.2】 ECR 私有儲存庫應設定標籤不可變性](#)
- [【ECR.3】 ECR 儲存庫應至少設定一個生命週期政策](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ECR.5】 ECR 儲存庫應使用客戶受管加密 AWS KMS keys](#)
- [【ECS.3】 ECS 任務定義不應共用主機的程序命名空間](#)
- [【ECS.4】 ECS 容器應以非特殊權限執行](#)
- [【ECS.5】 ECS 任務定義應將容器設定為僅限對根檔案系統的唯讀存取](#)
- [【ECS.8】 不應將秘密做為容器環境變數傳遞](#)
- [【ECS.9】 ECS 任務定義應具有記錄組態](#)
- [【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行](#)
- [【ECS.12】 ECS 叢集應使用 Container Insights](#)
- [【ECS.17】 ECS 任務定義不應使用主機網路模式](#)
- [【ECS.19】 ECS 容量提供者應啟用受管終止保護](#)
- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【EFS.3】 EFS 存取點應強制執行根目錄](#)
- [【EFS.4】 EFS 存取點應強制執行使用者身分](#)
- [【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯](#)
- [【EFS.7】 EFS 檔案系統應該啟用自動備份](#)
- [【EFS.8】 EFS 檔案系統應靜態加密](#)

- [【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)
- [【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密](#)
- [【EKS.7】 EKS 身分提供者組態應加上標籤](#)
- [【EKS.8】 EKS 叢集應該啟用稽核記錄](#)
- [【ELB.10】 Classic Load Balancer 應跨越多個可用區域](#)
- [【ELB.12】 Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.13】 應用程式、網路和閘道負載平衡器應跨越多個可用區域](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.2】 ElastiCache 叢集應該啟用自動次要版本升級](#)
- [【ElastiCache.3】 ElastiCache 複寫群組應該啟用自動容錯移轉](#)
- [【ElastiCache.4】 ElastiCache 複寫群組應靜態加密](#)
- [【ElastiCache.5】 ElastiCache 複寫群組應在傳輸中加密](#)
- [【ElastiCache.6】 舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】 ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【EMR.2】 應啟用 Amazon EMR 封鎖公開存取設定](#)
- [【EMR.3】 Amazon EMR 安全組態應靜態加密](#)
- [【EMR.4】 Amazon EMR 安全組態應在傳輸中加密](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【ES.9】 應標記 Elasticsearch 網域](#)
- [【EventBridge.3】 EventBridge 自訂事件匯流排應連接以資源為基礎的政策](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)

- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.1】 FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)
- [【FSx.2】 FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)
- [【FSx.3】 FSx for OpenZFS 檔案系統應設定為異地同步備份部署](#)
- [【FSx.4】 FSx for NetApp ONTAP 檔案系統應設定為異地同步備份部署](#)
- [【FSx.5】 FSx for Windows File Server 檔案系統應設定為異地同步備份部署](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【Glue.1】 AWS Glue 工作應加上標籤](#)
- [【Glue.3】 AWS Glue 機器學習轉換應該靜態加密](#)
- [【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.2】 GuardDuty 篩選條件應加上標籤](#)
- [【GuardDuty.5】 應啟用 GuardDuty EKS 稽核日誌監控](#)
- [【GuardDuty.6】 應啟用 GuardDuty Lambda 保護](#)
- [【GuardDuty.7】 應啟用 GuardDuty EKS 執行期監控](#)
- [【GuardDuty.8】 應啟用 EC2 的 GuardDuty 惡意軟體防護](#)
- [【GuardDuty.9】 應啟用 GuardDuty RDS 保護](#)
- [【GuardDuty.10】 應啟用 GuardDuty S3 保護](#)
- [【GuardDuty.11】 應啟用 GuardDuty 執行期監控](#)
- [【GuardDuty.12】 應啟用 GuardDuty ECS 執行期監控](#)
- [【GuardDuty.13】 應啟用 GuardDuty EC2 執行期監控](#)
- [【IAM.1】 IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】 IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】 IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.6】 應為根使用者啟用硬體 MFA](#)
- [【IAM.7】 IAM 使用者的密碼政策應具有強大的組態](#)

- [【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.9】 應為根使用者啟用 MFA](#)
- [【IAM.10】 IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.11】 確保 IAM 密碼政策至少需要一個大寫字母](#)
- [【IAM.12】 確保 IAM 密碼政策至少需要一個小寫字母](#)
- [【IAM.13】 確保 IAM 密碼政策至少需要一個符號](#)
- [【IAM.14】 確保 IAM 密碼政策至少需要一個數字](#)
- [【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)
- [【IAM.16】 確保 IAM 密碼政策防止密碼重複使用](#)
- [【IAM.17】 確保 IAM 密碼政策在 90 天內過期密碼](#)
- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】 IAM 身分不應連接 AWS CloudShellFullAccess 政策](#)
- [【IAM.28】 應啟用 IAM Access Analyzer 外部存取分析器](#)
- [【Inspector.1】 應啟用 Amazon Inspector EC2 掃描](#)
- [【Inspector.2】 應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】 應啟用 Amazon Inspector Lambda 標準掃描](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)

- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtTwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtTwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtTwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtTwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Kinesis.1】 Kinesis 串流應靜態加密](#)
- [【Kinesis.3】 Kinesis 串流應具有足夠的資料保留期](#)
- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【KMS.5】 不應公開存取 KMS 金鑰](#)
- [【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MQ.4】 Amazon MQ 代理程式應加上標籤](#)
- [【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式](#)
- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密](#)
- [【MSK.2】 MSK 叢集應已設定增強型監控](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)

- [【MSK.4】 MSK 叢集應停用公有存取](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【MSK.6】 MSK 叢集應停用未驗證的存取](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【NetworkFirewall.1】 網路防火牆防火牆應部署在多個可用區域](#)
- [【NetworkFirewall.2】 應啟用網路防火牆記錄](#)
- [【NetworkFirewall.3】 網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.4】 Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)
- [【NetworkFirewall.5】 網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】 無狀態網路防火牆規則群組不應為空](#)
- [【NetworkFirewall.9】 網路防火牆防火牆應啟用刪除保護](#)
- [【NetworkFirewall.10】 網路防火牆防火牆應啟用子網路變更保護](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.9】 應標記 OpenSearch 網域](#)

- [【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【PCA.1】 應停用 AWS 私有 CA 根憑證授權單位](#)
- [【PCA.2】 應標記 AWS 私有 CA 憑證授權單位](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.18】 RDS 執行個體應部署在 VPC 中](#)
- [【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱](#)
- [【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)
- [【RDS.26】 RDS 資料庫執行個體應受備份計劃保護](#)
- [【RDS.27】 RDS 資料庫叢集應靜態加密](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.36】 RDS for PostgreSQL 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.38】 RDS for PostgreSQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.39】 RDS for MySQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.40】 RDS for SQL Server 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.41】 RDS for SQL Server 資料庫執行個體應在傳輸中加密](#)
- [【RDS.42】 RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密](#)
- [【RDS.44】 RDS for MariaDB 資料庫執行個體應在傳輸中加密](#)
- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【RDS.46】 RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中](#)
- [【RDS.47】 RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠](#)

- [【Redshift.16】 Redshift 叢集子網路群組應具有來自多個可用區域的子網路](#)
- [【Redshift.17】 應標記 Redshift 叢集參數群組](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)
- [【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.7】 S3 一般用途儲存貯體應使用跨區域複寫](#)
- [【S3.10】 已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態](#)
- [【S3.11】 S3 一般用途儲存貯體應啟用事件通知](#)
- [【S3.12】 ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取](#)
- [【S3.13】 S3 一般用途儲存貯體應具有生命週期組態](#)
- [【S3.19】 S3 存取點應啟用封鎖公開存取設定](#)
- [【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除](#)
- [【S3.22】 S3 一般用途儲存貯體應記錄物件層級寫入事件](#)
- [【S3.23】 S3 一般用途儲存貯體應記錄物件層級讀取事件](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.4】 SageMaker 端點生產變體的初始執行個體計數應大於 1](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】 應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】 應標記 SageMaker 映像](#)

- [【SageMaker.8】SageMaker 筆記本執行個體應在支援的平台上執行](#)
- [【SageMaker.9】SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.17】SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.18】使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.19】SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.3】SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【ServiceCatalog.1】Service Catalog 產品組合只能在 AWS 組織內共用](#)
- [【SNS.4】SNS 主題存取政策不應允許公開存取](#)
- [【SQS.1】Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】SQS 佇列應加上標籤](#)
- [【SQS.3】SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.4】SSM 文件不應公開](#)
- [【SSM.5】SSM 文件應加上標籤](#)
- [【SSM.6】SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【SSM.7】SSM 文件應啟用封鎖公開共用設定](#)
- [【StepFunctions.1】Step Functions 狀態機器應該已開啟記錄](#)
- [【Transfer.2】Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線](#)
- [【Transfer.3】Transfer Family 連接器應該已啟用記錄](#)
- [【Transfer.4】Transfer Family 協議應加上標籤](#)
- [【Transfer.5】Transfer Family 憑證應加上標籤](#)
- [【Transfer.6】Transfer Family 連接器應加上標籤](#)
- [【Transfer.7】轉移系列設定檔應加上標籤](#)

- [【WAF.1】應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.2】AWS WAF 傳統區域規則應至少有一個條件](#)
- [【WAF.3】AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.4】AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.6】AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.12】AWS WAF 規則應啟用 CloudWatch 指標](#)
- [【WorkSpaces.1】應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】WorkSpaces 根磁碟區應靜態加密](#)

亞太地區 (墨爾本)

亞太區域 (墨爾本) 區域不支援下列控制項。

- [【APIGateway.8】API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】應為 API Gateway V2 階段設定存取記錄](#)
- [【Amplify.1】Amplify 應用程式應加上標籤](#)
- [【Amplify.2】Amplify 分支應加上標籤](#)
- [【AppFlow.1】Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.2】AWS AppSync 應該啟用欄位層級記錄](#)
- [【AppSync.5】AWS AppSync GraphQL APIs 不應使用 API 金鑰進行身分驗證](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【Backup.1】AWS Backup 復原點應靜態加密](#)
- [【Batch.1】批次任務佇列應加上標籤](#)
- [【Batch.3】批次運算環境應加上標籤](#)

- [【Batch.4】 應標記受管批次運算環境中的運算資源屬性](#)
- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.3】 CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】 CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】 Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)

- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【Detective.1】 應標記 Detective 行為圖表](#)
- [【DMS.2】 DMS 憑證應加上標籤](#)
- [【DMS.3】 DMS 事件訂閱應加上標籤](#)
- [【DMS.4】 DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】 DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】 DMS 端點應使用 SSL](#)
- [【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】 DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】 Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】 已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.14】 安全群組不應允許從 0.0.0.0/0 或 :::/0 傳入連接埠 3389](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】 Amazon EC2 啟動範本不應將公 IPs 指派給網路介面](#)
- [【EC2.34】 EC2 傳輸閘道路由表應加上標籤](#)

- [【EC2.40】 EC2 NAT 閘道應加上標籤](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.181】 EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.2】 ElastiCache 叢集應該啟用自動次要版本升級](#)
- [【ElastiCache.3】 ElastiCache 複寫群組應該啟用自動容錯移轉](#)
- [【ElastiCache.4】 ElastiCache 複寫群組應靜態加密](#)
- [【ElastiCache.5】 ElastiCache 複寫群組應在傳輸中加密](#)
- [【ElastiCache.6】 舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】 ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)

- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.1】 FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)
- [【FSx.3】 FSx for OpenZFS 檔案系統應設定為異地同步備份部署](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.2】 GuardDuty 篩選條件應加上標籤](#)
- [【IAM.1】 IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】 IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.5】 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.6】 應為根使用者啟用硬體 MFA](#)
- [【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.10】 IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.11】 確保 IAM 密碼政策至少需要一個大寫字母](#)
- [【IAM.12】 確保 IAM 密碼政策至少需要一個小寫字母](#)
- [【IAM.13】 確保 IAM 密碼政策至少需要一個符號](#)
- [【IAM.14】 確保 IAM 密碼政策至少需要一個數字](#)
- [【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)
- [【IAM.16】 確保 IAM 密碼政策防止密碼重複使用](#)
- [【IAM.17】 確保 IAM 密碼政策在 90 天內過期密碼](#)
- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】 IAM 身分不應連接 AWSCloudShellFullAccess 政策](#)
- [【Inspector.1】 應啟用 Amazon Inspector EC2 掃描](#)

- [【Inspector.2】 應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】 應啟用 Amazon Inspector Lambda 標準掃描](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】 AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】 AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】 AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Kinesis.1】 Kinesis 串流應靜態加密](#)

- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.9】 應標記 OpenSearch 網域](#)
- [【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【RDS.1】 RDS 快照應為私有](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)

- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)
- [【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】 應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】 應標記 SageMaker 映像](#)
- [【SageMaker.8】 SageMaker 筆記本執行個體應在支援的平台上執行](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.17】 SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)

- [【SageMaker.18】使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.19】SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.1】SES 聯絡人清單應加上標籤](#)
- [【SES.2】SES 組態集應加上標籤](#)
- [【SES.3】SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【SQS.1】Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】SQS 佇列應加上標籤](#)
- [【SQS.3】SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.4】SSM 文件不應公開](#)
- [【SSM.7】SSM 文件應啟用封鎖公開共用設定](#)
- [【StepFunctions.1】Step Functions 狀態機器應該已開啟記錄](#)
- [【Transfer.3】Transfer Family 連接器應該已啟用記錄](#)
- [【Transfer.4】Transfer Family 協議應加上標籤](#)
- [【WAF.1】應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】WorkSpaces 根磁碟區應靜態加密](#)

亞太地區 (孟買)

亞太區域（孟買）區域不支援下列控制項。

- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)

- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoT TwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoT Wireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoT Wireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoT Wireless.3】 AWS IoT FUOTA 任務應加上標籤](#)

- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

亞太區域 (紐西蘭)

亞太區域（紐西蘭）區域不支援下列控制項。

- [【ACM.1】 匯入和 ACM 發行的憑證應在指定的期間之後續約](#)
- [【ACM.2】 由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)
- [【Account.1】 應針對 提供安全性聯絡資訊 AWS 帳戶](#)
- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.1】 應啟用 API Gateway REST 和 WebSocket API 執行記錄](#)
- [【APIGateway.2】 API Gateway REST API 階段應設定為使用 SSL 憑證進行後端身分驗證](#)
- [【APIGateway.3】 API Gateway REST API 階段應該已啟用 AWS X-Ray 追蹤](#)
- [【APIGateway.4】 API Gateway 應與 WAF Web ACL 建立關聯](#)
- [【APIGateway.5】 API Gateway REST API 快取資料應靜態加密](#)
- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)
- [【APIGateway.10】 API Gateway V2 整合應使用 HTTPS 進行私有連線](#)
- [【APIGateway.11】 API Gateway 網域名稱應使用建議的安全政策](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppConfig.1】 AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】 AWS AppConfig 組態設定檔應加上標籤](#)

- [【AppConfig.3】AWS AppConfig 環境應加上標籤](#)
- [【AppConfig.4】AWS AppConfig 應標記延伸關聯](#)
- [【AppFlow.1】Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.2】AWS AppSync 應該啟用欄位層級記錄](#)
- [【AppSync.4】AWS AppSync GraphQL APIs應加上標籤](#)
- [【AppSync.5】AWS AppSync GraphQL APIs不應使用 API 金鑰進行身分驗證](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【Athena.2】應標記 Athena 資料目錄](#)
- [【Athena.3】應標記 Athena 工作群組](#)
- [【Athena.4】Athena 工作群組應該已啟用記錄](#)
- [【AutoScaling.2】Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域](#)
- [【AutoScaling.3】Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【AutoScaling.6】Auto Scaling 群組應在多個可用區域中使用多個執行個體類型](#)
- [【AutoScaling.9】Amazon EC2 Auto Scaling 群組應使用 Amazon EC2 啟動範本](#)
- [【Backup.1】AWS Backup 復原點應靜態加密](#)
- [【Backup.2】AWS Backup 復原點應加上標籤](#)
- [【Backup.4】應標記 AWS Backup 報告計劃](#)
- [【Batch.1】批次任務佇列應加上標籤](#)
- [【Batch.2】批次排程政策應加上標籤](#)
- [【Batch.3】批次運算環境應加上標籤](#)
- [【Batch.4】應標記受管批次運算環境中的運算資源屬性](#)
- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)

- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.3】CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)
- [【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)
- [【CloudTrail.10】CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys](#)
- [【CloudWatch.17】應啟用 CloudWatch 警示動作](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料](#)
- [【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料](#)
- [【CodeBuild.3】CodeBuild S3 日誌應加密](#)
- [【CodeBuild.4】CodeBuild AWS Config專案環境應具有記錄 URL](#)
- [【CodeBuild.7】CodeBuild 報告群組匯出應靜態加密](#)

- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】Cognito 身分集區不應允許未驗證的身分](#)
- [【Cognito.3】Cognito 使用者集區的密碼政策應具有強大的組態](#)
- [【Cognito.4】Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證](#)
- [【Cognito.5】應為 Cognito 使用者集區啟用 MFA](#)
- [【Cognito.6】Cognito 使用者集區應啟用刪除保護](#)
- [【Connect.1】Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DataFirehose.1】Firehose 交付串流應靜態加密](#)
- [【DataSync.1】DataSync 任務應該已啟用記錄](#)
- [【DataSync.2】應標記 DataSync 任務](#)
- [【Detective.1】應標記 Detective 行為圖表](#)
- [【DMS.2】DMS 憑證應加上標籤](#)
- [【DMS.3】DMS 事件訂閱應加上標籤](#)
- [【DMS.4】DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】DMS 端點應使用 SSL](#)
- [【DMS.10】Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DocumentDB.1】Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】Amazon DocumentDB 叢集應具有足夠的備份保留期](#)

- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】 Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.4】 DynamoDB 資料表應存在於備份計畫中](#)
- [【DynamoDB.6】 DynamoDB 資料表應該已啟用刪除保護](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】 已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】 Amazon EC2 啟動範本不應將公 IPs 指派給網路介面](#)
- [【EC2.28】 備份計畫應涵蓋 EBS 磁碟區](#)
- [【EC2.34】 EC2 傳輸閘道路由表應加上標籤](#)
- [【EC2.40】 EC2 NAT 閘道應加上標籤](#)
- [【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.53】 EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.54】 EC2 安全群組不應允許從 ::/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.55】 VPCs 應使用 ECR API 的介面端點進行設定](#)
- [【EC2.56】 VPCs 應使用 Docker 登錄檔的介面端點進行設定](#)
- [【EC2.57】 VPCs 應使用 Systems Manager 的介面端點進行設定](#)
- [【EC2.58】 VPCs 應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs 應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.171】 EC2 VPN 連線應該已啟用記錄](#)
- [【EC2.172】 EC2 VPC 封鎖公開存取設定應封鎖網際網路閘道流量](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)

- [【EC2.174】 EC2 DHCP 選項集應加上標籤](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.176】 EC2 字首清單應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.178】 應標記 EC2 流量鏡像篩選條件](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【EC2.180】 EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.181】 EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【EC2.182】 應為 Amazon EBS 快照啟用封鎖公開存取設定](#)
- [【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定](#)
- [【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)
- [【ECR.2】 ECR 私有儲存庫應設定標籤不可變性](#)
- [【ECR.3】 ECR 儲存庫應至少設定一個生命週期政策](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ECR.5】 ECR 儲存庫應使用客戶受管加密 AWS KMS keys](#)
- [【ECS.3】 ECS 任務定義不應共用主機的程式命名空間](#)
- [【ECS.4】 ECS 容器應以非特殊權限執行](#)
- [【ECS.5】 ECS 任務定義應將容器設定為僅限對根檔案系統的唯讀存取](#)
- [【ECS.8】 不應將秘密做為容器環境變數傳遞](#)
- [【ECS.9】 ECS 任務定義應具有記錄組態](#)
- [【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行](#)
- [【ECS.12】 ECS 叢集應使用 Container Insights](#)
- [【ECS.16】 ECS 任務集不應自動指派公有 IP 地址](#)
- [【ECS.17】 ECS 任務定義不應使用主機網路模式](#)
- [【ECS.18】 ECS 任務定義應針對 EFS 磁碟區使用傳輸中加密](#)
- [【ECS.19】 ECS 容量提供者應啟用受管終止保護](#)
- [【ECS.20】 ECS 任務定義應在 Linux 容器定義中設定非根使用者](#)
- [【ECS.21】 ECS 任務定義應在 Windows 容器定義中設定非管理員使用者](#)
- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)

- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【EFS.3】 EFS 存取點應強制執行根目錄](#)
- [【EFS.4】 EFS 存取點應強制執行使用者身分](#)
- [【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯](#)
- [【EFS.7】 EFS 檔案系統應該啟用自動備份](#)
- [【EFS.8】 EFS 檔案系統應靜態加密](#)
- [【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)
- [【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密](#)
- [【EKS.7】 EKS 身分提供者組態應加上標籤](#)
- [【EKS.8】 EKS 叢集應該啟用稽核記錄](#)
- [【EKS.9】 EKS 節點群組應在支援的 Kubernetes 版本上執行](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【ELB.10】 Classic Load Balancer 應跨越多個可用區域](#)
- [【ELB.12】 Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.13】 應用程式、網路和閘道負載平衡器應跨越多個可用區域](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.16】 Application Load Balancer 應與 AWS WAF Web ACL 建立關聯](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ELB.21】 應用程式和 Network Load Balancer 目標群組應使用加密的運作狀態檢查通訊協定](#)
- [【ELB.22】 ELB 目標群組應使用加密傳輸通訊協定](#)
- [【ElasticCache.1】 ElasticCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElasticCache.2】 ElasticCache 叢集應該啟用自動次要版本升級](#)
- [【ElasticCache.3】 ElasticCache 複寫群組應該啟用自動容錯移轉](#)
- [【ElasticCache.4】 ElasticCache 複寫群組應靜態加密](#)
- [【ElasticCache.5】 ElasticCache 複寫群組應在傳輸中加密](#)
- [【ElasticCache.6】 舊版的 ElasticCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElasticCache.7】 ElasticCache 叢集不應使用預設子網路群組](#)

- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【EMR.2】 應啟用 Amazon EMR 封鎖公開存取設定](#)
- [【EMR.3】 Amazon EMR 安全組態應靜態加密](#)
- [【EMR.4】 Amazon EMR 安全組態應在傳輸中加密](#)
- [【ES.3】 Elasticsearch 網域應該加密節點之間傳送的資料](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【ES.9】 應標記 Elasticsearch 網域](#)
- [【EventBridge.3】 EventBridge 自訂事件匯流排應連接以資源為基礎的政策](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.1】 FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)
- [【FSx.2】 FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)
- [【FSx.3】 FSx for OpenZFS 檔案系統應設定為異地同步備份部署](#)
- [【FSx.4】 FSx for NetApp ONTAP 檔案系統應設定為異地同步備份部署](#)
- [【FSx.5】 FSx for Windows File Server 檔案系統應設定為異地同步備份部署](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【Glue.1】 AWS Glue 工作應加上標籤](#)
- [【Glue.3】 AWS Glue 機器學習轉換應該靜態加密](#)
- [【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.1】 應啟用 GuardDuty](#)
- [【GuardDuty.2】 GuardDuty 篩選條件應加上標籤](#)
- [【GuardDuty.3】 GuardDuty IPSets 應加上標籤](#)
- [【GuardDuty.4】 GuardDuty 偵測器應加上標籤](#)

- [【GuardDuty.5】應啟用 GuardDuty EKS 稽核日誌監控](#)
- [【GuardDuty.6】應啟用 GuardDuty Lambda 保護](#)
- [【GuardDuty.7】應啟用 GuardDuty EKS 執行期監控](#)
- [【GuardDuty.8】應啟用 EC2 的 GuardDuty 惡意軟體防護](#)
- [【GuardDuty.9】應啟用 GuardDuty RDS 保護](#)
- [【GuardDuty.10】應啟用 GuardDuty S3 保護](#)
- [【GuardDuty.11】應啟用 GuardDuty 執行期監控](#)
- [【GuardDuty.12】應啟用 GuardDuty ECS 執行期監控](#)
- [【GuardDuty.13】應啟用 GuardDuty EC2 執行期監控](#)
- [【IAM.1】IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.6】應為根使用者啟用硬體 MFA](#)
- [【IAM.7】IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.8】應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.9】應為根使用者啟用 MFA](#)
- [【IAM.10】IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.11】確保 IAM 密碼政策至少需要一個大寫字母](#)
- [【IAM.12】確保 IAM 密碼政策至少需要一個小寫字母](#)
- [【IAM.13】確保 IAM 密碼政策至少需要一個符號](#)
- [【IAM.14】確保 IAM 密碼政策至少需要一個數字](#)
- [【IAM.15】確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)
- [【IAM.16】確保 IAM 密碼政策防止密碼重複使用](#)
- [【IAM.17】確保 IAM 密碼政策在 90 天內過期密碼](#)
- [【IAM.18】確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)

- [【IAM.22】應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.24】IAM 角色應加上標籤](#)
- [【IAM.25】IAM 使用者應加上標籤](#)
- [【IAM.26】應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】IAM 身分不應連接 AWS CloudShellFullAccess 政策](#)
- [【IAM.28】應啟用 IAM Access Analyzer 外部存取分析器](#)
- [【Inspector.1】應啟用 Amazon Inspector EC2 掃描](#)
- [【Inspector.2】應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】應啟用 Amazon Inspector Lambda 標準掃描](#)
- [【IoT.1】AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinMaker.1】AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinMaker.2】AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinMaker.3】AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinMaker.4】AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】AWS IoT Wireless 多點傳送群組應加上標籤](#)

- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Kinesis.1】 Kinesis 串流應靜態加密](#)
- [【Kinesis.3】 Kinesis 串流應具有足夠的資料保留期](#)
- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【KMS.5】 不應公開存取 KMS 金鑰](#)
- [【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MQ.4】 Amazon MQ 代理程式應加上標籤](#)
- [【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式](#)
- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密](#)
- [【MSK.2】 MSK 叢集應已設定增強型監控](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.4】 MSK 叢集應停用公有存取](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【MSK.6】 MSK 叢集應停用未驗證的存取](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)

- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【NetworkFirewall.1】 網路防火牆防火牆應部署在多個可用區域](#)
- [【NetworkFirewall.2】 應啟用網路防火牆記錄](#)
- [【NetworkFirewall.3】 網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.4】 Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)
- [【NetworkFirewall.5】 網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】 無狀態網路防火牆規則群組不應為空](#)
- [【NetworkFirewall.9】 網路防火牆防火牆應啟用刪除保護](#)
- [【NetworkFirewall.10】 網路防火牆防火牆應啟用子網路變更保護](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.9】 應標記 OpenSearch 網域](#)
- [【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【PCA.1】 應停用 AWS 私有 CA 根憑證授權單位](#)
- [【PCA.2】 應標記 AWS 私有 CA 憑證授權單位](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.18】 RDS 執行個體應部署在 VPC 中](#)
- [【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱](#)

- [【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)
- [【RDS.26】 RDS 資料庫執行個體應受備份計劃保護](#)
- [【RDS.27】 RDS 資料庫叢集應靜態加密](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.36】 RDS for PostgreSQL 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.38】 RDS for PostgreSQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.39】 RDS for MySQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.40】 RDS for SQL Server 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.41】 RDS for SQL Server 資料庫執行個體應在傳輸中加密](#)
- [【RDS.42】 RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密](#)
- [【RDS.44】 RDS for MariaDB 資料庫執行個體應在傳輸中加密](#)
- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【RDS.46】 RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中](#)
- [【RDS.47】 RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.48】 RDS for MySQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.50】 RDS 資料庫叢集應設定足夠的備份保留期間](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【Redshift.1】 Amazon Redshift 叢集應禁止公開存取](#)
- [【Redshift.3】 Amazon Redshift 叢集應該啟用自動快照](#)
- [【Redshift.4】 Amazon Redshift 叢集應該啟用稽核記錄](#)
- [【Redshift.6】 Amazon Redshift 應已啟用主要版本的自動升級](#)
- [【Redshift.7】 Redshift 叢集應使用增強型 VPC 路由](#)
- [【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.11】 應標記 Redshift 叢集](#)

- [【Redshift.13】 應標記 Redshift 叢集快照](#)
- [【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠](#)
- [【Redshift.16】 Redshift 叢集子網路群組應具有來自多個可用區域的子網路](#)
- [【Redshift.17】 應標記 Redshift 叢集參數群組](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)
- [【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.7】 S3 一般用途儲存貯體應使用跨區域複寫](#)
- [【S3.10】 已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態](#)
- [【S3.11】 S3 一般用途儲存貯體應啟用事件通知](#)
- [【S3.12】 ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取](#)
- [【S3.13】 S3 一般用途儲存貯體應具有生命週期組態](#)
- [【S3.19】 S3 存取點應啟用封鎖公開存取設定](#)
- [【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除](#)
- [【S3.22】 S3 一般用途儲存貯體應記錄物件層級寫入事件](#)
- [【S3.23】 S3 一般用途儲存貯體應記錄物件層級讀取事件](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.4】 SageMaker 端點生產變體的初始執行個體計數應大於 1](#)

- [【SageMaker.5】SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】應標記 SageMaker 映像](#)
- [【SageMaker.8】SageMaker 筆記本執行個體應在支援的平台上執行](#)
- [【SageMaker.9】SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.17】SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.18】使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.19】SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.1】SES 聯絡人清單應加上標籤](#)
- [【SES.2】SES 組態集應加上標籤](#)
- [【SES.3】SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【ServiceCatalog.1】Service Catalog 產品組合只能在 AWS 組織內共用](#)
- [【SNS.4】SNS 主題存取政策不應允許公開存取](#)
- [【SQS.1】Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】SQS 佇列應加上標籤](#)
- [【SQS.3】SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.1】Amazon EC2 執行個體應該由 管理 AWS Systems Manager](#)
- [【SSM.2】Systems Manager 管理的 Amazon EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態](#)
- [【SSM.3】Systems Manager 管理的 Amazon EC2 執行個體應具有 COMPLIANT 的關聯合規狀態](#)
- [【SSM.4】SSM 文件不應公開](#)
- [【SSM.5】SSM 文件應加上標籤](#)

- [【SSM.6】 SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)
- [【StepFunctions.1】 Step Functions 狀態機器應該已開啟記錄](#)
- [【Transfer.1】 AWS Transfer Family 工作流程應加上標籤](#)
- [【Transfer.2】 Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線](#)
- [【Transfer.3】 Transfer Family 連接器應該已啟用記錄](#)
- [【Transfer.4】 Transfer Family 協議應加上標籤](#)
- [【Transfer.5】 Transfer Family 憑證應加上標籤](#)
- [【Transfer.6】 Transfer Family 連接器應加上標籤](#)
- [【Transfer.7】 轉移系列設定檔應加上標籤](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.2】 AWS WAF 傳統區域規則應至少有一個條件](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.4】 AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.11】 應該啟用 AWS WAF Web ACL 記錄](#)
- [【WAF.12】 AWS WAF 規則應啟用 CloudWatch 指標](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

亞太地區 (大阪)

亞太區域（大阪）區域不支援下列控制項。

- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)

- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【Backup.1】 AWS Backup 復原點應靜態加密](#)
- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)

- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【Detective.1】 應標記 Detective 行為圖表](#)
- [【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】 Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】 已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.14】 安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.55】 VPCs 應使用 ECR API 的介面端點進行設定](#)
- [【EC2.56】 VPCs 應使用 Docker 登錄檔的介面端點進行設定](#)
- [【EC2.57】 VPCs 應使用 Systems Manager 的介面端點進行設定](#)
- [【EC2.58】 VPCs 應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs 應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.7】 ElastiCache 叢集不應使用預設子網路群組](#)

- [【ElasticBeanstalk.1】Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【FraudDetector.1】Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【IAM.26】應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoT.1】AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】AWS IoT Wireless 服務設定檔應加上標籤](#)

- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)
- [【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SSM.2】 Systems Manager 管理的 Amazon EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態](#)
- [【SSM.3】 Systems Manager 管理的 Amazon EC2 執行個體應具有 COMPLIANT 的關聯合規狀態](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)

- [【WorkSpaces.1】應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】WorkSpaces 根磁碟區應靜態加密](#)

亞太地區 (首爾)

亞太區域 (首爾) 區域不支援下列控制項。

- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)

- [【Cognito.2】 Cognito 身分集區不應允許未驗證的身分](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.180】 EC2 網路介面應啟用來源/目的地檢查](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoT TwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)

- [【SSM.6】 SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

亞太地區 (新加坡)

亞太區域（新加坡）區域不支援下列控制項。

- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)

- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【IAM.26】應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IoTWireless.1】AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】IVS 記錄組態應加上標籤](#)
- [【IVS.3】IVS 頻道應加上標籤](#)
- [【Route53.1】應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】S3 目錄儲存貯體應該具有生命週期組態](#)
- [【WAF.1】應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

亞太地區 (悉尼)

亞太區域（雪梨）區域不支援下列控制項。

- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)

- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

亞太區域 (台北)

亞太區域（台北）區域不支援下列控制項。

- [【ACM.1】 匯入和 ACM 發行的憑證應在指定的期間之後續約](#)
- [【ACM.2】 由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)

- [【ACM.3】 ACM 憑證應加上標籤](#)
- [【Account.1】 應針對 提供安全性聯絡資訊 AWS 帳戶](#)
- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.1】 應啟用 API Gateway REST 和 WebSocket API 執行記錄](#)
- [【APIGateway.2】 API Gateway REST API 階段應設定為使用 SSL 憑證進行後端身分驗證](#)
- [【APIGateway.3】 API Gateway REST API 階段應該已啟用 AWS X-Ray 追蹤](#)
- [【APIGateway.4】 API Gateway 應與 WAF Web ACL 建立關聯](#)
- [【APIGateway.5】 API Gateway REST API 快取資料應靜態加密](#)
- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)
- [【APIGateway.10】 API Gateway V2 整合應使用 HTTPS 進行私有連線](#)
- [【APIGateway.11】 API Gateway 網域名稱應使用建議的安全政策](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppConfig.1】 AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】 AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】 AWS AppConfig 環境應加上標籤](#)
- [【AppConfig.4】 AWS AppConfig 應標記延伸關聯](#)
- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)
- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.2】 AWS AppSync 應該啟用欄位層級記錄](#)
- [【AppSync.4】 AWS AppSync GraphQL APIs應加上標籤](#)
- [【AppSync.5】 AWS AppSync GraphQL APIs不應使用 API 金鑰進行身分驗證](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【Athena.2】 應標記 Athena 資料目錄](#)
- [【Athena.3】 應標記 Athena 工作群組](#)

- [【Athena.4】 Athena 工作群組應該已啟用記錄](#)
- [【AutoScaling.1】 與負載平衡器相關聯的 Auto Scaling 群組應使用 ELB 運作狀態檢查](#)
- [【AutoScaling.2】 Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域](#)
- [【AutoScaling.3】 Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【AutoScaling.6】 Auto Scaling 群組應在多個可用區域中使用多個執行個體類型](#)
- [【AutoScaling.9】 Amazon EC2 Auto Scaling 群組應使用 Amazon EC2 啟動範本](#)
- [【AutoScaling.10】 應標記 EC2 Auto Scaling 群組](#)
- [【Autoscaling.5】 使用 Auto Scaling 群組啟動組態啟動的 Amazon EC2 執行個體不應具有公有 IP 地址](#)
- [【Backup.1】 AWS Backup 復原點應靜態加密](#)
- [【Backup.2】 AWS Backup 復原點應加上標籤](#)
- [【Backup.3】 保存 AWS Backup 庫應加上標籤](#)
- [【Backup.4】 應標記 AWS Backup 報告計劃](#)
- [【Backup.5】 AWS Backup 備份計劃應加上標籤](#)
- [【Batch.1】 批次任務佇列應加上標籤](#)
- [【Batch.2】 批次排程政策應加上標籤](#)
- [【Batch.3】 批次運算環境應加上標籤](#)
- [【Batch.4】 應標記受管批次運算環境中的運算資源屬性](#)
- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.2】 應標記 CloudFormation 堆疊](#)
- [【CloudFormation.3】 CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】 CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)

- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)
- [【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)
- [【CloudTrail.9】應標記 CloudTrail 追蹤](#)
- [【CloudTrail.10】CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys](#)
- [【CloudWatch.17】應啟用 CloudWatch 警示動作](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料](#)
- [【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料](#)
- [【CodeBuild.3】CodeBuild S3 日誌應加密](#)
- [【CodeBuild.4】CodeBuild AWS Config專案環境應具有記錄 URL](#)
- [【CodeBuild.7】CodeBuild 報告群組匯出應靜態加密](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)

- [【Cognito.2】 Cognito 身分集區不應允許未驗證的身分](#)
- [【Cognito.3】 Cognito 使用者集區的密碼政策應具有強大的組態](#)
- [【Cognito.4】 Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證](#)
- [【Cognito.5】 應為 Cognito 使用者集區啟用 MFA](#)
- [【Cognito.6】 Cognito 使用者集區應啟用刪除保護](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DataFirehose.1】 Firehose 交付串流應靜態加密](#)
- [【DataSync.1】 DataSync 任務應該已啟用記錄](#)
- [【DataSync.2】 應標記 DataSync 任務](#)
- [【Detective.1】 應標記 Detective 行為圖表](#)
- [【DMS.1】 Database Migration Service 複寫執行個體不應為公有](#)
- [【DMS.2】 DMS 憑證應加上標籤](#)
- [【DMS.3】 DMS 事件訂閱應加上標籤](#)
- [【DMS.4】 DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】 DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】 DMS 端點應使用 SSL](#)
- [【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】 DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)

- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】 Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.4】 DynamoDB 資料表應存在於備份計畫中](#)
- [【DynamoDB.5】 DynamoDB 資料表應加上標籤](#)
- [【DynamoDB.6】 DynamoDB 資料表應該已啟用刪除保護](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】 已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.10】 Amazon EC2 應設定為使用為 Amazon EC2 服務建立的 VPC 端點](#)
- [【EC2.19】 安全群組不應允許無限制存取高風險的連接埠](#)
- [【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】 Amazon EC2 啟動範本不應將公IPs 指派給網路介面](#)
- [【EC2.28】 備份計畫應涵蓋 EBS 磁碟區](#)
- [【EC2.33】 EC2 傳輸閘道附件應加上標籤](#)
- [【EC2.34】 EC2 傳輸閘道路由表應加上標籤](#)
- [【EC2.35】 EC2 網路介面應加上標籤](#)
- [【EC2.36】 EC2 客戶閘道應加上標籤](#)
- [【EC2.37】 EC2 彈性 IP 地址應加上標籤](#)
- [【EC2.38】 應標記 EC2 執行個體](#)
- [【EC2.39】 EC2 網際網路閘道應加上標籤](#)
- [【EC2.40】 EC2 NAT 閘道應加上標籤](#)
- [【EC2.41】 EC2 網路 ACLs 應加上標籤](#)
- [【EC2.42】 EC2 路由表應加上標籤](#)
- [【EC2.43】 EC2 安全群組應加上標籤](#)
- [【EC2.44】 EC2 子網路應加上標籤](#)

- [【EC2.45】 EC2 磁碟區應加上標籤](#)
- [【EC2.46】 Amazon VPCs應加上標籤](#)
- [【EC2.47】 Amazon VPC 端點服務應加上標籤](#)
- [【EC2.48】 Amazon VPC 流程日誌應加上標籤](#)
- [【EC2.49】 Amazon VPC 互連連線應加上標籤](#)
- [【EC2.50】 EC2 VPN 閘道應加上標籤](#)
- [【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.52】 EC2 傳輸閘道應加上標籤](#)
- [【EC2.53】 EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.54】 EC2 安全群組不應允許從 ::/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.55】 VPCs應使用 ECR API 的介面端點進行設定](#)
- [【EC2.56】 VPCs應使用 Docker 登錄檔的介面端點進行設定](#)
- [【EC2.57】 VPCs應使用 Systems Manager 的介面端點進行設定](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.171】 EC2 VPN 連線應該已啟用記錄](#)
- [【EC2.172】 EC2 VPC 封鎖公開存取設定應封鎖網際網路閘道流量](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.174】 EC2 DHCP 選項集應加上標籤](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.176】 EC2 字首清單應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.178】 應標記 EC2 流量鏡像篩選條件](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【EC2.180】 EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.181】 EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【EC2.182】 應為 Amazon EBS 快照啟用封鎖公開存取設定](#)

- [【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定](#)
- [【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)
- [【ECR.2】 ECR 私有儲存庫應設定標籤不可變性](#)
- [【ECR.3】 ECR 儲存庫應至少設定一個生命週期政策](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ECR.5】 ECR 儲存庫應使用客戶受管加密 AWS KMS keys](#)
- [【ECS.1】 Amazon ECS 任務定義應具有安全的聯網模式和使用使用者定義](#)
- [【ECS.2】 ECS 服務不應自動為其指派公有 IP 地址](#)
- [【ECS.3】 ECS 任務定義不應共用主機的程序命名空間](#)
- [【ECS.4】 ECS 容器應以非特殊權限執行](#)
- [【ECS.5】 ECS 任務定義應將容器設定為僅限對根檔案系統的唯讀存取](#)
- [【ECS.8】 不應將秘密做為容器環境變數傳遞](#)
- [【ECS.9】 ECS 任務定義應具有記錄組態](#)
- [【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行](#)
- [【ECS.12】 ECS 叢集應使用 Container Insights](#)
- [【ECS.13】 ECS 服務應加上標籤](#)
- [【ECS.14】 ECS 叢集應加上標籤](#)
- [【ECS.15】 ECS 任務定義應加上標籤](#)
- [【ECS.16】 ECS 任務集不應自動指派公有 IP 地址](#)
- [【ECS.17】 ECS 任務定義不應使用主機網路模式](#)
- [【ECS.18】 ECS 任務定義應針對 EFS 磁碟區使用傳輸中加密](#)
- [【ECS.19】 ECS 容量提供者應啟用受管終止保護](#)
- [【ECS.20】 ECS 任務定義應在 Linux 容器定義中設定非根使用者](#)
- [【ECS.21】 ECS 任務定義應在 Windows 容器定義中設定非管理員使用者](#)
- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【EFS.3】 EFS 存取點應強制執行根目錄](#)
- [【EFS.4】 EFS 存取點應強制執行使用者身分](#)

- [【EFS.5】 EFS 存取點應加上標籤](#)
- [【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯](#)
- [【EFS.7】 EFS 檔案系統應該啟用自動備份](#)
- [【EFS.8】 EFS 檔案系統應靜態加密](#)
- [【EKS.1】 不應公開存取 EKS 叢集端點](#)
- [【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)
- [【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密](#)
- [【EKS.6】 EKS 叢集應加上標籤](#)
- [【EKS.7】 EKS 身分提供者組態應加上標籤](#)
- [【EKS.8】 EKS 叢集應該啟用稽核記錄](#)
- [【EKS.9】 EKS 節點群組應在支援的 Kubernetes 版本上執行](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【ELB.3】 Classic Load Balancer 接聽程式應使用 HTTPS 或 TLS 終止設定](#)
- [【ELB.7】 Classic Load Balancer 應啟用連線耗盡](#)
- [【ELB.8】 具有 SSL AWS Config接聽程式的 Classic Load Balancer 應使用預先定義的安全政策，該政策具有強烈驅動](#)
- [【ELB.10】 Classic Load Balancer 應跨越多個可用區域](#)
- [【ELB.12】 Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.13】 應用程式、網路和閘道負載平衡器應跨越多個可用區域](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.16】 Application Load Balancer 應與 AWS WAF Web ACL 建立關聯](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ELB.21】 應用程式和 Network Load Balancer 目標群組應使用加密的運作狀態檢查通訊協定](#)
- [【ELB.22】 ELB 目標群組應使用加密傳輸通訊協定](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.2】 ElastiCache 叢集應該啟用自動次要版本升級](#)
- [【ElastiCache.3】 ElastiCache 複寫群組應該啟用自動容錯移轉](#)

- [【ElastiCache.4】ElastiCache 複寫群組應靜態加密](#)
- [【ElastiCache.5】ElastiCache 複寫群組應在傳輸中加密](#)
- [【ElastiCache.6】舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【EMR.2】 應啟用 Amazon EMR 封鎖公開存取設定](#)
- [【EMR.3】 Amazon EMR 安全組態應靜態加密](#)
- [【EMR.4】 Amazon EMR 安全組態應在傳輸中加密](#)
- [【ES.1】 Elasticsearch 網域應該啟用靜態加密](#)
- [【ES.2】 不應公開存取 Elasticsearch 網域](#)
- [【ES.3】 Elasticsearch 網域應該加密節點之間傳送的資料](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【ES.5】 Elasticsearch 網域應該啟用稽核記錄](#)
- [【ES.6】 Elasticsearch 網域應至少具有三個資料節點](#)
- [【ES.7】 Elasticsearch 網域應該至少設定三個專用主節點](#)
- [【ES.8】 應使用最新的 TLS 安全政策加密與 Elasticsearch 網域的連線](#)
- [【ES.9】 應標記 Elasticsearch 網域](#)
- [【EventBridge.2】應標記 EventBridge 事件匯流排](#)
- [【EventBridge.3】EventBridge 自訂事件匯流排應連接以資源為基礎的政策](#)
- [【EventBridge.4】EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.1】FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)

- [【FSx.2】FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)
- [【FSx.3】FSx for OpenZFS 檔案系統應設定為異地同步備份部署](#)
- [【FSx.4】FSx for NetApp ONTAP 檔案系統應設定為異地同步備份部署](#)
- [【FSx.5】FSx for Windows File Server 檔案系統應設定為異地同步備份部署](#)
- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【Glue.1】AWS Glue 工作應加上標籤](#)
- [【Glue.3】AWS Glue 機器學習轉換應該靜態加密](#)
- [【Glue.4】AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.1】應啟用 GuardDuty](#)
- [【GuardDuty.2】GuardDuty 篩選條件應加上標籤](#)
- [【GuardDuty.3】GuardDuty IPSets 應加上標籤](#)
- [【GuardDuty.4】GuardDuty 偵測器應加上標籤](#)
- [【GuardDuty.5】應啟用 GuardDuty EKS 稽核日誌監控](#)
- [【GuardDuty.6】應啟用 GuardDuty Lambda 保護](#)
- [【GuardDuty.7】應啟用 GuardDuty EKS 執行期監控](#)
- [【GuardDuty.8】應啟用 EC2 的 GuardDuty 惡意軟體防護](#)
- [【GuardDuty.9】應啟用 GuardDuty RDS 保護](#)
- [【GuardDuty.10】應啟用 GuardDuty S3 保護](#)
- [【GuardDuty.11】應啟用 GuardDuty 執行期監控](#)
- [【GuardDuty.12】應啟用 GuardDuty ECS 執行期監控](#)
- [【GuardDuty.13】應啟用 GuardDuty EC2 執行期監控](#)
- [【IAM.1】IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.6】應為根使用者啟用硬體 MFA](#)
- [【IAM.7】IAM 使用者的密碼政策應具有強大的組態](#)

- [【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.9】 應為根使用者啟用 MFA](#)
- [【IAM.10】 IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.11】 確保 IAM 密碼政策至少需要一個大寫字母](#)
- [【IAM.12】 確保 IAM 密碼政策至少需要一個小寫字母](#)
- [【IAM.13】 確保 IAM 密碼政策至少需要一個符號](#)
- [【IAM.14】 確保 IAM 密碼政策至少需要一個數字](#)
- [【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)
- [【IAM.16】 確保 IAM 密碼政策防止密碼重複使用](#)
- [【IAM.17】 確保 IAM 密碼政策在 90 天內過期密碼](#)
- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.23】 IAM Access Analyzer 分析器應加上標籤](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】 IAM 身分不應連接 AWS CloudShellFullAccess 政策](#)
- [【IAM.28】 應啟用 IAM Access Analyzer 外部存取分析器](#)
- [【Inspector.1】 應啟用 Amazon Inspector EC2 掃描](#)
- [【Inspector.2】 應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】 應啟用 Amazon Inspector Lambda 標準掃描](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】 AWS IoT Core 授權方應加上標籤](#)

- [【IoT.5】 AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】 AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Kinesis.1】 Kinesis 串流應靜態加密](#)
- [【Kinesis.2】 Kinesis 串流應加上標籤](#)
- [【Kinesis.3】 Kinesis 串流應具有足夠的資料保留期](#)
- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【KMS.3】 AWS KMS keys 不應意外刪除](#)
- [【KMS.5】 不應公開存取 KMS 金鑰](#)

- [【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作](#)
- [【Lambda.6】 應標記 Lambda 函數](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MQ.4】 Amazon MQ 代理程式應加上標籤](#)
- [【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式](#)
- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密](#)
- [【MSK.2】 MSK 叢集應已設定增強型監控](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.4】 MSK 叢集應停用公有存取](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【MSK.6】 MSK 叢集應停用未驗證的存取](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【NetworkFirewall.1】 網路防火牆防火牆應部署在多個可用區域](#)
- [【NetworkFirewall.2】 應啟用網路防火牆記錄](#)
- [【NetworkFirewall.3】 網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.4】 Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)

- [【NetworkFirewall.5】網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】無狀態網路防火牆規則群組不應為空](#)
- [【NetworkFirewall.7】應標記網路防火牆](#)
- [【NetworkFirewall.8】應標記網路防火牆防火牆政策](#)
- [【NetworkFirewall.9】網路防火牆防火牆應啟用刪除保護](#)
- [【NetworkFirewall.10】網路防火牆防火牆應啟用子網路變更保護](#)
- [【Opensearch.1】OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.9】應標記 OpenSearch 網域](#)
- [【Opensearch.10】OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】OpenSearch 網域應至少具有三個專用主節點](#)
- [【PCA.1】應停用 AWS 私有 CA 根憑證授權單位](#)
- [【PCA.2】應標記 AWS 私有 CA 憑證授權單位](#)
- [【RDS.14】Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.16】Aurora 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.17】RDS 資料庫執行個體應設定為將標籤複製到快照](#)
- [【RDS.18】RDS 執行個體應部署在 VPC 中](#)
- [【RDS.19】應為關鍵叢集事件設定現有的 RDS 事件通知訂閱](#)
- [【RDS.20】應為關鍵資料庫執行個體事件設定現有的 RDS 事件通知訂閱](#)
- [【RDS.21】應為關鍵資料庫參數群組事件設定 RDS 事件通知訂閱](#)
- [【RDS.22】應為關鍵資料庫安全群組事件設定 RDS 事件通知訂閱](#)
- [【RDS.23】RDS 執行個體不應使用資料庫引擎預設連接埠](#)

- [【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱](#)
- [【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)
- [【RDS.26】 RDS 資料庫執行個體應受備份計劃保護](#)
- [【RDS.27】 RDS 資料庫叢集應靜態加密](#)
- [【RDS.28】 RDS 資料庫叢集應加上標籤](#)
- [【RDS.29】 應標記 RDS 資料庫叢集快照](#)
- [【RDS.30】 RDS 資料庫執行個體應加上標籤](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.32】 RDS 資料庫快照應加上標籤](#)
- [【RDS.33】 RDS 資料庫子網路群組應加上標籤](#)
- [【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.36】 RDS for PostgreSQL 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.38】 RDS for PostgreSQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.39】 RDS for MySQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.40】 RDS for SQL Server 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.41】 RDS for SQL Server 資料庫執行個體應在傳輸中加密](#)
- [【RDS.42】 RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密](#)
- [【RDS.44】 RDS for MariaDB 資料庫執行個體應在傳輸中加密](#)
- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【RDS.46】 RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中](#)
- [【RDS.47】 RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.48】 RDS for MySQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.50】 RDS 資料庫叢集應設定足夠的備份保留期間](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【Redshift.1】 Amazon Redshift 叢集應禁止公開存取](#)

- [【Redshift.2】 與 Amazon Redshift 叢集的連線應在傳輸中加密](#)
- [【Redshift.3】 Amazon Redshift 叢集應該啟用自動快照](#)
- [【Redshift.4】 Amazon Redshift 叢集應該啟用稽核記錄](#)
- [【Redshift.6】 Amazon Redshift 應已啟用主要版本的自動升級](#)
- [【Redshift.7】 Redshift 叢集應使用增強型 VPC 路由](#)
- [【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.11】 應標記 Redshift 叢集](#)
- [【Redshift.12】 應標記 Redshift 事件通知訂閱](#)
- [【Redshift.13】 應標記 Redshift 叢集快照](#)
- [【Redshift.14】 應標記 Redshift 叢集子網路群組](#)
- [【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠](#)
- [【Redshift.16】 Redshift 叢集子網路群組應具有來自多個可用區域的子網路](#)
- [【Redshift.17】 應標記 Redshift 叢集參數群組](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)
- [【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.7】 S3 一般用途儲存貯體應使用跨區域複寫](#)
- [【S3.10】 已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態](#)
- [【S3.11】 S3 一般用途儲存貯體應啟用事件通知](#)
- [【S3.12】 ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取](#)
- [【S3.13】 S3 一般用途儲存貯體應具有生命週期組態](#)

- [【S3.17】 S3 一般用途儲存貯體應使用 靜態加密 AWS KMS keys](#)
- [【S3.19】 S3 存取點應啟用封鎖公開存取設定](#)
- [【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除](#)
- [【S3.22】 S3 一般用途儲存貯體應記錄物件層級寫入事件](#)
- [【S3.23】 S3 一般用途儲存貯體應記錄物件層級讀取事件](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.4】 SageMaker 端點生產變體的初始執行個體計數應大於 1](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】 應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】 應標記 SageMaker 映像](#)
- [【SageMaker.8】 SageMaker 筆記本執行個體應在支援的平台上執行](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應該啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.17】 SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.18】 使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.1】 SES 聯絡人清單應加上標籤](#)
- [【SES.2】 SES 組態集應加上標籤](#)

- [【SES.3】 SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【SecretsManager.1】 Secrets Manager 秘密應該已啟用自動輪換](#)
- [【SecretsManager.2】 設定自動輪換的 Secrets Manager 秘密應能成功輪換](#)
- [【SecretsManager.3】 移除未使用的 Secrets Manager 秘密](#)
- [【SecretsManager.4】 Secrets Manager 秘密應在指定的天數內輪換](#)
- [【SecretsManager.5】 Secrets Manager 秘密應加上標籤](#)
- [【ServiceCatalog.1】 Service Catalog 產品組合只能在 AWS 組織內共用](#)
- [【SNS.3】 SNS 主題應加上標籤](#)
- [【SNS.4】 SNS 主題存取政策不應允許公開存取](#)
- [【SQS.1】 Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】 SQS 佇列應加上標籤](#)
- [【SQS.3】 SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.1】 Amazon EC2 執行個體應該由 管理 AWS Systems Manager](#)
- [【SSM.2】 Systems Manager 管理的 Amazon EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態](#)
- [【SSM.3】 Systems Manager 管理的 Amazon EC2 執行個體應具有 COMPLIANT 的關聯合規狀態](#)
- [【SSM.4】 SSM 文件不應公開](#)
- [【SSM.5】 SSM 文件應加上標籤](#)
- [【SSM.6】 SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)
- [【StepFunctions.1】 Step Functions 狀態機器應該已開啟記錄](#)
- [【StepFunctions.2】 應標記 Step Functions 活動](#)
- [【Transfer.1】 AWS Transfer Family 工作流程應加上標籤](#)
- [【Transfer.2】 Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線](#)
- [【Transfer.3】 Transfer Family 連接器應該已啟用記錄](#)
- [【Transfer.4】 Transfer Family 協議應加上標籤](#)
- [【Transfer.5】 Transfer Family 憑證應加上標籤](#)
- [【Transfer.6】 Transfer Family 連接器應加上標籤](#)
- [【Transfer.7】 轉移系列設定檔應加上標籤](#)

- [【WAF.1】應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.2】AWS WAF 傳統區域規則應至少有一個條件](#)
- [【WAF.3】AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.4】AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.6】AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.11】應該啟用 AWS WAF Web ACL 記錄](#)
- [【WAF.12】AWS WAF 規則應啟用 CloudWatch 指標](#)
- [【WorkSpaces.1】應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】WorkSpaces 根磁碟區應靜態加密](#)

亞太區域 (泰國)

亞太區域 (泰國) 區域不支援下列控制項。

- [【ACM.1】匯入和 ACM 發行的憑證應在指定的期間之後續約](#)
- [【ACM.2】由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)
- [【Account.1】應針對提供安全性聯絡資訊 AWS 帳戶](#)
- [【Account.2】AWS 帳戶應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.8】API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】應為 API Gateway V2 階段設定存取記錄](#)
- [【APIGateway.10】API Gateway V2 整合應使用 HTTPS 進行私有連線](#)
- [【Amplify.1】Amplify 應用程式應加上標籤](#)
- [【Amplify.2】Amplify 分支應加上標籤](#)
- [【AppConfig.1】AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】AWS AppConfig 環境應加上標籤](#)
- [【AppConfig.4】AWS AppConfig 應標記延伸關聯](#)

- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)
- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.2】 AWS AppSync 應該啟用欄位層級記錄](#)
- [【AppSync.5】 AWS AppSync GraphQL APIs不應使用 API 金鑰進行身分驗證](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【Athena.2】 應標記 Athena 資料目錄](#)
- [【Athena.3】 應標記 Athena 工作群組](#)
- [【Athena.4】 Athena 工作群組應該已啟用記錄](#)
- [【AutoScaling.2】 Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域](#)
- [【AutoScaling.3】 Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【AutoScaling.6】 Auto Scaling 群組應在多個可用區域中使用多個執行個體類型](#)
- [【AutoScaling.9】 Amazon EC2 Auto Scaling 群組應使用 Amazon EC2 啟動範本](#)
- [【Backup.1】 AWS Backup 復原點應靜態加密](#)
- [【Backup.2】 AWS Backup 復原點應加上標籤](#)
- [【Backup.4】 應標記 AWS Backup 報告計劃](#)
- [【Batch.1】 批次任務佇列應加上標籤](#)
- [【Batch.2】 批次排程政策應加上標籤](#)
- [【Batch.3】 批次運算環境應加上標籤](#)
- [【Batch.4】 應標記受管批次運算環境中的運算資源屬性](#)
- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.3】 CloudFormation 堆疊應啟用終止保護](#)

- [【CloudFormation.4】CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)
- [【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)
- [【CloudTrail.10】CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys](#)
- [【CloudWatch.17】應啟用 CloudWatch 警示動作](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料](#)
- [【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料](#)
- [【CodeBuild.3】CodeBuild S3 日誌應加密](#)
- [【CodeBuild.4】CodeBuild AWS Config專案環境應具有記錄 URL](#)
- [【CodeBuild.7】CodeBuild 報告群組匯出應靜態加密](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)

- [【Cognito.1】 Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】 Cognito 身分集區不應允許未驗證的身分](#)
- [【Cognito.3】 Cognito 使用者集區的密碼政策應具有強大的組態](#)
- [【Cognito.4】 Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證](#)
- [【Cognito.5】 應為 Cognito 使用者集區啟用 MFA](#)
- [【Cognito.6】 Cognito 使用者集區應啟用刪除保護](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DataFirehose.1】 Firehose 交付串流應靜態加密](#)
- [【DataSync.1】 DataSync 任務應該已啟用記錄](#)
- [【DataSync.2】 應標記 DataSync 任務](#)
- [【Detective.1】 應標記 Detective 行為圖表](#)
- [【DMS.2】 DMS 憑證應加上標籤](#)
- [【DMS.3】 DMS 事件訂閱應加上標籤](#)
- [【DMS.4】 DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】 DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】 DMS 端點應使用 SSL](#)
- [【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】 DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)

- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】 Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.4】 DynamoDB 資料表應存在於備份計畫中](#)
- [【DynamoDB.6】 DynamoDB 資料表應該已啟用刪除保護](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】 已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】 Amazon EC2 啟動範本不應將公 IPs 指派給網路介面](#)
- [【EC2.28】 備份計畫應涵蓋 EBS 磁碟區](#)
- [【EC2.34】 EC2 傳輸閘道路由表應加上標籤](#)
- [【EC2.40】 EC2 NAT 閘道應加上標籤](#)
- [【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.53】 EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.54】 EC2 安全群組不應允許從 :::/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.55】 VPCs 應使用 ECR API 的介面端點進行設定](#)
- [【EC2.56】 VPCs 應使用 Docker 登錄檔的介面端點進行設定](#)
- [【EC2.57】 VPCs 應使用 Systems Manager 的介面端點進行設定](#)
- [【EC2.58】 VPCs 應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs 應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.171】 EC2 VPN 連線應該已啟用記錄](#)
- [【EC2.172】 EC2 VPC 封鎖公開存取設定應封鎖網際網路閘道流量](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.174】 EC2 DHCP 選項集應加上標籤](#)

- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.176】 EC2 字首清單應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.178】 應標記 EC2 流量鏡像篩選條件](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【EC2.180】 EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.181】 EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【EC2.182】 應為 Amazon EBS 快照啟用封鎖公開存取設定](#)
- [【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定](#)
- [【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)
- [【ECR.2】 ECR 私有儲存庫應設定標籤不可變性](#)
- [【ECR.3】 ECR 儲存庫應至少設定一個生命週期政策](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ECR.5】 ECR 儲存庫應使用客戶受管加密 AWS KMS keys](#)
- [【ECS.3】 ECS 任務定義不應共用主機的程序命名空間](#)
- [【ECS.4】 ECS 容器應以非特殊權限執行](#)
- [【ECS.5】 ECS 任務定義應將容器設定為僅限對根檔案系統的唯讀存取](#)
- [【ECS.8】 不應將秘密做為容器環境變數傳遞](#)
- [【ECS.9】 ECS 任務定義應具有記錄組態](#)
- [【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行](#)
- [【ECS.12】 ECS 叢集應使用 Container Insights](#)
- [【ECS.16】 ECS 任務集不應自動指派公有 IP 地址](#)
- [【ECS.17】 ECS 任務定義不應使用主機網路模式](#)
- [【ECS.18】 ECS 任務定義應針對 EFS 磁碟區使用傳輸中加密](#)
- [【ECS.19】 ECS 容量提供者應啟用受管終止保護](#)
- [【ECS.20】 ECS 任務定義應在 Linux 容器定義中設定非根使用者](#)
- [【ECS.21】 ECS 任務定義應在 Windows 容器定義中設定非管理員使用者](#)
- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)

- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【EFS.3】 EFS 存取點應強制執行根目錄](#)
- [【EFS.4】 EFS 存取點應強制執行使用者身分](#)
- [【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯](#)
- [【EFS.7】 EFS 檔案系統應該啟用自動備份](#)
- [【EFS.8】 EFS 檔案系統應靜態加密](#)
- [【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)
- [【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密](#)
- [【EKS.7】 EKS 身分提供者組態應加上標籤](#)
- [【EKS.8】 EKS 叢集應該啟用稽核記錄](#)
- [【EKS.9】 EKS 節點群組應在支援的 Kubernetes 版本上執行](#)
- [【ELB.10】 Classic Load Balancer 應跨越多個可用區域](#)
- [【ELB.12】 Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.13】 應用程式、網路和閘道負載平衡器應跨越多個可用區域](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ElasticCache.1】 ElasticCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElasticCache.2】 ElasticCache 叢集應該啟用自動次要版本升級](#)
- [【ElasticCache.3】 ElasticCache 複寫群組應該啟用自動容錯移轉](#)
- [【ElasticCache.4】 ElasticCache 複寫群組應靜態加密](#)
- [【ElasticCache.5】 ElasticCache 複寫群組應在傳輸中加密](#)
- [【ElasticCache.6】 舊版的 ElasticCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElasticCache.7】 ElasticCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)

- [【EMR.2】應啟用 Amazon EMR 封鎖公開存取設定](#)
- [【EMR.3】Amazon EMR 安全組態應靜態加密](#)
- [【EMR.4】Amazon EMR 安全組態應在傳輸中加密](#)
- [【ES.4】應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【ES.9】應標記 Elasticsearch 網域](#)
- [【EventBridge.3】EventBridge 自訂事件匯流排應連接以資源為基礎的政策](#)
- [【EventBridge.4】EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.1】FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)
- [【FSx.2】FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)
- [【FSx.3】FSx for OpenZFS 檔案系統應設定為異地同步備份部署](#)
- [【FSx.4】FSx for NetApp ONTAP 檔案系統應設定為異地同步備份部署](#)
- [【FSx.5】FSx for Windows File Server 檔案系統應設定為異地同步備份部署](#)
- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【Glue.1】AWS Glue 工作應加上標籤](#)
- [【Glue.3】AWS Glue 機器學習轉換應該靜態加密](#)
- [【Glue.4】AWS Glue Spark 任務應在支援的版本上執行 AWS Glue](#)
- [【GuardDuty.1】應啟用 GuardDuty](#)
- [【GuardDuty.2】GuardDuty 篩選條件應加上標籤](#)
- [【GuardDuty.5】應啟用 GuardDuty EKS 稽核日誌監控](#)
- [【GuardDuty.6】應啟用 GuardDuty Lambda 保護](#)
- [【GuardDuty.7】應啟用 GuardDuty EKS 執行期監控](#)
- [【GuardDuty.8】應啟用 EC2 的 GuardDuty 惡意軟體防護](#)
- [【GuardDuty.9】應啟用 GuardDuty RDS 保護](#)
- [【GuardDuty.10】應啟用 GuardDuty S3 保護](#)
- [【GuardDuty.11】應啟用 GuardDuty 執行期監控](#)

- [【GuardDuty.12】應啟用 GuardDuty ECS 執行期監控](#)
- [【GuardDuty.13】應啟用 GuardDuty EC2 執行期監控](#)
- [【IAM.1】IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.6】應為根使用者啟用硬體 MFA](#)
- [【IAM.7】IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.8】應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.9】應為根使用者啟用 MFA](#)
- [【IAM.10】IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.11】確保 IAM 密碼政策至少需要一個大寫字母](#)
- [【IAM.12】確保 IAM 密碼政策至少需要一個小寫字母](#)
- [【IAM.13】確保 IAM 密碼政策至少需要一個符號](#)
- [【IAM.14】確保 IAM 密碼政策至少需要一個數字](#)
- [【IAM.15】確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)
- [【IAM.16】確保 IAM 密碼政策防止密碼重複使用](#)
- [【IAM.17】確保 IAM 密碼政策在 90 天內過期密碼](#)
- [【IAM.18】確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.24】IAM 角色應加上標籤](#)
- [【IAM.25】IAM 使用者應加上標籤](#)
- [【IAM.26】應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】IAM 身分不應連接 AWSCloudShellFullAccess 政策](#)
- [【IAM.28】應啟用 IAM Access Analyzer 外部存取分析器](#)
- [【Inspector.1】應啟用 Amazon Inspector EC2 掃描](#)

- [【Inspector.2】 應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】 應啟用 Amazon Inspector Lambda 標準掃描](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】 AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】 AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】 AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Kinesis.1】 Kinesis 串流應靜態加密](#)

- [【Kinesis.3】 Kinesis 串流應具有足夠的資料保留期](#)
- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【KMS.5】 不應公開存取 KMS 金鑰](#)
- [【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MQ.4】 Amazon MQ 代理程式應加上標籤](#)
- [【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式](#)
- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密](#)
- [【MSK.2】 MSK 叢集應已設定增強型監控](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.4】 MSK 叢集應停用公有存取](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【MSK.6】 MSK 叢集應停用未驗證的存取](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【NetworkFirewall.1】 網路防火牆防火牆應部署在多個可用區域](#)
- [【NetworkFirewall.2】 應啟用網路防火牆記錄](#)

- [【NetworkFirewall.3】網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.4】Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)
- [【NetworkFirewall.5】網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】無狀態網路防火牆規則群組不應為空](#)
- [【NetworkFirewall.9】網路防火牆防火牆應啟用刪除保護](#)
- [【NetworkFirewall.10】網路防火牆防火牆應啟用子網路變更保護](#)
- [【Opensearch.1】OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.9】應標記 OpenSearch 網域](#)
- [【Opensearch.10】OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】OpenSearch 網域應至少具有三個專用主節點](#)
- [【PCA.1】應停用 AWS 私有 CA 根憑證授權單位](#)
- [【PCA.2】應標記 AWS 私有 CA 憑證授權單位](#)
- [【RDS.14】Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.18】RDS 執行個體應部署在 VPC 中](#)
- [【RDS.24】RDS 資料庫叢集應使用自訂管理員使用者名稱](#)
- [【RDS.25】RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)
- [【RDS.26】RDS 資料庫執行個體應受備份計劃保護](#)
- [【RDS.27】RDS 資料庫叢集應靜態加密](#)
- [【RDS.31】RDS 資料庫安全群組應加上標籤](#)
- [【RDS.34】Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【RDS.35】RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.36】RDS for PostgreSQL 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)

- [【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.38】 RDS for PostgreSQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.39】 RDS for MySQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.40】 RDS for SQL Server 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.41】 RDS for SQL Server 資料庫執行個體應在傳輸中加密](#)
- [【RDS.42】 RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密](#)
- [【RDS.44】 RDS for MariaDB 資料庫執行個體應在傳輸中加密](#)
- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【RDS.46】 RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中](#)
- [【RDS.47】 RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.48】 RDS for MySQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠](#)
- [【Redshift.16】 Redshift 叢集子網路群組應具有來自多個可用區域的子網路](#)
- [【Redshift.17】 應標記 Redshift 叢集參數群組](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)
- [【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.7】 S3 一般用途儲存貯體應使用跨區域複寫](#)
- [【S3.10】 已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態](#)

- [【S3.11】 S3 一般用途儲存貯體應啟用事件通知](#)
- [【S3.12】 ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取](#)
- [【S3.13】 S3 一般用途儲存貯體應具有生命週期組態](#)
- [【S3.19】 S3 存取點應啟用封鎖公開存取設定](#)
- [【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除](#)
- [【S3.22】 S3 一般用途儲存貯體應記錄物件層級寫入事件](#)
- [【S3.23】 S3 一般用途儲存貯體應記錄物件層級讀取事件](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.4】 SageMaker 端點生產變體的初始執行個體計數應大於 1](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】 應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】 應標記 SageMaker 映像](#)
- [【SageMaker.8】 SageMaker 筆記本執行個體應在支援的平台上執行](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.17】 SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.18】 使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.1】 SES 聯絡人清單應加上標籤](#)

- [【SES.2】 SES 組態集應加上標籤](#)
- [【SES.3】 SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【ServiceCatalog.1】 Service Catalog 產品組合只能在 AWS 組織內共用](#)
- [【SNS.4】 SNS 主題存取政策不應允許公開存取](#)
- [【SQS.1】 Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】 SQS 佇列應加上標籤](#)
- [【SQS.3】 SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.3】 Systems Manager 管理的 Amazon EC2 執行個體應具有 COMPLIANT 的關聯合規狀態](#)
- [【SSM.4】 SSM 文件不應公開](#)
- [【SSM.5】 SSM 文件應加上標籤](#)
- [【SSM.6】 SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)
- [【StepFunctions.1】 Step Functions 狀態機器應該已開啟記錄](#)
- [【Transfer.1】 AWS Transfer Family 工作流程應加上標籤](#)
- [【Transfer.2】 Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線](#)
- [【Transfer.3】 Transfer Family 連接器應該已啟用記錄](#)
- [【Transfer.4】 Transfer Family 協議應加上標籤](#)
- [【Transfer.5】 Transfer Family 憑證應加上標籤](#)
- [【Transfer.6】 Transfer Family 連接器應加上標籤](#)
- [【Transfer.7】 轉移系列設定檔應加上標籤](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.2】 AWS WAF 傳統區域規則應至少有一個條件](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.4】 AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.12】 AWS WAF 規則應啟用 CloudWatch 指標](#)

- [【WorkSpaces.1】應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】WorkSpaces 根磁碟區應靜態加密](#)

亞太地區 (東京)

亞太區域 (東京) 區域不支援下列控制項。

- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【EC2.173】具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】ECR 公有儲存庫應加上標籤](#)
- [【FraudDetector.1】Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】Amazon Fraud Detector 變數應加上標籤](#)

- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【IAM.26】應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IoT TwinMaker.4】AWS IoT TwinMaker 實體應加上標籤](#)
- [【Route53.1】應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【WAF.1】應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

加拿大 (中部)

加拿大（中部）區域不支援下列控制項。

- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)

- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoT TwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoT TwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoT TwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoT TwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoT Wireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoT Wireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoT Wireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)

- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Kinesis.3】 Kinesis 串流應具有足夠的資料保留期](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

加拿大西部 (卡加利)

加拿大西部 (卡加利) 區域不支援下列控制項。

- [【ACM.1】 匯入和 ACM 發行的憑證應在指定的期間之後續約](#)
- [【ACM.2】 由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)
- [【Account.1】 應針對 提供安全性聯絡資訊 AWS 帳戶](#)
- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppConfig.1】 AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】 AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】 AWS AppConfig 環境應加上標籤](#)
- [【AppConfig.4】 AWS AppConfig 應標記延伸關聯](#)
- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)

- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)
- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.2】 AWS AppSync 應該啟用欄位層級記錄](#)
- [【AppSync.5】 AWS AppSync GraphQL APIs不應使用 API 金鑰進行身分驗證](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【Athena.4】 Athena 工作群組應該已啟用記錄](#)
- [【AutoScaling.2】 Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域](#)
- [【AutoScaling.3】 Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【AutoScaling.6】 Auto Scaling 群組應在多個可用區域中使用多個執行個體類型](#)
- [【AutoScaling.9】 Amazon EC2 Auto Scaling 群組應使用 Amazon EC2 啟動範本](#)
- [【Backup.1】 AWS Backup 復原點應靜態加密](#)
- [【Backup.4】 應標記 AWS Backup 報告計劃](#)
- [【Batch.1】 批次任務佇列應加上標籤](#)
- [【Batch.3】 批次運算環境應加上標籤](#)
- [【Batch.4】 應標記受管批次運算環境中的運算資源屬性](#)
- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.3】 CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】 CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)

- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)
- [【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)
- [【CloudTrail.10】CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys](#)
- [【CloudWatch.17】應啟用 CloudWatch 警示動作](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料](#)
- [【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料](#)
- [【CodeBuild.3】CodeBuild S3 日誌應加密](#)
- [【CodeBuild.4】CodeBuild AWS Config專案環境應具有記錄 URL](#)
- [【CodeBuild.7】CodeBuild 報告群組匯出應靜態加密](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】Cognito 身分集區不應允許未驗證的身分](#)
- [【Connect.1】Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DataFirehose.1】Firehose 交付串流應靜態加密](#)

- [【DataSync.1】DataSync 任務應該已啟用記錄](#)
- [【Detective.1】應標記 Detective 行為圖表](#)
- [【DMS.2】DMS 憑證應加上標籤](#)
- [【DMS.3】DMS 事件訂閱應加上標籤](#)
- [【DMS.4】DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】DMS 端點應使用 SSL](#)
- [【DMS.10】Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DocumentDB.1】Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.4】DynamoDB 資料表應存在於備份計畫中](#)
- [【DynamoDB.6】DynamoDB 資料表應該已啟用刪除保護](#)
- [【DynamoDB.7】DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.21】網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)
- [【EC2.22】應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)

- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】 Amazon EC2 啟動範本不應將公IPs 指派給網路介面](#)
- [【EC2.28】 備份計畫應涵蓋 EBS 磁碟區](#)
- [【EC2.34】 EC2 傳輸閘道路由表應加上標籤](#)
- [【EC2.40】 EC2 NAT 閘道應加上標籤](#)
- [【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.53】 EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.54】 EC2 安全群組不應允許從 ::/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.55】 VPCs應使用 ECR API 的介面端點進行設定](#)
- [【EC2.56】 VPCs應使用 Docker 登錄檔的介面端點進行設定](#)
- [【EC2.57】 VPCs應使用 Systems Manager 的介面端點進行設定](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.171】 EC2 VPN 連線應該已啟用記錄](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【EC2.180】 EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.181】 EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定](#)
- [【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)
- [【ECR.2】 ECR 私有儲存庫應設定標籤不可變性](#)
- [【ECR.3】 ECR 儲存庫應至少設定一個生命週期政策](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ECR.5】 ECR 儲存庫應使用客戶受管加密 AWS KMS keys](#)
- [【ECS.3】 ECS 任務定義不應共用主機的程序命名空間](#)

- [【ECS.4】 ECS 容器應以非特殊權限執行](#)
- [【ECS.5】 ECS 任務定義應將容器設定為僅限對根檔案系統的唯讀存取](#)
- [【ECS.8】 不應將秘密做為容器環境變數傳遞](#)
- [【ECS.9】 ECS 任務定義應具有記錄組態](#)
- [【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行](#)
- [【ECS.12】 ECS 叢集應使用 Container Insights](#)
- [【ECS.16】 ECS 任務集不應自動指派公有 IP 地址](#)
- [【ECS.17】 ECS 任務定義不應使用主機網路模式](#)
- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【EFS.3】 EFS 存取點應強制執行根目錄](#)
- [【EFS.4】 EFS 存取點應強制執行使用者身分](#)
- [【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯](#)
- [【EFS.7】 EFS 檔案系統應該啟用自動備份](#)
- [【EFS.8】 EFS 檔案系統應靜態加密](#)
- [【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)
- [【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密](#)
- [【EKS.7】 EKS 身分提供者組態應加上標籤](#)
- [【EKS.8】 EKS 叢集應該啟用稽核記錄](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【ELB.10】 Classic Load Balancer 應跨越多個可用區域](#)
- [【ELB.12】 Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.13】 應用程式、網路和閘道負載平衡器應跨越多個可用區域](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.2】 ElastiCache 叢集應該啟用自動次要版本升級](#)

- [【ElastiCache.3】ElastiCache 複寫群組應該啟用自動容錯移轉](#)
- [【ElastiCache.4】ElastiCache 複寫群組應靜態加密](#)
- [【ElastiCache.5】ElastiCache 複寫群組應在傳輸中加密](#)
- [【ElastiCache.6】舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【EMR.2】 應啟用 Amazon EMR 封鎖公開存取設定](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【EventBridge.3】EventBridge 自訂事件匯流排應連接以資源為基礎的政策](#)
- [【EventBridge.4】EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.1】FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)
- [【FSx.2】FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)
- [【FSx.3】FSx for OpenZFS 檔案系統應設定為異地同步備份部署](#)
- [【FSx.4】FSx for NetApp ONTAP 檔案系統應設定為異地同步備份部署](#)
- [【FSx.5】FSx for Windows File Server 檔案系統應設定為異地同步備份部署](#)
- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【Glue.3】 AWS Glue 機器學習轉換應該靜態加密](#)
- [【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.2】GuardDuty 篩選條件應加上標籤](#)
- [【GuardDuty.5】應啟用 GuardDuty EKS 稽核日誌監控](#)
- [【GuardDuty.6】應啟用 GuardDuty Lambda 保護](#)

- [【GuardDuty.7】應啟用 GuardDuty EKS 執行期監控](#)
- [【GuardDuty.8】應啟用 EC2 的 GuardDuty 惡意軟體防護](#)
- [【GuardDuty.9】應啟用 GuardDuty RDS 保護](#)
- [【GuardDuty.10】應啟用 GuardDuty S3 保護](#)
- [【GuardDuty.11】應啟用 GuardDuty 執行期監控](#)
- [【GuardDuty.12】應啟用 GuardDuty ECS 執行期監控](#)
- [【GuardDuty.13】應啟用 GuardDuty EC2 執行期監控](#)
- [【IAM.1】IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.6】應為根使用者啟用硬體 MFA](#)
- [【IAM.7】IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.8】應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.9】應為根使用者啟用 MFA](#)
- [【IAM.10】IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.11】確保 IAM 密碼政策至少需要一個大寫字母](#)
- [【IAM.12】確保 IAM 密碼政策至少需要一個小寫字母](#)
- [【IAM.13】確保 IAM 密碼政策至少需要一個符號](#)
- [【IAM.14】確保 IAM 密碼政策至少需要一個數字](#)
- [【IAM.15】確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)
- [【IAM.16】確保 IAM 密碼政策防止密碼重複使用](#)
- [【IAM.17】確保 IAM 密碼政策在 90 天內過期密碼](#)
- [【IAM.18】確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】應移除 45 天內未使用的 IAM 使用者登入資料](#)

- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】 IAM 身分不應連接 AWS CloudShellFullAccess 政策](#)
- [【IAM.28】 應啟用 IAM Access Analyzer 外部存取分析器](#)
- [【Inspector.1】 應啟用 Amazon Inspector EC2 掃描](#)
- [【Inspector.2】 應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】 應啟用 Amazon Inspector Lambda 標準掃描](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】 AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】 AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】 AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoT TwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoT TwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoT TwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoT TwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)

- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Kinesis.1】 Kinesis 串流應靜態加密](#)
- [【Kinesis.3】 Kinesis 串流應具有足夠的資料保留期](#)
- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【KMS.5】 不應公開存取 KMS 金鑰](#)
- [【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MQ.4】 Amazon MQ 代理程式應加上標籤](#)
- [【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式](#)
- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密](#)
- [【MSK.2】 MSK 叢集應已設定增強型監控](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.4】 MSK 叢集應停用公有存取](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【MSK.6】 MSK 叢集應停用未驗證的存取](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)

- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【NetworkFirewall.1】 網路防火牆防火牆應部署在多個可用區域](#)
- [【NetworkFirewall.2】 應啟用網路防火牆記錄](#)
- [【NetworkFirewall.3】 網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.4】 Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)
- [【NetworkFirewall.5】 網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】 無狀態網路防火牆規則群組不應為空](#)
- [【NetworkFirewall.9】 網路防火牆防火牆應啟用刪除保護](#)
- [【NetworkFirewall.10】 網路防火牆防火牆應啟用子網路變更保護](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.9】 應標記 OpenSearch 網域](#)
- [【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【PCA.1】 應停用 AWS 私有 CA 根憑證授權單位](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.18】 RDS 執行個體應部署在 VPC 中](#)

- [【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱](#)
- [【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)
- [【RDS.26】 RDS 資料庫執行個體應受備份計劃保護](#)
- [【RDS.27】 RDS 資料庫叢集應靜態加密](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.36】 RDS for PostgreSQL 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.38】 RDS for PostgreSQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.39】 RDS for MySQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.40】 RDS for SQL Server 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.41】 RDS for SQL Server 資料庫執行個體應在傳輸中加密](#)
- [【RDS.42】 RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密](#)
- [【RDS.44】 RDS for MariaDB 資料庫執行個體應在傳輸中加密](#)
- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【RDS.46】 RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠](#)
- [【Redshift.16】 Redshift 叢集子網路群組應具有來自多個可用區域的子網路](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)

- [【RedshiftServerless.5】Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.7】S3 一般用途儲存貯體應使用跨區域複寫](#)
- [【S3.10】已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態](#)
- [【S3.11】S3 一般用途儲存貯體應啟用事件通知](#)
- [【S3.12】ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取](#)
- [【S3.13】S3 一般用途儲存貯體應具有生命週期組態](#)
- [【S3.19】S3 存取點應啟用封鎖公開存取設定](#)
- [【S3.20】S3 一般用途儲存貯體應啟用 MFA 刪除](#)
- [【S3.22】S3 一般用途儲存貯體應記錄物件層級寫入事件](#)
- [【S3.23】S3 一般用途儲存貯體應記錄物件層級讀取事件](#)
- [【S3.24】S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.4】SageMaker 端點生產變體的初始執行個體計數應大於 1](#)
- [【SageMaker.5】SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】應標記 SageMaker 映像](#)
- [【SageMaker.8】SageMaker 筆記本執行個體應在支援的平台上執行](#)
- [【SageMaker.9】SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】SageMaker 模型品質任務定義應該啟用容器間流量加密](#)

- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.17】 SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.18】 使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.3】 SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【ServiceCatalog.1】 Service Catalog 產品組合只能在 AWS 組織內共用](#)
- [【SNS.4】 SNS 主題存取政策不應允許公開存取](#)
- [【SQS.1】 Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】 SQS 佇列應加上標籤](#)
- [【SQS.3】 SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.4】 SSM 文件不應公開](#)
- [【SSM.6】 SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)
- [【StepFunctions.1】 Step Functions 狀態機器應該已開啟記錄](#)
- [【Transfer.2】 Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線](#)
- [【Transfer.3】 Transfer Family 連接器應該已啟用記錄](#)
- [【Transfer.4】 Transfer Family 協議應加上標籤](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.2】 AWS WAF 傳統區域規則應至少有一個條件](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.4】 AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.12】 AWS WAF 規則應啟用 CloudWatch 指標](#)

- [【WorkSpaces.1】應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】WorkSpaces 根磁碟區應靜態加密](#)

中國 (北京)

中國（北京）區域不支援下列控制項。

- [【ACM.1】匯入和 ACM 發行的憑證應在指定的期間之後續約](#)
- [【ACM.2】由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)
- [【Account.2】AWS 帳戶應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.2】API Gateway REST API 階段應設定為使用 SSL 憑證進行後端身分驗證](#)
- [【APIGateway.10】API Gateway V2 整合應使用 HTTPS 進行私有連線](#)
- [【APIGateway.11】API Gateway 網域名稱應使用建議的安全政策](#)
- [【Amplify.1】Amplify 應用程式應加上標籤](#)
- [【Amplify.2】Amplify 分支應加上標籤](#)
- [【AppConfig.1】AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】AWS AppConfig 環境應加上標籤](#)
- [【AppConfig.4】AWS AppConfig 應標記延伸關聯](#)
- [【AppFlow.1】Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【Backup.1】AWS Backup 復原點應靜態加密](#)
- [【Backup.4】應標記 AWS Backup 報告計劃](#)
- [【Batch.1】批次任務佇列應加上標籤](#)
- [【Batch.2】批次排程政策應加上標籤](#)
- [【Batch.3】批次運算環境應加上標籤](#)
- [【Batch.4】應標記受管批次運算環境中的運算資源屬性](#)

- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudTrail.10】 CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】 Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】 Cognito 身分集區不應允許未驗證的身分](#)
- [【Cognito.3】 Cognito 使用者集區的密碼政策應具有強大的組態](#)
- [【Cognito.4】 Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證](#)

- [【Cognito.5】 應為 Cognito 使用者集區啟用 MFA](#)
- [【Cognito.6】 Cognito 使用者集區應啟用刪除保護](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DataFirehose.1】 Firehose 交付串流應靜態加密](#)
- [【DataSync.2】 應標記 DataSync 任務](#)
- [【Detective.1】 應標記 Detective 行為圖表](#)
- [【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.4】 DynamoDB 資料表應存在於備份計畫中](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.20】 用於 an AWS Site-to-Site VPN 連線的兩個 VPN 通道都應啟動](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.28】 備份計畫應涵蓋 EBS 磁碟區](#)
- [【EC2.36】 EC2 客戶閘道應加上標籤](#)
- [【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.53】 EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.54】 EC2 安全群組不應允許從 :::/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.58】 VPCs 應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs 應使用 Systems Manager Incident Manager 的介面端點進行設定](#)

- [【EC2.171】 EC2 VPN 連線應該已啟用記錄](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.174】 EC2 DHCP 選項集應加上標籤](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.176】 EC2 字首清單應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.178】 應標記 EC2 流量鏡像篩選條件](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【EC2.180】 EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定](#)
- [【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯](#)
- [【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用提供的憑證 AWS Certificate Manager](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.21】 應用程式和 Network Load Balancer 目標群組應使用加密的運作狀態檢查通訊協定](#)
- [【ELB.22】 ELB 目標群組應使用加密傳輸通訊協定](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.2】 應啟用 Amazon EMR 封鎖公開存取設定](#)
- [【EMR.3】 Amazon EMR 安全組態應靜態加密](#)
- [【EMR.4】 Amazon EMR 安全組態應在傳輸中加密](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)

- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.1】 FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)
- [【FSx.2】 FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)
- [【FSx.5】 FSx for Windows File Server 檔案系統應設定為異地同步備份部署](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【GuardDuty.3】 GuardDuty IPSets 應加上標籤](#)
- [【GuardDuty.4】 GuardDuty 偵測器應加上標籤](#)
- [【GuardDuty.5】 應啟用 GuardDuty EKS 稽核日誌監控](#)
- [【GuardDuty.6】 應啟用 GuardDuty Lambda 保護](#)
- [【GuardDuty.7】 應啟用 GuardDuty EKS 執行期監控](#)
- [【GuardDuty.8】 應啟用 EC2 的 GuardDuty 惡意軟體防護](#)
- [【GuardDuty.9】 應啟用 GuardDuty RDS 保護](#)
- [【GuardDuty.10】 應啟用 GuardDuty S3 保護](#)
- [【GuardDuty.11】 應啟用 GuardDuty 執行期監控](#)
- [【GuardDuty.12】 應啟用 GuardDuty ECS 執行期監控](#)
- [【GuardDuty.13】 應啟用 GuardDuty EC2 執行期監控](#)
- [【IAM.6】 應為根使用者啟用硬體 MFA](#)
- [【IAM.9】 應為根使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.23】 IAM Access Analyzer 分析器應加上標籤](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】 IAM 身分不應連接 AWSCloudShellFullAccess 政策](#)
- [【IAM.28】 應啟用 IAM Access Analyzer 外部存取分析器](#)
- [【Inspector.1】 應啟用 Amazon Inspector EC2 掃描](#)
- [【Inspector.2】 應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】 應啟用 Amazon Inspector Lambda 標準掃描](#)

- [【IoTEvents.1】AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtTwinMaker.1】AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtTwinMaker.2】AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtTwinMaker.3】AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtTwinMaker.4】AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】IVS 記錄組態應加上標籤](#)
- [【IVS.3】IVS 頻道應加上標籤](#)
- [【Keyspaces.1】Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Macie.1】應啟用 Amazon Macie](#)
- [【Macie.2】應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.2】ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MSK.3】MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.5】MSK 連接器應該已啟用記錄](#)
- [【Neptune.1】Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】Neptune 資料庫叢集應該啟用自動備份](#)

- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【NetworkFirewall.1】 網路防火牆防火牆應部署在多個可用區域](#)
- [【NetworkFirewall.2】 應啟用網路防火牆記錄](#)
- [【NetworkFirewall.3】 網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.4】 Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)
- [【NetworkFirewall.5】 網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】 無狀態網路防火牆規則群組不應為空](#)
- [【NetworkFirewall.9】 網路防火牆防火牆應啟用刪除保護](#)
- [【NetworkFirewall.10】 網路防火牆防火牆應啟用子網路變更保護](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【PCA.1】 應停用 AWS 私有 CA 根憑證授權單位](#)
- [【PCA.2】 應標記 AWS 私有 CA 憑證授權單位](#)
- [【RDS.7】 RDS 叢集應該啟用刪除保護](#)
- [【RDS.12】 應為 RDS 叢集設定 IAM 身分驗證](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.15】 應為多個可用區域設定 RDS 資料庫叢集](#)
- [【RDS.16】 Aurora 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱](#)

- [【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)
- [【RDS.26】 RDS 資料庫執行個體應受備份計劃保護](#)
- [【RDS.27】 RDS 資料庫叢集應靜態加密](#)
- [【RDS.28】 RDS 資料庫叢集應加上標籤](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.42】 RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密](#)
- [【RDS.44】 RDS for MariaDB 資料庫執行個體應在傳輸中加密](#)
- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【RDS.47】 RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.48】 RDS for MySQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.50】 RDS 資料庫叢集應設定足夠的備份保留期間](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠](#)
- [【Redshift.17】 應標記 Redshift 叢集參數群組](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.22】 S3 一般用途儲存貯體應記錄物件層級寫入事件](#)
- [【S3.23】 S3 一般用途儲存貯體應記錄物件層級讀取事件](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.4】 SageMaker 端點生產變體的初始執行個體計數應大於 1](#)

- [【SageMaker.5】SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】應標記 SageMaker 映像](#)
- [【SageMaker.9】SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.19】SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.1】SES 聯絡人清單應加上標籤](#)
- [【SES.2】SES 組態集應加上標籤](#)
- [【SES.3】SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【ServiceCatalog.1】Service Catalog 產品組合只能在 AWS 組織內共用](#)
- [【SSM.5】SSM 文件應加上標籤](#)
- [【SSM.6】SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【Transfer.2】Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線](#)
- [【Transfer.4】Transfer Family 協議應加上標籤](#)
- [【Transfer.5】Transfer Family 憑證應加上標籤](#)
- [【Transfer.6】Transfer Family 連接器應加上標籤](#)
- [【Transfer.7】轉移系列設定檔應加上標籤](#)
- [【WAF.1】應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.3】AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.6】AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】應靜態加密 WorkSpaces 使用者磁碟區](#)

- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

中國 (寧夏)

中國 (寧夏) 區域不支援下列控制項。

- [【ACM.1】 匯入和 ACM 發行的憑證應在指定的期間之後續約](#)
- [【ACM.2】 由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)
- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.2】 API Gateway REST API 階段應設定為使用 SSL 憑證進行後端身分驗證](#)
- [【APIGateway.10】 API Gateway V2 整合應使用 HTTPS 進行私有連線](#)
- [【APIGateway.11】 API Gateway 網域名稱應使用建議的安全政策](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppConfig.1】 AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】 AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】 AWS AppConfig 環境應加上標籤](#)
- [【AppConfig.4】 AWS AppConfig 應標記延伸關聯](#)
- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)
- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【Backup.1】 AWS Backup 復原點應靜態加密](#)
- [【Backup.4】 應標記 AWS Backup 報告計劃](#)
- [【Batch.1】 批次任務佇列應加上標籤](#)
- [【Batch.2】 批次排程政策應加上標籤](#)
- [【Batch.3】 批次運算環境應加上標籤](#)
- [【Batch.4】 應標記受管批次運算環境中的運算資源屬性](#)
- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)

- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudTrail.10】 CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】 Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】 Cognito 身分集區不應允許未驗證的身分](#)
- [【Cognito.3】 Cognito 使用者集區的密碼政策應具有強大的組態](#)
- [【Cognito.4】 Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證](#)

- [【Cognito.5】 應為 Cognito 使用者集區啟用 MFA](#)
- [【Cognito.6】 Cognito 使用者集區應啟用刪除保護](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DataFirehose.1】 Firehose 交付串流應靜態加密](#)
- [【DataSync.2】 應標記 DataSync 任務](#)
- [【Detective.1】 應標記 Detective 行為圖表](#)
- [【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.4】 DynamoDB 資料表應存在於備份計畫中](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.20】 用於 an AWS Site-to-Site VPN 連線的兩個 VPN 通道都應啟動](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.28】 備份計畫應涵蓋 EBS 磁碟區](#)
- [【EC2.36】 EC2 客戶閘道應加上標籤](#)
- [【EC2.50】 EC2 VPN 閘道應加上標籤](#)
- [【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.171】 EC2 VPN 連線應該已啟用記錄](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.174】 EC2 DHCP 選項集應加上標籤](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)

- [【EC2.176】 EC2 字首清單應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.178】 應標記 EC2 流量鏡像篩選條件](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定](#)
- [【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【EFS.3】 EFS 存取點應強制執行根目錄](#)
- [【EFS.4】 EFS 存取點應強制執行使用者身分](#)
- [【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯](#)
- [【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.21】 應用程式和 Network Load Balancer 目標群組應使用加密的運作狀態檢查通訊協定](#)
- [【ELB.22】 ELB 目標群組應使用加密傳輸通訊協定](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.2】 應啟用 Amazon EMR 封鎖公開存取設定](#)
- [【EMR.3】 Amazon EMR 安全組態應靜態加密](#)
- [【EMR.4】 Amazon EMR 安全組態應在傳輸中加密](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.1】 FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)
- [【FSx.2】 FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)

- [【FSx.5】FSx for Windows File Server 檔案系統應設定為異地同步備份部署](#)
- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【Glue.3】AWS Glue 機器學習轉換應該靜態加密](#)
- [【GuardDuty.3】GuardDuty IPSets 應加上標籤](#)
- [【GuardDuty.4】GuardDuty 偵測器應加上標籤](#)
- [【GuardDuty.5】應啟用 GuardDuty EKS 稽核日誌監控](#)
- [【GuardDuty.6】應啟用 GuardDuty Lambda 保護](#)
- [【GuardDuty.7】應啟用 GuardDuty EKS 執行期監控](#)
- [【GuardDuty.8】應啟用 EC2 的 GuardDuty 惡意軟體防護](#)
- [【GuardDuty.9】應啟用 GuardDuty RDS 保護](#)
- [【GuardDuty.10】應啟用 GuardDuty S3 保護](#)
- [【GuardDuty.11】應啟用 GuardDuty 執行期監控](#)
- [【GuardDuty.12】應啟用 GuardDuty ECS 執行期監控](#)
- [【GuardDuty.13】應啟用 GuardDuty EC2 執行期監控](#)
- [【IAM.6】應為根使用者啟用硬體 MFA](#)
- [【IAM.9】應為根使用者啟用 MFA](#)
- [【IAM.21】您建立的 IAM 客戶受管政策不應允許服務的萬用字元動作](#)
- [【IAM.23】IAM Access Analyzer 分析器應加上標籤](#)
- [【IAM.24】IAM 角色應加上標籤](#)
- [【IAM.25】IAM 使用者應加上標籤](#)
- [【IAM.26】應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】IAM 身分不應連接 AWSCloudShellFullAccess 政策](#)
- [【IAM.28】應啟用 IAM Access Analyzer 外部存取分析器](#)
- [【Inspector.1】應啟用 Amazon Inspector EC2 掃描](#)
- [【Inspector.2】應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】應啟用 Amazon Inspector Lambda 標準掃描](#)
- [【IoTEvents.1】AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】AWS IoT Events 偵測器模型應加上標籤](#)

- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtTwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtTwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtTwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtTwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Lambda.1】 Lambda 函數政策應禁止公開存取](#)
- [【Lambda.2】 Lambda 函數應使用支援的執行時間](#)
- [【Lambda.3】 Lambda 函數應該位於 VPC 中](#)
- [【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作](#)
- [【Lambda.6】 應標記 Lambda 函數](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)

- [【NetworkFirewall.1】網路防火牆防火牆應部署在多個可用區域](#)
- [【NetworkFirewall.2】應啟用網路防火牆記錄](#)
- [【NetworkFirewall.3】網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.4】Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)
- [【NetworkFirewall.5】網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】無狀態網路防火牆規則群組不應為空](#)
- [【NetworkFirewall.9】網路防火牆防火牆應啟用刪除保護](#)
- [【NetworkFirewall.10】網路防火牆防火牆應啟用子網路變更保護](#)
- [【Opensearch.1】OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.11】OpenSearch 網域應至少具有三個專用主節點](#)
- [【PCA.1】應停用 AWS 私有 CA 根憑證授權單位](#)
- [【PCA.2】應標記 AWS 私有 CA 憑證授權單位](#)
- [【RDS.14】Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.24】RDS 資料庫叢集應使用自訂管理員使用者名稱](#)
- [【RDS.25】RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)
- [【RDS.26】RDS 資料庫執行個體應受備份計劃保護](#)
- [【RDS.31】RDS 資料庫安全群組應加上標籤](#)
- [【RDS.34】Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【RDS.35】RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.42】RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.43】RDS 資料庫代理應該需要連線的 TLS 加密](#)
- [【RDS.44】RDS for MariaDB 資料庫執行個體應在傳輸中加密](#)

- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【RDS.50】 RDS 資料庫叢集應設定足夠的備份保留期間](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠](#)
- [【Redshift.17】 應標記 Redshift 叢集參數群組](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.4】 SageMaker 端點生產變體的初始執行個體計數應大於 1](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】 應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】 應標記 SageMaker 映像](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.3】 SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【ServiceCatalog.1】 Service Catalog 產品組合只能在 AWS 組織內共用](#)
- [【SSM.5】 SSM 文件應加上標籤](#)

- [【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)
- [【StepFunctions.2】應標記 Step Functions 活動](#)
- [【Transfer.2】 Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線](#)
- [【Transfer.4】 Transfer Family 協議應加上標籤](#)
- [【Transfer.5】 Transfer Family 憑證應加上標籤](#)
- [【Transfer.6】 Transfer Family 連接器應加上標籤](#)
- [【Transfer.7】 轉移系列設定檔應加上標籤](#)
- [【WAF.1】應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

歐洲 (法蘭克福)

歐洲 (法蘭克福) 區域不支援下列控制項。

- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)

- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

歐洲 (愛爾蘭)

歐洲 (愛爾蘭) 區域不支援下列控制項。

- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)

- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

歐洲 (倫敦)

歐洲 (倫敦) 區域不支援下列控制項。

- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)

- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【EC2.24】不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.173】具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】ECR 公有儲存庫應加上標籤](#)
- [【FraudDetector.1】Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【IAM.26】應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IoTSiteWise.1】AWS IoT SiteWise 資產模型應加上標籤](#)

- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtTwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtTwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtTwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtTwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

歐洲 (米蘭)

歐洲 (米蘭) 區域不支援下列控制項。

- [【APIGateway.11】 API Gateway 網域名稱應使用建議的安全政策](#)

- [【AppFlow.1】Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)

- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】 已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.14】 安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】 AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】 AWS IoT Core 角色別名應加上標籤](#)

- [【IoT.6】 AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)

- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【RDS.1】 RDS 快照應為私有](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)
- [【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SSM.2】 Systems Manager 管理的 Amazon EC2 執行個體在修補程式安裝後應具有 COMPLIANT 的修補程式合規狀態](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

- [【WorkSpaces.1】應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】WorkSpaces 根磁碟區應靜態加密](#)

Europe (Paris)

歐洲（巴黎）區域不支援下列控制項。

- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Connect.1】Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DMS.13】DMS 複寫執行個體應設定為使用多個可用區域](#)

- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.5】 FSx for Windows File Server 檔案系統應設定為異地同步備份部署](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)

- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

歐洲 (西班牙)

歐洲（西班牙）區域不支援下列控制項。

- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppConfig.1】 AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】 AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】 AWS AppConfig 環境應加上標籤](#)
- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)
- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)

- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【Backup.1】 AWS Backup 復原點應靜態加密](#)
- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.3】 CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】 CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)

- [【Cognito.1】 Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】 Cognito 身分集區不應允許未驗證的身分](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【Detective.1】 應標記 Detective 行為圖表](#)
- [【DMS.2】 DMS 憑證應加上標籤](#)
- [【DMS.3】 DMS 事件訂閱應加上標籤](#)
- [【DMS.4】 DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】 DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】 DMS 端點應使用 SSL](#)
- [【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】 DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】 Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.1】 Amazon EBS 快照不應設定為可公開還原](#)
- [【EC2.4】 已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.14】 安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389](#)

- [【EC2.22】應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.24】不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】Amazon EC2 啟動範本不應將公IPs 指派給網路介面](#)
- [【EC2.34】EC2 傳輸閘道路由表應加上標籤](#)
- [【EC2.40】EC2 NAT 閘道應加上標籤](#)
- [【EC2.51】EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.58】VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.173】具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.175】EC2 啟動範本應加上標籤](#)
- [【EC2.177】應標記 EC2 流量鏡像工作階段](#)
- [【EC2.179】應標記 EC2 流量鏡像目標](#)
- [【EC2.180】EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.181】EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【ECR.4】ECR 公有儲存庫應加上標籤](#)
- [【EFS.1】彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】Amazon EFS 磁碟區應位於備份計劃中](#)
- [【ELB.2】具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【ELB.14】Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.17】具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ElastiCache.1】ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.6】舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】Elastic Beanstalk 應將日誌串流至 CloudWatch](#)

- [【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.2】 GuardDuty 篩選條件應加上標籤](#)
- [【IAM.1】 IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】 IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】 IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】 IAM 身分不應連接 AWS CloudShellFullAccess 政策](#)
- [【Inspector.1】 應啟用 Amazon Inspector EC2 掃描](#)
- [【Inspector.2】 應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】 應啟用 Amazon Inspector Lambda 標準掃描](#)

- [【IoTEvents.1】AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】IVS 記錄組態應加上標籤](#)
- [【IVS.3】IVS 頻道應加上標籤](#)
- [【Keyspaces.1】Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【KMS.1】IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【Lambda.1】Lambda 函數政策應禁止公開存取](#)
- [【Lambda.7】Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】應啟用 Amazon Macie](#)
- [【Macie.2】應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.2】ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MQ.4】Amazon MQ 代理程式應加上標籤](#)
- [【MQ.5】ActiveMQ 代理程式應使用作用中/待命部署模式](#)

- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.4】 MSK 叢集應停用公有存取](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【MSK.6】 MSK 叢集應停用未驗證的存取](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.9】 應標記 OpenSearch 網域](#)
- [【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【RDS.1】 RDS 快照應為私有](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)

- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應該啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.1】 SES 聯絡人清單應加上標籤](#)
- [【SES.2】 SES 組態集應加上標籤](#)
- [【SES.3】 SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【SQS.1】 Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】 SQS 佇列應加上標籤](#)
- [【SQS.3】 SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.6】 SSM Automation 應該啟用 CloudWatch 記錄](#)

- [【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)
- [【Transfer.3】 Transfer Family 連接器應該已啟用記錄](#)
- [【Transfer.4】 Transfer Family 協議應加上標籤](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

歐洲 (斯德哥爾摩)

歐洲 (斯德哥爾摩) 區域不支援下列控制項。

- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)
- [【AppSync.1】 AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】 AWS AppSync API 快取應在傳輸中加密](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】 CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】 CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)

- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】 Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)

- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtTwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtTwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtTwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtTwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

- [【WorkSpaces.1】應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】WorkSpaces 根磁碟區應靜態加密](#)

歐洲 (蘇黎世)

歐洲 (蘇黎世) 區域不支援下列控制項。

- [【APIGateway.8】API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】應為 API Gateway V2 階段設定存取記錄](#)
- [【Amplify.1】Amplify 應用程式應加上標籤](#)
- [【Amplify.2】Amplify 分支應加上標籤](#)
- [【AppConfig.1】AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】AWS AppConfig 環境應加上標籤](#)
- [【AppFlow.1】Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【Backup.1】AWS Backup 復原點應靜態加密](#)
- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.3】CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)

- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)
- [【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】Cognito 身分集區不應允許未驗證的身分](#)
- [【Connect.1】Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【Detective.1】應標記 Detective 行為圖表](#)
- [【DMS.2】DMS 憑證應加上標籤](#)
- [【DMS.3】DMS 事件訂閱應加上標籤](#)
- [【DMS.4】DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】DMS 複寫執行個體應啟用自動次要版本升級](#)

- [【DMS.7】目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】DMS 端點應使用 SSL](#)
- [【DMS.10】Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DocumentDB.1】Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.14】安全群組不應允許從 0.0.0.0/0 或 :::/0 傳入連接埠 3389](#)
- [【EC2.22】應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.24】不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】Amazon EC2 啟動範本不應將公 IPs 指派給網路介面](#)
- [【EC2.58】VPCs 應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】VPCs 應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.173】具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.175】EC2 啟動範本應加上標籤](#)
- [【EC2.180】EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.181】EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【ECR.4】ECR 公有儲存庫應加上標籤](#)

- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.6】 舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】 ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.2】 GuardDuty 篩選條件應加上標籤](#)
- [【IAM.1】 IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】 IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】 IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)

- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】 IAM 身分不應連接 AWSCloudShellFullAccess 政策](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】 AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】 AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】 AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtTwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtTwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtTwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtTwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)

- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MQ.4】 Amazon MQ 代理程式應加上標籤](#)
- [【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式](#)
- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.4】 MSK 叢集應停用公有存取](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【MSK.6】 MSK 叢集應停用未驗證的存取](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)

- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.9】 應標記 OpenSearch 網域](#)
- [【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【RDS.1】 RDS 快照應為私有](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】 應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】 應標記 SageMaker 映像](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)

- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.3】 SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【SQS.1】 Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】 SQS 佇列應加上標籤](#)
- [【SQS.3】 SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.6】 SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)
- [【Transfer.3】 Transfer Family 連接器應該已啟用記錄](#)
- [【Transfer.4】 Transfer Family 協議應加上標籤](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

以色列 (特拉維夫)

以色列 (特拉維夫) 區域不支援下列控制項。

- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)

- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.2】AWS AppSync 應該啟用欄位層級記錄](#)
- [【AppSync.5】AWS AppSync GraphQL APIs不應使用 API 金鑰進行身分驗證](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【Backup.1】AWS Backup 復原點應靜態加密](#)
- [【Backup.4】應標記 AWS Backup 報告計劃](#)
- [【Batch.1】批次任務佇列應加上標籤](#)
- [【Batch.3】批次運算環境應加上標籤](#)
- [【Batch.4】應標記受管批次運算環境中的運算資源屬性](#)
- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.3】CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)

- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.2】 Cognito 身分集區不應允許未驗證的身分](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DMS.2】 DMS 憑證應加上標籤](#)
- [【DMS.3】 DMS 事件訂閱應加上標籤](#)
- [【DMS.4】 DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】 DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】 DMS 端點應使用 SSL](#)
- [【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】 DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】 Amazon DocumentDB 叢集應在傳輸中加密](#)

- [【DynamoDB.3】DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.4】DynamoDB 資料表應存在於備份計畫中](#)
- [【DynamoDB.7】DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.14】安全群組不應允許從 0.0.0.0/0 或 ::/0 傳入連接埠 3389](#)
- [【EC2.22】應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】Amazon EC2 啟動範本不應將公 IPs 指派給網路介面](#)
- [【EC2.28】備份計畫應涵蓋 EBS 磁碟區](#)
- [【EC2.34】EC2 傳輸閘道路由表應加上標籤](#)
- [【EC2.40】EC2 NAT 閘道應加上標籤](#)
- [【EC2.51】EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.55】VPCs 應使用 ECR API 的介面端點進行設定](#)
- [【EC2.56】VPCs 應使用 Docker 登錄檔的介面端點進行設定](#)
- [【EC2.57】VPCs 應使用 Systems Manager 的介面端點進行設定](#)
- [【EC2.58】VPCs 應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】VPCs 應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.173】具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.175】EC2 啟動範本應加上標籤](#)
- [【EC2.177】應標記 EC2 流量鏡像工作階段](#)
- [【EC2.179】應標記 EC2 流量鏡像目標](#)
- [【EC2.180】EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.181】EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【ECR.2】ECR 私有儲存庫應設定標籤不可變性](#)
- [【ECR.3】ECR 儲存庫應至少設定一個生命週期政策](#)
- [【ECR.4】ECR 公有儲存庫應加上標籤](#)
- [【ECR.5】ECR 儲存庫應使用客戶受管加密 AWS KMS keys](#)

- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【EFS.3】 EFS 存取點應強制執行根目錄](#)
- [【EFS.4】 EFS 存取點應強制執行使用者身分](#)
- [【EFS.8】 EFS 檔案系統應靜態加密](#)
- [【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)
- [【EKS.7】 EKS 身分提供者組態應加上標籤](#)
- [【EKS.8】 EKS 叢集應該啟用稽核記錄](#)
- [【ELB.2】 具有 SSL/HTTPS 接聽程式的 Classic Load Balancer 應使用 提供的憑證 AWS Certificate Manager](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ElasticCache.1】 ElasticCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElasticCache.2】 ElasticCache 叢集應該啟用自動次要版本升級](#)
- [【ElasticCache.3】 ElasticCache 複寫群組應該啟用自動容錯移轉](#)
- [【ElasticCache.4】 ElasticCache 複寫群組應靜態加密](#)
- [【ElasticCache.5】 ElasticCache 複寫群組應在傳輸中加密](#)
- [【ElasticCache.6】 舊版的 ElasticCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElasticCache.7】 ElasticCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)

- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.2】 GuardDuty 篩選條件應加上標籤](#)
- [【IAM.1】 IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】 IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】 IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.6】 應為根使用者啟用硬體 MFA](#)
- [【IAM.7】 IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.9】 應為根使用者啟用 MFA](#)
- [【IAM.10】 IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.11】 確保 IAM 密碼政策至少需要一個大寫字母](#)
- [【IAM.12】 確保 IAM 密碼政策至少需要一個小寫字母](#)
- [【IAM.13】 確保 IAM 密碼政策至少需要一個符號](#)
- [【IAM.14】 確保 IAM 密碼政策至少需要一個數字](#)
- [【IAM.15】 確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)
- [【IAM.16】 確保 IAM 密碼政策防止密碼重複使用](#)
- [【IAM.17】 確保 IAM 密碼政策在 90 天內過期密碼](#)
- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】 IAM 身分不應連接 AWSCloudShellFullAccess 政策](#)

- [【IAM.28】 應啟用 IAM Access Analyzer 外部存取分析器](#)
- [【Inspector.1】 應啟用 Amazon Inspector EC2 掃描](#)
- [【Inspector.2】 應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】 應啟用 Amazon Inspector Lambda 標準掃描](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】 AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】 AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】 AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)

- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Kinesis.1】 Kinesis 串流應靜態加密](#)
- [【Kinesis.3】 Kinesis 串流應具有足夠的資料保留期](#)
- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MQ.4】 Amazon MQ 代理程式應加上標籤](#)
- [【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式](#)
- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密](#)
- [【MSK.2】 MSK 叢集應已設定增強型監控](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.4】 MSK 叢集應停用公有存取](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【MSK.6】 MSK 叢集應停用未驗證的存取](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【NetworkFirewall.10】 網路防火牆防火牆應啟用子網路變更保護](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)

- [【Opensearch.9】 應標記 OpenSearch 網域](#)
- [【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【RDS.1】 RDS 快照應為私有](#)
- [【RDS.4】 RDS 叢集快照和資料庫快照應靜態加密](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.26】 RDS 資料庫執行個體應受備份計劃保護](#)
- [【RDS.29】 應標記 RDS 資料庫叢集快照](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)
- [【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應該啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)

- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【ServiceCatalog.1】 Service Catalog 產品組合只能在 AWS 組織內共用](#)
- [【SQS.1】 Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】 SQS 佇列應加上標籤](#)
- [【SQS.3】 SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.4】 SSM 文件不應公開](#)
- [【SSM.6】 SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)
- [【StepFunctions.1】 Step Functions 狀態機器應該已開啟記錄](#)
- [【Transfer.3】 Transfer Family 連接器應該已啟用記錄](#)
- [【Transfer.4】 Transfer Family 協議應加上標籤](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

墨西哥 (中部)

墨西哥 (中部) 區域不支援下列控制項。

- [【ACM.1】 匯入和 ACM 發行的憑證應在指定的期間之後續約](#)
- [【ACM.2】 由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)
- [【Account.1】 應針對 提供安全性聯絡資訊 AWS 帳戶](#)
- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)

- [【APIGateway.9】應為 API Gateway V2 階段設定存取記錄](#)
- [【APIGateway.10】API Gateway V2 整合應使用 HTTPS 進行私有連線](#)
- [【Amplify.1】Amplify 應用程式應加上標籤](#)
- [【Amplify.2】Amplify 分支應加上標籤](#)
- [【AppConfig.1】AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】AWS AppConfig 環境應加上標籤](#)
- [【AppConfig.4】AWS AppConfig 應標記延伸關聯](#)
- [【AppFlow.1】Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.2】AWS AppSync 應該啟用欄位層級記錄](#)
- [【AppSync.4】AWS AppSync GraphQL APIs應加上標籤](#)
- [【AppSync.5】AWS AppSync GraphQL APIs不應使用 API 金鑰進行身分驗證](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【Athena.4】Athena 工作群組應該已啟用記錄](#)
- [【AutoScaling.2】Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域](#)
- [【AutoScaling.3】Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【AutoScaling.6】Auto Scaling 群組應在多個可用區域中使用多個執行個體類型](#)
- [【AutoScaling.9】Amazon EC2 Auto Scaling 群組應使用 Amazon EC2 啟動範本](#)
- [【Backup.1】AWS Backup 復原點應靜態加密](#)
- [【Backup.2】AWS Backup 復原點應加上標籤](#)
- [【Backup.4】應標記 AWS Backup 報告計劃](#)
- [【Batch.1】批次任務佇列應加上標籤](#)
- [【Batch.2】批次排程政策應加上標籤](#)
- [【Batch.3】批次運算環境應加上標籤](#)
- [【Batch.4】應標記受管批次運算環境中的運算資源屬性](#)

- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.3】CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudTrail.6】確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)
- [【CloudTrail.7】確定 CloudTrail S3 儲存貯體上已啟用 S3 儲存貯體存取記錄](#)
- [【CloudTrail.10】CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys](#)
- [【CloudWatch.17】應啟用 CloudWatch 警示動作](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeBuild.1】CodeBuild Bitbucket 來源儲存庫 URLs 不應包含敏感登入資料](#)

- [【CodeBuild.2】CodeBuild 專案環境變數不應包含純文字登入資料](#)
- [【CodeBuild.3】CodeBuild S3 日誌應加密](#)
- [【CodeBuild.4】CodeBuild AWS Config專案環境應具有記錄 URL](#)
- [【CodeBuild.7】CodeBuild 報告群組匯出應靜態加密](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】Cognito 身分集區不應允許未驗證的身分](#)
- [【Cognito.3】Cognito 使用者集區的密碼政策應具有強大的組態](#)
- [【Cognito.4】Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證](#)
- [【Cognito.5】應為 Cognito 使用者集區啟用 MFA](#)
- [【Cognito.6】Cognito 使用者集區應啟用刪除保護](#)
- [【Connect.1】Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DataFirehose.1】Firehose 交付串流應靜態加密](#)
- [【DataSync.1】DataSync 任務應該已啟用記錄](#)
- [【DataSync.2】應標記 DataSync 任務](#)
- [【Detective.1】應標記 Detective 行為圖表](#)
- [【DMS.2】DMS 憑證應加上標籤](#)
- [【DMS.3】DMS 事件訂閱應加上標籤](#)
- [【DMS.4】DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】DMS 端點應使用 SSL](#)
- [【DMS.10】Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】MongoDB 的 DMS 端點應啟用身分驗證機制](#)

- [【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】 DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】 Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.4】 DynamoDB 資料表應存在於備份計畫中](#)
- [【DynamoDB.6】 DynamoDB 資料表應該已啟用刪除保護](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】 已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】 Amazon EC2 啟動範本不應將公IPs 指派給網路介面](#)
- [【EC2.28】 備份計畫應涵蓋 EBS 磁碟區](#)
- [【EC2.34】 EC2 傳輸閘道路由表應加上標籤](#)
- [【EC2.40】 EC2 NAT 閘道應加上標籤](#)
- [【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.53】 EC2 安全群組不應允許從 0.0.0.0/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.54】 EC2 安全群組不應允許從 ::/0 傳入遠端伺服器管理連接埠](#)
- [【EC2.55】 VPCs應使用 ECR API 的介面端點進行設定](#)
- [【EC2.56】 VPCs應使用 Docker 登錄檔的介面端點進行設定](#)
- [【EC2.57】 VPCs應使用 Systems Manager 的介面端點進行設定](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)

- [【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.171】 EC2 VPN 連線應該已啟用記錄](#)
- [【EC2.172】 EC2 VPC 封鎖公開存取設定應封鎖網際網路閘道流量](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.174】 EC2 DHCP 選項集應加上標籤](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.176】 EC2 字首清單應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.178】 應標記 EC2 流量鏡像篩選條件](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【EC2.180】 EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.181】 EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【EC2.182】 應為 Amazon EBS 快照啟用封鎖公開存取設定](#)
- [【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定](#)
- [【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)
- [【ECR.2】 ECR 私有儲存庫應設定標籤不可變性](#)
- [【ECR.3】 ECR 儲存庫應至少設定一個生命週期政策](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ECR.5】 ECR 儲存庫應使用客戶受管加密 AWS KMS keys](#)
- [【ECS.3】 ECS 任務定義不應共用主機的程序命名空間](#)
- [【ECS.4】 ECS 容器應以非特殊權限執行](#)
- [【ECS.5】 ECS 任務定義應將容器設定為僅限對根檔案系統的唯一讀存取](#)
- [【ECS.8】 不應將秘密做為容器環境變數傳遞](#)
- [【ECS.9】 ECS 任務定義應具有記錄組態](#)
- [【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行](#)
- [【ECS.12】 ECS 叢集應使用 Container Insights](#)
- [【ECS.16】 ECS 任務集不應自動指派公有 IP 地址](#)
- [【ECS.17】 ECS 任務定義不應使用主機網路模式](#)
- [【ECS.18】 ECS 任務定義應針對 EFS 磁碟區使用傳輸中加密](#)

- [【ECS.19】 ECS 容量提供者應啟用受管終止保護](#)
- [【ECS.20】 ECS 任務定義應在 Linux 容器定義中設定非根使用者](#)
- [【ECS.21】 ECS 任務定義應在 Windows 容器定義中設定非管理員使用者](#)
- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【EFS.3】 EFS 存取點應強制執行根目錄](#)
- [【EFS.4】 EFS 存取點應強制執行使用者身分](#)
- [【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯](#)
- [【EFS.7】 EFS 檔案系統應該啟用自動備份](#)
- [【EFS.8】 EFS 檔案系統應靜態加密](#)
- [【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)
- [【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密](#)
- [【EKS.7】 EKS 身分提供者組態應加上標籤](#)
- [【EKS.8】 EKS 叢集應該啟用稽核記錄](#)
- [【EKS.9】 EKS 節點群組應在支援的 Kubernetes 版本上執行](#)
- [【ELB.10】 Classic Load Balancer 應跨越多個可用區域](#)
- [【ELB.12】 Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.13】 應用程式、網路和閘道負載平衡器應跨越多個可用區域](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.2】 ElastiCache 叢集應該啟用自動次要版本升級](#)
- [【ElastiCache.3】 ElastiCache 複寫群組應該啟用自動容錯移轉](#)
- [【ElastiCache.4】 ElastiCache 複寫群組應靜態加密](#)
- [【ElastiCache.5】 ElastiCache 複寫群組應在傳輸中加密](#)
- [【ElastiCache.6】 舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】 ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)

- [【ElasticBeanstalk.2】應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.1】Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【EMR.2】應啟用 Amazon EMR 封鎖公開存取設定](#)
- [【EMR.3】Amazon EMR 安全組態應靜態加密](#)
- [【EMR.4】Amazon EMR 安全組態應在傳輸中加密](#)
- [【ES.3】Elasticsearch 網域應該加密節點之間傳送的資料](#)
- [【ES.4】應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【ES.9】應標記 Elasticsearch 網域](#)
- [【EventBridge.3】EventBridge 自訂事件匯流排應連接以資源為基礎的政策](#)
- [【EventBridge.4】EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.1】FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)
- [【FSx.2】FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)
- [【FSx.3】FSx for OpenZFS 檔案系統應設定為異地同步備份部署](#)
- [【FSx.4】FSx for NetApp ONTAP 檔案系統應設定為異地同步備份部署](#)
- [【FSx.5】FSx for Windows File Server 檔案系統應設定為異地同步備份部署](#)
- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【Glue.1】AWS Glue 工作應加上標籤](#)
- [【Glue.3】AWS Glue 機器學習轉換應該靜態加密](#)
- [【Glue.4】AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.1】應啟用 GuardDuty](#)
- [【GuardDuty.2】GuardDuty 篩選條件應加上標籤](#)
- [【GuardDuty.5】應啟用 GuardDuty EKS 稽核日誌監控](#)
- [【GuardDuty.6】應啟用 GuardDuty Lambda 保護](#)
- [【GuardDuty.7】應啟用 GuardDuty EKS 執行期監控](#)

- [【GuardDuty.8】應啟用 EC2 的 GuardDuty 惡意軟體防護](#)
- [【GuardDuty.9】應啟用 GuardDuty RDS 保護](#)
- [【GuardDuty.10】應啟用 GuardDuty S3 保護](#)
- [【GuardDuty.11】應啟用 GuardDuty 執行期監控](#)
- [【GuardDuty.12】應啟用 GuardDuty ECS 執行期監控](#)
- [【GuardDuty.13】應啟用 GuardDuty EC2 執行期監控](#)
- [【IAM.1】IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.6】應為根使用者啟用硬體 MFA](#)
- [【IAM.7】IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.8】應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.9】應為根使用者啟用 MFA](#)
- [【IAM.10】IAM 使用者的密碼政策應具有強大的組態](#)
- [【IAM.11】確保 IAM 密碼政策至少需要一個大寫字母](#)
- [【IAM.12】確保 IAM 密碼政策至少需要一個小寫字母](#)
- [【IAM.13】確保 IAM 密碼政策至少需要一個符號](#)
- [【IAM.14】確保 IAM 密碼政策至少需要一個數字](#)
- [【IAM.15】確保 IAM 密碼政策要求密碼長度下限為 14 或更高](#)
- [【IAM.16】確保 IAM 密碼政策防止密碼重複使用](#)
- [【IAM.17】確保 IAM 密碼政策在 90 天內過期密碼](#)
- [【IAM.18】確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.24】IAM 角色應加上標籤](#)
- [【IAM.25】IAM 使用者應加上標籤](#)

- [【IAM.26】應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】IAM 身分不應連接 AWS CloudShellFullAccess 政策](#)
- [【IAM.28】應啟用 IAM Access Analyzer 外部存取分析器](#)
- [【Inspector.1】應啟用 Amazon Inspector EC2 掃描](#)
- [【Inspector.2】應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【Inspector.4】應啟用 Amazon Inspector Lambda 標準掃描](#)
- [【IoT.1】AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】AWS IoT Core 維度應加上標籤](#)
- [【IoT.4】AWS IoT Core 授權方應加上標籤](#)
- [【IoT.5】AWS IoT Core 角色別名應加上標籤](#)
- [【IoT.6】AWS IoT Core 政策應加上標籤](#)
- [【IoTEvents.1】AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】AWS IoT SiteWise 專案應加上標籤](#)
- [【IoT TwinMaker.1】AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoT TwinMaker.2】AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoT TwinMaker.3】AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoT TwinMaker.4】AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】IVS 播放金鑰對應加上標籤](#)

- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Kinesis.1】 Kinesis 串流應靜態加密](#)
- [【Kinesis.3】 Kinesis 串流應具有足夠的資料保留期](#)
- [【KMS.1】 IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】 IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【KMS.5】 不應公開存取 KMS 金鑰](#)
- [【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作](#)
- [【Lambda.7】 Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch](#)
- [【MQ.4】 Amazon MQ 代理程式應加上標籤](#)
- [【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式](#)
- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密](#)
- [【MSK.2】 MSK 叢集應已設定增強型監控](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.4】 MSK 叢集應停用公有存取](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【MSK.6】 MSK 叢集應停用未驗證的存取](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)

- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【NetworkFirewall.1】 網路防火牆防火牆應部署在多個可用區域](#)
- [【NetworkFirewall.2】 應啟用網路防火牆記錄](#)
- [【NetworkFirewall.3】 網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.4】 Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)
- [【NetworkFirewall.5】 網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】 無狀態網路防火牆規則群組不應為空](#)
- [【NetworkFirewall.9】 網路防火牆防火牆應啟用刪除保護](#)
- [【NetworkFirewall.10】 網路防火牆防火牆應啟用子網路變更保護](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.9】 應標記 OpenSearch 網域](#)
- [【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【PCA.1】 應停用 AWS 私有 CA 根憑證授權單位](#)
- [【PCA.2】 應標記 AWS 私有 CA 憑證授權單位](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.18】 RDS 執行個體應部署在 VPC 中](#)
- [【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱](#)
- [【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)
- [【RDS.26】 RDS 資料庫執行個體應受備份計劃保護](#)
- [【RDS.27】 RDS 資料庫叢集應靜態加密](#)

- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.36】 RDS for PostgreSQL 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.38】 RDS for PostgreSQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.39】 RDS for MySQL 資料庫執行個體應在傳輸中加密](#)
- [【RDS.40】 RDS for SQL Server 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.41】 RDS for SQL Server 資料庫執行個體應在傳輸中加密](#)
- [【RDS.42】 RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密](#)
- [【RDS.44】 RDS for MariaDB 資料庫執行個體應在傳輸中加密](#)
- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【RDS.46】 RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中](#)
- [【RDS.47】 RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.48】 RDS for MySQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【Redshift.1】 Amazon Redshift 叢集應禁止公開存取](#)
- [【Redshift.2】 與 Amazon Redshift 叢集的連線應在傳輸中加密](#)
- [【Redshift.3】 Amazon Redshift 叢集應該啟用自動快照](#)
- [【Redshift.4】 Amazon Redshift 叢集應該啟用稽核記錄](#)
- [【Redshift.6】 Amazon Redshift 應已啟用主要版本的自動升級](#)
- [【Redshift.7】 Redshift 叢集應使用增強型 VPC 路由](#)
- [【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.11】 應標記 Redshift 叢集](#)
- [【Redshift.13】 應標記 Redshift 叢集快照](#)
- [【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠](#)
- [【Redshift.16】 Redshift 叢集子網路群組應具有來自多個可用區域的子網路](#)

- [【Redshift.17】 應標記 Redshift 叢集參數群組](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)
- [【RedshiftServerless.5】 Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.7】 S3 一般用途儲存貯體應使用跨區域複寫](#)
- [【S3.10】 已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態](#)
- [【S3.11】 S3 一般用途儲存貯體應啟用事件通知](#)
- [【S3.12】 ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取](#)
- [【S3.13】 S3 一般用途儲存貯體應具有生命週期組態](#)
- [【S3.19】 S3 存取點應啟用封鎖公開存取設定](#)
- [【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除](#)
- [【S3.22】 S3 一般用途儲存貯體應記錄物件層級寫入事件](#)
- [【S3.23】 S3 一般用途儲存貯體應記錄物件層級讀取事件](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.4】 SageMaker 端點生產變體的初始執行個體計數應大於 1](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】 應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】 應標記 SageMaker 映像](#)
- [【SageMaker.8】 SageMaker 筆記本執行個體應在支援的平台上執行](#)

- [【SageMaker.9】SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】SageMaker 模型可解釋性任務定義應該啟用容器間流量加密](#)
- [【SageMaker.11】SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.17】SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.18】使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.19】SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.1】SES 聯絡人清單應加上標籤](#)
- [【SES.2】SES 組態集應加上標籤](#)
- [【SES.3】SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【ServiceCatalog.1】Service Catalog 產品組合只能在 AWS 組織內共用](#)
- [【SNS.4】SNS 主題存取政策不應允許公開存取](#)
- [【SQS.1】Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】SQS 佇列應加上標籤](#)
- [【SQS.3】SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.3】Systems Manager 管理的 Amazon EC2 執行個體應具有 COMPLIANT 的關聯合規狀態](#)
- [【SSM.4】SSM 文件不應公開](#)
- [【SSM.5】SSM 文件應加上標籤](#)
- [【SSM.6】SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【SSM.7】SSM 文件應啟用封鎖公開共用設定](#)
- [【StepFunctions.1】Step Functions 狀態機器應該已開啟記錄](#)
- [【Transfer.2】Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線](#)
- [【Transfer.3】Transfer Family 連接器應該已啟用記錄](#)
- [【Transfer.4】Transfer Family 協議應加上標籤](#)
- [【Transfer.5】Transfer Family 憑證應加上標籤](#)

- [【Transfer.6】 Transfer Family 連接器應加上標籤](#)
- [【Transfer.7】 轉移系列設定檔應加上標籤](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.2】 AWS WAF 傳統區域規則應至少有一個條件](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.4】 AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.12】 AWS WAF 規則應啟用 CloudWatch 指標](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

Middle East (Bahrain)

中東（巴林）區域不支援下列控制項。

- [【APIGateway.11】 API Gateway 網域名稱應使用建議的安全政策](#)
- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】 App Runner 服務應加上標籤](#)
- [【AppRunner.2】 應標記 App Runner VPC 連接器](#)
- [【BedrockAgentCore.1】 Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】 Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】 Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】 Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】 Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】 Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFront.1】 CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】 CloudFront 分佈應要求傳輸中加密](#)

- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudTrail.10】CloudTrail Lake 事件資料存放區應使用客戶受管加密 AWS KMS keys](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Connect.1】Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DocumentDB.1】Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DocumentDB.6】Amazon DocumentDB 叢集應在傳輸中加密](#)
- [【DynamoDB.3】DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.20】用於 an AWS Site-to-Site VPN 連線的兩個 VPN 通道都應啟動](#)
- [【EC2.24】不應使用 Amazon EC2 全虛擬化執行個體類型](#)

- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ECR.5】 ECR 儲存庫應使用客戶受管加密 AWS KMS keys](#)
- [【ECS.17】 ECS 任務定義不應使用主機網路模式](#)
- [【EKS.9】 EKS 節點群組應在支援的 Kubernetes 版本上執行](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.3】 FSx for OpenZFS 檔案系統應設定為異地同步備份部署](#)
- [【FSx.4】 FSx for NetApp ONTAP 檔案系統應設定為異地同步備份部署](#)
- [【FSx.5】 FSx for Windows File Server 檔案系統應設定為異地同步備份部署](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.11】 應啟用 GuardDuty 執行期監控](#)
- [【GuardDuty.12】 應啟用 GuardDuty ECS 執行期監控](#)
- [【GuardDuty.13】 應啟用 GuardDuty EC2 執行期監控](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)

- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtTwinMaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtTwinMaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtTwinMaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtTwinMaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【NetworkFirewall.10】 網路防火牆防火牆應啟用子網路變更保護](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.41】 RDS for SQL Server 資料庫執行個體應在傳輸中加密](#)
- [【RDS.42】 RDS for MariaDB 資料庫執行個體應將日誌發佈至 CloudWatch Logs](#)
- [【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密](#)
- [【RDS.44】 RDS for MariaDB 資料庫執行個體應在傳輸中加密](#)
- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【RDS.46】 RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.4】 Redshift Serverless 命名空間應使用客戶受管加密 AWS KMS keys](#)

- [【RedshiftServerless.5】Redshift Serverless 命名空間不應使用預設的管理員使用者名稱](#)
- [【RedshiftServerless.6】Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.8】SageMaker 筆記本執行個體應在支援的平台上執行](#)
- [【SageMaker.16】SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.17】SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.18】使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.19】SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SQS.3】SQS 佇列存取政策不應允許公開存取](#)
- [【Transfer.3】Transfer Family 連接器應該已啟用記錄](#)
- [【WAF.1】應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】WorkSpaces 根磁碟區應靜態加密](#)

中東 (阿拉伯聯合大公國)

中東 (阿拉伯聯合大公國) 區域不支援下列控制項。

- [【APIGateway.8】API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】應為 API Gateway V2 階段設定存取記錄](#)
- [【APIGateway.11】API Gateway 網域名稱應使用建議的安全政策](#)
- [【Amplify.1】Amplify 應用程式應加上標籤](#)
- [【Amplify.2】Amplify 分支應加上標籤](#)
- [【AppConfig.1】AWS AppConfig 應用程式應加上標籤](#)

- [【AppConfig.2】AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】AWS AppConfig 環境應加上標籤](#)
- [【AppFlow.1】Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【Backup.1】AWS Backup 復原點應靜態加密](#)
- [【Backup.4】應標記 AWS Backup 報告計劃](#)
- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFormation.3】CloudFormation 堆疊應啟用終止保護](#)
- [【CloudFormation.4】CloudFormation 堆疊應具有相關聯的服務角色](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)

- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudTrail.6】 確保用於存放 CloudTrail 日誌的 S3 儲存貯體不可公開存取](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】 Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】 Cognito 身分集區不應允許未驗證的身分](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【Detective.1】 應標記 Detective 行為圖表](#)
- [【DMS.2】 DMS 憑證應加上標籤](#)
- [【DMS.3】 DMS 事件訂閱應加上標籤](#)
- [【DMS.4】 DMS 複寫執行個體應加上標籤](#)
- [【DMS.5】 DMS 複寫子網路群組應加上標籤](#)
- [【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.9】 DMS 端點應使用 SSL](#)
- [【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權](#)
- [【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制](#)
- [【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS](#)
- [【DMS.13】 DMS 複寫執行個體應設定為使用多個可用區域](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.4】 已停止的 EC2 執行個體應在指定的期間之後移除](#)
- [【EC2.14】 安全群組不應允許從 0.0.0.0/0 或 :::/0 傳入連接埠 3389](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)

- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】 Amazon EC2 啟動範本不應將公IPs 指派給網路介面](#)
- [【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【EC2.180】 EC2 網路介面應啟用來源/目的地檢查](#)
- [【EC2.181】 EC2 啟動範本應為連接的 EBS 磁碟區啟用加密](#)
- [【EC2.183】 EC2 VPN 連線應使用 IKEv2 通訊協定](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【EFS.1】 彈性檔案系統應設定為使用 加密靜態檔案資料 AWS KMS](#)
- [【EFS.2】 Amazon EFS 磁碟區應位於備份計劃中](#)
- [【EKS.9】 EKS 節點群組應在支援的 Kubernetes 版本上執行](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策](#)
- [【ELB.18】 應用程式和 Network Load Balancer 接聽程式應使用安全通訊協定來加密傳輸中的資料](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.2】 ElastiCache 叢集應該啟用自動次要版本升級](#)
- [【ElastiCache.3】 ElastiCache 複寫群組應該啟用自動容錯移轉](#)
- [【ElastiCache.4】 ElastiCache 複寫群組應靜態加密](#)
- [【ElastiCache.5】 ElastiCache 複寫群組應在傳輸中加密](#)
- [【ElastiCache.6】 舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】 ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)

- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.1】 Amazon EMR 叢集主節點不應具有公有 IP 地址](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue](#)
- [【GuardDuty.2】 GuardDuty 篩選條件應加上標籤](#)
- [【IAM.1】 IAM 政策不應允許完整的「*」管理權限](#)
- [【IAM.2】 IAM 使用者不應連接 IAM 政策](#)
- [【IAM.3】 IAM 使用者的存取金鑰應每 90 天或更短時間輪換一次](#)
- [【IAM.4】 IAM 根使用者存取金鑰不應存在](#)
- [【IAM.5】 應為所有擁有主控台密碼的 IAM 使用者啟用 MFA](#)
- [【IAM.6】 應為根使用者啟用硬體 MFA](#)
- [【IAM.8】 應移除未使用的 IAM 使用者登入資料](#)
- [【IAM.9】 應為根使用者啟用 MFA](#)
- [【IAM.18】 確保已建立支援角色來使用 管理事件 AWS 支援](#)
- [【IAM.19】 應為所有 IAM 使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.22】 應移除 45 天內未使用的 IAM 使用者登入資料](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.27】 IAM 身分不應連接 AWSCloudShellFullAccess 政策](#)
- [【Inspector.1】 應啟用 Amazon Inspector EC2 掃描](#)
- [【Inspector.2】 應啟用 Amazon Inspector ECR 掃描](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)

- [【Inspector.4】應啟用 Amazon Inspector Lambda 標準掃描](#)
- [【IoTEvents.1】AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】IVS 記錄組態應加上標籤](#)
- [【IVS.3】IVS 頻道應加上標籤](#)
- [【Keyspaces.1】Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【KMS.1】IAM 客戶受管政策不應允許對所有 KMS 金鑰執行解密動作](#)
- [【KMS.2】IAM 主體不應具有允許對所有 KMS 金鑰執行解密動作的 IAM 內嵌政策](#)
- [【Lambda.7】Lambda 函數應該啟用 AWS X-Ray 主動追蹤](#)
- [【Macie.1】應啟用 Amazon Macie](#)
- [【Macie.2】應啟用 Macie 自動化敏感資料探索](#)
- [【MSK.3】MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.4】MSK 叢集應停用公有存取](#)
- [【MSK.5】MSK 連接器應該已啟用記錄](#)
- [【MSK.6】MSK 叢集應停用未驗證的存取](#)

- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【Opensearch.9】 應標記 OpenSearch 網域](#)
- [【Opensearch.10】 OpenSearch 網域應已安裝最新的軟體更新](#)
- [【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【Redshift.18】 Redshift 叢集應啟用異地同步備份部署](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.9】 SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】 SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】 SageMaker 資料品質任務定義應該啟用網路隔離](#)

- [【SageMaker.12】 SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】 SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】 SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】 SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】 SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.17】 SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.18】 使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.19】 SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.1】 SES 聯絡人清單應加上標籤](#)
- [【SES.2】 SES 組態集應加上標籤](#)
- [【SES.3】 SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【SQS.1】 Amazon SQS 佇列應靜態加密](#)
- [【SQS.2】 SQS 佇列應加上標籤](#)
- [【SQS.3】 SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.6】 SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【SSM.7】 SSM 文件應啟用封鎖公開共用設定](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

南美洲 (聖保羅)

南美洲 (聖保羅) 區域不支援下列控制項。

- [【AppRunner.1】 App Runner 服務應加上標籤](#)

- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】應標記 CloudFront 分佈](#)
- [【CloudFront.15】CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeGuruProfiler.1】應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.5】應為 Cognito 使用者集區啟用 MFA](#)
- [【Connect.1】Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】Connect Customer 執行個體應啟用 CloudWatch 記錄](#)

- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【IAM.26】 應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoT.1】 AWS IoT Device Defender 安全設定檔應加上標籤](#)
- [【IoT.2】 AWS IoT Core 應標記緩解動作](#)
- [【IoT.3】 AWS IoT Core 維度應加上標籤](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)

- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)

AWS GovCloud (美國東部)

AWS GovCloud (美國東部) 區域不支援下列控制項。

- [【ACM.2】 由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)
- [【Account.1】 應針對 提供安全性聯絡資訊 AWS 帳戶](#)
- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.2】 API Gateway REST API 階段應設定為使用 SSL 憑證進行後端身分驗證](#)
- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)
- [【APIGateway.10】 API Gateway V2 整合應使用 HTTPS 進行私有連線](#)
- [【APIGateway.11】 API Gateway 網域名稱應使用建議的安全政策](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppConfig.1】 AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】 AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】 AWS AppConfig 環境應加上標籤](#)
- [【AppConfig.4】 AWS AppConfig 應標記延伸關聯](#)
- [【AppFlow.1】 Amazon AppFlow 流程應加上標籤](#)

- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.2】AWS AppSync 應該啟用欄位層級記錄](#)
- [【AppSync.4】AWS AppSync GraphQL APIs應加上標籤](#)
- [【AppSync.5】AWS AppSync GraphQL APIs不應使用 API 金鑰進行身分驗證](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【AutoScaling.2】Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域](#)
- [【AutoScaling.3】Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【AutoScaling.6】Auto Scaling 群組應在多個可用區域中使用多個執行個體類型](#)
- [【AutoScaling.9】Amazon EC2 Auto Scaling 群組應使用 Amazon EC2 啟動範本](#)
- [【Backup.4】應標記 AWS Backup 報告計劃](#)
- [【Batch.1】批次任務佇列應加上標籤](#)
- [【Batch.2】批次排程政策應加上標籤](#)
- [【Batch.3】批次運算環境應加上標籤](#)
- [【Batch.4】應標記受管批次運算環境中的運算資源屬性](#)
- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)
- [【CloudFront.6】CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)

- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudWatch.17】 應啟用 CloudWatch 警示動作](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeBuild.3】 CodeBuild S3 日誌應加密](#)
- [【CodeBuild.4】 CodeBuild AWS Config專案環境應具有記錄 URL](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】 Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.2】 Cognito 身分集區不應允許未驗證的身分](#)
- [【Cognito.3】 Cognito 使用者集區的密碼政策應具有強大的組態](#)
- [【Cognito.4】 Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證](#)
- [【Cognito.5】 應為 Cognito 使用者集區啟用 MFA](#)
- [【Cognito.6】 Cognito 使用者集區應啟用刪除保護](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄](#)
- [【DataSync.2】 應標記 DataSync 任務](#)
- [【DMS.2】 DMS 憑證應加上標籤](#)
- [【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)

- [【DMS.9】 DMS 端點應使用 SSL](#)
- [【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】 Amazon EC2 啟動範本不應將公IPs 指派給網路介面](#)
- [【EC2.47】 Amazon VPC 端點服務應加上標籤](#)
- [【EC2.52】 EC2 傳輸閘道應加上標籤](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.174】 EC2 DHCP 選項集應加上標籤](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.176】 EC2 字首清單應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.178】 應標記 EC2 流量鏡像篩選條件](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)
- [【ECR.2】 ECR 私有儲存庫應設定標籤不可變性](#)
- [【ECR.3】 ECR 儲存庫應至少設定一個生命週期政策](#)

- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)
- [【ECS.3】 ECS 任務定義不應共用主機的程序命名空間](#)
- [【ECS.4】 ECS 容器應以非特殊權限執行](#)
- [【ECS.5】 ECS 任務定義應將容器設定為僅限對根檔案系統的唯一讀存取](#)
- [【ECS.8】 不應將秘密做為容器環境變數傳遞](#)
- [【ECS.9】 ECS 任務定義應具有記錄組態](#)
- [【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行](#)
- [【ECS.12】 ECS 叢集應使用 Container Insights](#)
- [【EFS.3】 EFS 存取點應強制執行根目錄](#)
- [【EFS.4】 EFS 存取點應強制執行使用者身分](#)
- [【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)
- [【EKS.8】 EKS 叢集應該啟用稽核記錄](#)
- [【ELB.10】 Classic Load Balancer 應跨越多個可用區域](#)
- [【ELB.12】 Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.13】 應用程式、網路和閘道負載平衡器應跨越多個可用區域](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.21】 應用程式和 Network Load Balancer 目標群組應使用加密的運作狀態檢查通訊協定](#)
- [【ELB.22】 ELB 目標群組應使用加密傳輸通訊協定](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.2】 ElastiCache 叢集應該啟用自動次要版本升級](#)
- [【ElastiCache.3】 ElastiCache 複寫群組應該啟用自動容錯移轉](#)
- [【ElastiCache.4】 ElastiCache 複寫群組應靜態加密](#)
- [【ElastiCache.5】 ElastiCache 複寫群組應在傳輸中加密](#)
- [【ElastiCache.6】 舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】 ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)

- [【EMR.2】應啟用 Amazon EMR 封鎖公開存取設定](#)
- [【EMR.3】Amazon EMR 安全組態應靜態加密](#)
- [【EMR.4】Amazon EMR 安全組態應在傳輸中加密](#)
- [【ES.4】應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【EventBridge.3】EventBridge 自訂事件匯流排應連接以資源為基礎的政策](#)
- [【EventBridge.4】EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.1】FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)
- [【FSx.2】FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)
- [【GlobalAccelerator.1】應標記 Global Accelerator 加速器](#)
- [【Glue.3】AWS Glue 機器學習轉換應該靜態加密](#)
- [【GuardDuty.7】應啟用 GuardDuty EKS 執行期監控](#)
- [【GuardDuty.8】應啟用 EC2 的 GuardDuty 惡意軟體防護](#)
- [【GuardDuty.9】應啟用 GuardDuty RDS 保護](#)
- [【GuardDuty.11】應啟用 GuardDuty 執行期監控](#)
- [【GuardDuty.12】應啟用 GuardDuty ECS 執行期監控](#)
- [【GuardDuty.13】應啟用 GuardDuty EC2 執行期監控](#)
- [【IAM.6】應為根使用者啟用硬體 MFA](#)
- [【IAM.9】應為根使用者啟用 MFA](#)
- [【IAM.21】您建立的 IAM 客戶受管政策不應允許服務的萬用字元動作](#)
- [【IAM.24】IAM 角色應加上標籤](#)
- [【IAM.25】IAM 使用者應加上標籤](#)
- [【IAM.26】應移除在 IAM 中管理的過期 SSL/TLS 憑證](#)
- [【IAM.28】應啟用 IAM Access Analyzer 外部存取分析器](#)
- [【Inspector.3】應啟用 Amazon Inspector Lambda 程式碼掃描](#)

- [【IoTEvents.1】AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】AWS IoT SiteWise 儀表板應加上標籤](#)
- [【IoTSiteWise.3】AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtTwinMaker.1】AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtTwinMaker.2】AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtTwinMaker.3】AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtTwinMaker.4】AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】IVS 記錄組態應加上標籤](#)
- [【IVS.3】IVS 頻道應加上標籤](#)
- [【Keyspaces.1】Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Kinesis.1】Kinesis 串流應靜態加密](#)
- [【KMS.5】不應公開存取 KMS 金鑰](#)
- [【Lambda.5】VPC Lambda 函數應該在多個可用區域中操作](#)
- [【Macie.1】應啟用 Amazon Macie](#)
- [【Macie.2】應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.5】ActiveMQ 代理程式應使用作用中/待命部署模式](#)
- [【MQ.6】RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.1】MSK 叢集應在代理程式節點之間傳輸時加密](#)
- [【MSK.2】MSK 叢集應已設定增強型監控](#)
- [【MSK.3】MSK Connect 連接器應在傳輸中加密](#)

- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)
- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【NetworkFirewall.1】 網路防火牆防火牆應部署在多個可用區域](#)
- [【NetworkFirewall.2】 應啟用網路防火牆記錄](#)
- [【NetworkFirewall.3】 網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.4】 Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)
- [【NetworkFirewall.5】 網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】 無狀態網路防火牆規則群組不應為空](#)
- [【NetworkFirewall.9】 網路防火牆防火牆應啟用刪除保護](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【PCA.1】 應停用 AWS 私有 CA 根憑證授權單位](#)
- [【PCA.2】 應標記 AWS 私有 CA 憑證授權單位](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.15】 應為多個可用區域設定 RDS 資料庫叢集](#)

- [【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱](#)
- [【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)
- [【RDS.27】 RDS 資料庫叢集應靜態加密](#)
- [【RDS.31】 RDS 資料庫安全群組應加上標籤](#)
- [【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)
- [【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密](#)
- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【RDS.47】 RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.48】 RDS for MySQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.50】 RDS 資料庫叢集應設定足夠的備份保留期間](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.17】 應標記 Redshift 叢集參數群組](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.10】 已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態](#)
- [【S3.11】 S3 一般用途儲存貯體應啟用事件通知](#)
- [【S3.12】 ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取](#)
- [【S3.13】 S3 一般用途儲存貯體應具有生命週期組態](#)
- [【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.1】 Amazon SageMaker 筆記本執行個體不應具有直接網際網路存取](#)

- [【SageMaker.2】應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.5】SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】應標記 SageMaker 應用程式映像組態](#)
- [【SageMaker.7】應標記 SageMaker 映像](#)
- [【SageMaker.9】SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.16】SageMaker 模型應將 VPC 中的私有登錄檔用於主要容器](#)
- [【SageMaker.17】SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.18】使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.19】SageMaker 模型應該在 VPC 中使用私有登錄檔進行多容器推論管道](#)
- [【SES.1】SES 聯絡人清單應加上標籤](#)
- [【SES.2】SES 組態集應加上標籤](#)
- [【SES.3】SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【SNS.4】SNS 主題存取政策不應允許公開存取](#)
- [【SQS.3】SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.4】SSM 文件不應公開](#)
- [【SSM.5】SSM 文件應加上標籤](#)
- [【SSM.6】SSM Automation 應該啟用 CloudWatch 記錄](#)
- [【StepFunctions.1】Step Functions 狀態機器應該已開啟記錄](#)
- [【StepFunctions.2】應標記 Step Functions 活動](#)
- [【Transfer.4】Transfer Family 協議應加上標籤](#)
- [【Transfer.5】Transfer Family 憑證應加上標籤](#)
- [【Transfer.6】Transfer Family 連接器應加上標籤](#)

- [【Transfer.7】 轉移系列設定檔應加上標籤](#)
- [【WAF.1】 應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.2】 AWS WAF 傳統區域規則應至少有一個條件](#)
- [【WAF.3】 AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.4】 AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.6】 AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】 AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】 AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】 AWS WAF Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.12】 AWS WAF 規則應啟用 CloudWatch 指標](#)
- [【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區](#)
- [【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密](#)

AWS GovCloud (美國西部)

AWS GovCloud (美國西部) 區域不支援下列控制項。

- [【ACM.2】 由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度](#)
- [【Account.1】 應針對 提供安全性聯絡資訊 AWS 帳戶](#)
- [【Account.2】 AWS 帳戶 應該是 AWS Organizations 組織的一部分](#)
- [【APIGateway.2】 API Gateway REST API 階段應設定為使用 SSL 憑證進行後端身分驗證](#)
- [【APIGateway.8】 API Gateway 路由應指定授權類型](#)
- [【APIGateway.9】 應為 API Gateway V2 階段設定存取記錄](#)
- [【APIGateway.10】 API Gateway V2 整合應使用 HTTPS 進行私有連線](#)
- [【APIGateway.11】 API Gateway 網域名稱應使用建議的安全政策](#)
- [【Amplify.1】 Amplify 應用程式應加上標籤](#)
- [【Amplify.2】 Amplify 分支應加上標籤](#)
- [【AppConfig.1】 AWS AppConfig 應用程式應加上標籤](#)
- [【AppConfig.2】 AWS AppConfig 組態設定檔應加上標籤](#)
- [【AppConfig.3】 AWS AppConfig 環境應加上標籤](#)

- [【AppConfig.4】AWS AppConfig 應標記延伸關聯](#)
- [【AppFlow.1】Amazon AppFlow 流程應加上標籤](#)
- [【AppRunner.1】App Runner 服務應加上標籤](#)
- [【AppRunner.2】應標記 App Runner VPC 連接器](#)
- [【AppSync.1】AWS AppSync API 快取應靜態加密](#)
- [【AppSync.2】AWS AppSync 應該啟用欄位層級記錄](#)
- [【AppSync.4】AWS AppSync GraphQL APIs應加上標籤](#)
- [【AppSync.5】AWS AppSync GraphQL APIs不應使用 API 金鑰進行身分驗證](#)
- [【AppSync.6】AWS AppSync API 快取應在傳輸中加密](#)
- [【AutoScaling.2】Amazon EC2 Auto Scaling 群組應涵蓋多個可用區域](#)
- [【AutoScaling.3】Auto Scaling 群組啟動組態應將 EC2 執行個體設定為需要執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【AutoScaling.6】Auto Scaling 群組應在多個可用區域中使用多個執行個體類型](#)
- [【AutoScaling.9】Amazon EC2 Auto Scaling 群組應使用 Amazon EC2 啟動範本](#)
- [【Backup.4】應標記 AWS Backup 報告計劃](#)
- [【Batch.1】批次任務佇列應加上標籤](#)
- [【Batch.2】批次排程政策應加上標籤](#)
- [【Batch.3】批次運算環境應加上標籤](#)
- [【Batch.4】應標記受管批次運算環境中的運算資源屬性](#)
- [【BedrockAgentCore.1】Bedrock AgentCore 執行時間應使用 VPC 網路模式設定](#)
- [【BedrockAgentCore.2】Bedrock AgentCore Gateways 需要傳入請求的授權](#)
- [【BedrockAgentCore.3】Bedrock AgentCore 記憶體應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.4】Bedrock AgentCore Gateway 應使用客戶受管 AWS KMS 金鑰加密](#)
- [【BedrockAgentCore.5】Bedrock AgentCore 自訂瀏覽器不應使用公有網路模式](#)
- [【BedrockAgentCore.6】Bedrock AgentCore 自訂瀏覽器應啟用工作階段記錄](#)
- [【CloudFront.1】CloudFront 分佈應設定預設根物件](#)
- [【CloudFront.3】CloudFront 分佈應要求傳輸中加密](#)
- [【CloudFront.4】CloudFront 分佈應設定原始伺服器容錯移轉](#)
- [【CloudFront.5】CloudFront 分佈應該已啟用記錄](#)

- [【CloudFront.6】 CloudFront 分佈應該啟用 WAF](#)
- [【CloudFront.7】 CloudFront 分佈應使用自訂 SSL/TLS 憑證](#)
- [【CloudFront.8】 CloudFront 分佈應使用 SNI 來提供 HTTPS 請求](#)
- [【CloudFront.9】 CloudFront 分佈應該加密流量到自訂原始伺服器](#)
- [【CloudFront.10】 CloudFront 分佈不應在節點和自訂原始伺服器之間使用已取代的 SSL 通訊協定](#)
- [【CloudFront.12】 CloudFront 分佈不應指向不存在的 S3 原始伺服器](#)
- [【CloudFront.13】 CloudFront 分佈應使用原始存取控制](#)
- [【CloudFront.14】 應標記 CloudFront 分佈](#)
- [【CloudFront.15】 CloudFront 分佈應使用建議的 TLS 安全政策](#)
- [【CloudFront.16】 CloudFront 分佈應使用 Lambda 函數 URL 原始伺服器的原始存取控制](#)
- [【CloudFront.17】 CloudFront 分佈應針對簽章URLs 和 Cookie 使用信任的金鑰群組](#)
- [【CloudWatch.17】 應啟用 CloudWatch 警示動作](#)
- [【CodeArtifact.1】CodeArtifact 儲存庫應加上標籤](#)
- [【CodeBuild.3】 CodeBuild S3 日誌應加密](#)
- [【CodeBuild.4】 CodeBuild AWS Config專案環境應具有記錄 URL](#)
- [【CodeGuruProfiler.1】 應標記 CodeGuru Profiler 分析群組](#)
- [【CodeGuruReviewer.1】 應標記 CodeGuru Reviewer 儲存庫關聯](#)
- [【Cognito.1】 Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護](#)
- [【Cognito.3】 Cognito 使用者集區的密碼政策應具有強大的組態](#)
- [【Cognito.4】 Cognito 使用者集區應使用完整功能強制執行模式啟用威脅防護，以進行自訂身分驗證](#)
- [【Cognito.5】 應為 Cognito 使用者集區啟用 MFA](#)
- [【Cognito.6】 Cognito 使用者集區應啟用刪除保護](#)
- [【Connect.1】 Amazon Connect Customer Profiles 物件類型應加上標籤](#)
- [【DataSync.2】 應標記 DataSync 任務](#)
- [【DMS.2】 DMS 憑證應加上標籤](#)
- [【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級](#)
- [【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄](#)
- [【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄](#)

- [【DMS.9】 DMS 端點應使用 SSL](#)
- [【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密](#)
- [【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期](#)
- [【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開](#)
- [【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【DocumentDB.5】 Amazon DocumentDB 叢集應該啟用刪除保護](#)
- [【DynamoDB.3】 DynamoDB Accelerator \(DAX\) 叢集應靜態加密](#)
- [【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密](#)
- [【EC2.21】 網路 ACLs 不應允許從 0.0.0.0/0 傳入連接埠 22 或連接埠 3389](#)
- [【EC2.22】 應移除未使用的 Amazon EC2 安全群組](#)
- [【EC2.23】 Amazon EC2 Transit Gateways 不應自動接受 VPC 連接請求](#)
- [【EC2.24】 不應使用 Amazon EC2 全虛擬化執行個體類型](#)
- [【EC2.25】 Amazon EC2 啟動範本不應將公IPs 指派給網路介面](#)
- [【EC2.28】 備份計畫應涵蓋 EBS 磁碟區](#)
- [【EC2.38】 應標記 EC2 執行個體](#)
- [【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定](#)
- [【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定](#)
- [【EC2.170】 EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)](#)
- [【EC2.173】 具有啟動參數的 EC2 Spot 機群請求應啟用已連接 EBS 磁碟區的加密](#)
- [【EC2.174】 EC2 DHCP 選項集應加上標籤](#)
- [【EC2.175】 EC2 啟動範本應加上標籤](#)
- [【EC2.176】 EC2 字首清單應加上標籤](#)
- [【EC2.177】 應標記 EC2 流量鏡像工作階段](#)
- [【EC2.178】 應標記 EC2 流量鏡像篩選條件](#)
- [【EC2.179】 應標記 EC2 流量鏡像目標](#)
- [【ECR.1】 ECR 私有儲存庫應設定映像掃描](#)
- [【ECR.2】 ECR 私有儲存庫應設定標籤不可變性](#)
- [【ECR.3】 ECR 儲存庫應至少設定一個生命週期政策](#)
- [【ECR.4】 ECR 公有儲存庫應加上標籤](#)

- [【ECS.3】 ECS 任務定義不應共用主機的程序命名空間](#)
- [【ECS.4】 ECS 容器應以非特殊權限執行](#)
- [【ECS.5】 ECS 任務定義應將容器設定為僅限對根檔案系統的唯一讀存取](#)
- [【ECS.8】 不應將秘密做為容器環境變數傳遞](#)
- [【ECS.9】 ECS 任務定義應具有記錄組態](#)
- [【ECS.10】 ECS Fargate 服務應在最新的 Fargate 平台版本上執行](#)
- [【ECS.12】 ECS 叢集應使用 Container Insights](#)
- [【EFS.3】 EFS 存取點應強制執行根目錄](#)
- [【EFS.4】 EFS 存取點應強制執行使用者身分](#)
- [【EKS.2】 EKS 叢集應在支援的 Kubernetes 版本上執行](#)
- [【EKS.8】 EKS 叢集應該啟用稽核記錄](#)
- [【ELB.10】 Classic Load Balancer 應跨越多個可用區域](#)
- [【ELB.12】 Application Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.13】 應用程式、網路和閘道負載平衡器應跨越多個可用區域](#)
- [【ELB.14】 Classic Load Balancer 應設定為防禦性或最嚴格的非同步緩解模式](#)
- [【ELB.21】 應用程式和 Network Load Balancer 目標群組應使用加密的運作狀態檢查通訊協定](#)
- [【ELB.22】 ELB 目標群組應使用加密傳輸通訊協定](#)
- [【ElastiCache.1】 ElastiCache \(Redis OSS\) 叢集應該啟用自動備份](#)
- [【ElastiCache.2】 ElastiCache 叢集應該啟用自動次要版本升級](#)
- [【ElastiCache.3】 ElastiCache 複寫群組應該啟用自動容錯移轉](#)
- [【ElastiCache.4】 ElastiCache 複寫群組應靜態加密](#)
- [【ElastiCache.5】 ElastiCache 複寫群組應在傳輸中加密](#)
- [【ElastiCache.6】 舊版的 ElastiCache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH](#)
- [【ElastiCache.7】 ElastiCache 叢集不應使用預設子網路群組](#)
- [【ElasticBeanstalk.1】 Elastic Beanstalk 環境應啟用增強型運作狀態報告](#)
- [【ElasticBeanstalk.2】 應啟用 Elastic Beanstalk 受管平台更新](#)
- [【ElasticBeanstalk.3】 Elastic Beanstalk 應將日誌串流至 CloudWatch](#)
- [【EMR.2】 應啟用 Amazon EMR 封鎖公開存取設定](#)
- [【EMR.3】 Amazon EMR 安全組態應靜態加密](#)

- [【EMR.4】 Amazon EMR 安全組態應在傳輸中加密](#)
- [【ES.4】 應啟用記錄至 CloudWatch Logs 的 Elasticsearch 網域錯誤](#)
- [【EventBridge.3】 EventBridge 自訂事件匯流排應連接以資源為基礎的政策](#)
- [【EventBridge.4】 EventBridge 全域端點應啟用事件複寫](#)
- [【FraudDetector.1】 Amazon Fraud Detector 實體類型應加上標籤](#)
- [【FraudDetector.2】 Amazon Fraud Detector 標籤應加上標籤](#)
- [【FraudDetector.3】 Amazon Fraud Detector 結果應加上標籤](#)
- [【FraudDetector.4】 Amazon Fraud Detector 變數應加上標籤](#)
- [【FSx.1】 FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區](#)
- [【FSx.2】 FSx for Lustre 檔案系統應設定為將標籤複製到備份](#)
- [【GlobalAccelerator.1】 應標記 Global Accelerator 加速器](#)
- [【GuardDuty.7】 應啟用 GuardDuty EKS 執行期監控](#)
- [【GuardDuty.8】 應啟用 EC2 的 GuardDuty 惡意軟體防護](#)
- [【GuardDuty.9】 應啟用 GuardDuty RDS 保護](#)
- [【GuardDuty.11】 應啟用 GuardDuty 執行期監控](#)
- [【GuardDuty.12】 應啟用 GuardDuty ECS 執行期監控](#)
- [【GuardDuty.13】 應啟用 GuardDuty EC2 執行期監控](#)
- [【IAM.6】 應為根使用者啟用硬體 MFA](#)
- [【IAM.9】 應為根使用者啟用 MFA](#)
- [【IAM.21】 您建立的 IAM 客戶受管政策不應允許 服務的萬用字元動作](#)
- [【IAM.24】 IAM 角色應加上標籤](#)
- [【IAM.25】 IAM 使用者應加上標籤](#)
- [【IAM.28】 應啟用 IAM Access Analyzer 外部存取分析器](#)
- [【Inspector.3】 應啟用 Amazon Inspector Lambda 程式碼掃描](#)
- [【IoTEvents.1】 AWS IoT Events 輸入應加上標籤](#)
- [【IoTEvents.2】 AWS IoT Events 偵測器模型應加上標籤](#)
- [【IoTEvents.3】 AWS IoT Events 警示模型應加上標籤](#)
- [【IoTSiteWise.1】 AWS IoT SiteWise 資產模型應加上標籤](#)
- [【IoTSiteWise.2】 AWS IoT SiteWise 儀表板應加上標籤](#)

- [【IoTSiteWise.3】 AWS IoT SiteWise 閘道應加上標籤](#)
- [【IoTSiteWise.4】 AWS IoT SiteWise 入口網站應加上標籤](#)
- [【IoTSiteWise.5】 AWS IoT SiteWise 專案應加上標籤](#)
- [【IoTtwinmaker.1】 AWS 應標記 IoT TwinMaker 同步任務](#)
- [【IoTtwinmaker.2】 AWS IoT TwinMaker 工作區應加上標籤](#)
- [【IoTtwinmaker.3】 AWS IoT TwinMaker 場景應加上標籤](#)
- [【IoTtwinmaker.4】 AWS IoT TwinMaker 實體應加上標籤](#)
- [【IoTWireless.1】 AWS IoT Wireless 多點傳送群組應加上標籤](#)
- [【IoTWireless.2】 AWS IoT Wireless 服務設定檔應加上標籤](#)
- [【IoTWireless.3】 AWS IoT FUOTA 任務應加上標籤](#)
- [【IVS.1】 IVS 播放金鑰對應加上標籤](#)
- [【IVS.2】 IVS 記錄組態應加上標籤](#)
- [【IVS.3】 IVS 頻道應加上標籤](#)
- [【Keyspaces.1】 Amazon Keyspaces 金鑰空間應加上標籤](#)
- [【Kinesis.1】 Kinesis 串流應靜態加密](#)
- [【KMS.5】 不應公開存取 KMS 金鑰](#)
- [【Lambda.5】 VPC Lambda 函數應該在多個可用區域中操作](#)
- [【Macie.1】 應啟用 Amazon Macie](#)
- [【Macie.2】 應啟用 Macie 自動化敏感資料探索](#)
- [【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式](#)
- [【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式](#)
- [【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密](#)
- [【MSK.2】 MSK 叢集應已設定增強型監控](#)
- [【MSK.3】 MSK Connect 連接器應在傳輸中加密](#)
- [【MSK.5】 MSK 連接器應該已啟用記錄](#)
- [【Neptune.1】 Neptune 資料庫叢集應靜態加密](#)
- [【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【Neptune.3】 Neptune 資料庫叢集快照不應公開](#)
- [【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護](#)

- [【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份](#)
- [【Neptune.6】 Neptune 資料庫叢集快照應靜態加密](#)
- [【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證](#)
- [【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照](#)
- [【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域](#)
- [【NetworkFirewall.1】 網路防火牆防火牆應部署在多個可用區域](#)
- [【NetworkFirewall.2】 應啟用網路防火牆記錄](#)
- [【NetworkFirewall.3】 網路防火牆政策應至少有一個相關聯的規則群組](#)
- [【NetworkFirewall.4】 Network Firewall 政策的預設無狀態動作應為捨棄或轉送完整封包](#)
- [【NetworkFirewall.5】 網路防火牆政策的預設無狀態動作應為捨棄或轉送分段封包](#)
- [【NetworkFirewall.6】 無狀態網路防火牆規則群組不應為空](#)
- [【NetworkFirewall.9】 網路防火牆防火牆應啟用刪除保護](#)
- [【Opensearch.1】 OpenSearch 網域應該啟用靜態加密](#)
- [【Opensearch.2】 不應公開存取 OpenSearch 網域](#)
- [【Opensearch.3】 OpenSearch 網域應該加密節點之間傳送的資料](#)
- [【Opensearch.4】 應啟用 CloudWatch Logs 的 OpenSearch 網域錯誤記錄](#)
- [【Opensearch.5】 OpenSearch 網域應該啟用稽核記錄](#)
- [【Opensearch.6】 OpenSearch 網域應至少具有三個資料節點](#)
- [【Opensearch.7】 OpenSearch 網域應啟用精細存取控制](#)
- [【Opensearch.8】 應使用最新的 TLS 安全政策加密 OpenSearch 網域的連線](#)
- [【PCA.1】 應停用 AWS 私有 CA 根憑證授權單位](#)
- [【PCA.2】 應標記 AWS 私有 CA 憑證授權單位](#)
- [【RDS.14】 Amazon Aurora 叢集應該已啟用恢復](#)
- [【RDS.15】 應為多個可用區域設定 RDS 資料庫叢集](#)
- [【RDS.24】 RDS 資料庫叢集應使用自訂管理員使用者名稱](#)
- [【RDS.25】 RDS 資料庫執行個體應使用自訂管理員使用者名稱](#)
- [【RDS.27】 RDS 資料庫叢集應靜態加密](#)
- [【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs](#)
- [【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級](#)

- [【RDS.43】 RDS 資料庫代理應該需要連線的 TLS 加密](#)
- [【RDS.45】 Aurora MySQL 資料庫叢集應該啟用稽核記錄](#)
- [【RDS.47】 RDS for PostgreSQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.48】 RDS for MySQL 資料庫叢集應設定為將標籤複製到資料庫快照](#)
- [【RDS.50】 RDS 資料庫叢集應設定足夠的備份保留期間](#)
- [【RDS.51】 RDS 全域叢集應在支援的 Aurora MySQL 版本上執行](#)
- [【Redshift.7】 Redshift 叢集應使用增強型 VPC 路由](#)
- [【Redshift.8】 Amazon Redshift 叢集不應使用預設的 Admin 使用者名稱](#)
- [【Redshift.10】 應靜態加密 Redshift 叢集](#)
- [【Redshift.11】 應標記 Redshift 叢集](#)
- [【Redshift.13】 應標記 Redshift 叢集快照](#)
- [【Redshift.17】 應標記 Redshift 叢集參數群組](#)
- [【RedshiftServerless.1】 Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由](#)
- [【RedshiftServerless.2】 必須使用 SSL 連線到 Redshift Serverless 工作群組](#)
- [【RedshiftServerless.3】 Redshift Serverless 工作群組應禁止公開存取](#)
- [【RedshiftServerless.6】 Redshift Serverless 命名空間應將日誌匯出至 CloudWatch Logs](#)
- [【Route53.1】 應標記 Route 53 運作狀態檢查](#)
- [【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢](#)
- [【S3.10】 已啟用版本控制的 S3 一般用途儲存貯體應該具有生命週期組態](#)
- [【S3.11】 S3 一般用途儲存貯體應啟用事件通知](#)
- [【S3.12】 ACLs 不應用於管理使用者對 S3 一般用途儲存貯體的存取](#)
- [【S3.13】 S3 一般用途儲存貯體應具有生命週期組態](#)
- [【S3.20】 S3 一般用途儲存貯體應啟用 MFA 刪除](#)
- [【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定](#)
- [【S3.25】 S3 目錄儲存貯體應該具有生命週期組態](#)
- [【SageMaker.2】 應在自訂 VPC 中啟動 SageMaker 筆記本執行個體](#)
- [【SageMaker.3】 使用者不應擁有 SageMaker 筆記本執行個體的根存取權](#)
- [【SageMaker.5】 SageMaker 模型應該啟用網路隔離](#)
- [【SageMaker.6】 應標記 SageMaker 應用程式映像組態](#)

- [【SageMaker.7】應標記 SageMaker 映像](#)
- [【SageMaker.9】SageMaker 資料品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.10】SageMaker 模型可解釋性任務定義應啟用容器間流量加密](#)
- [【SageMaker.11】SageMaker 資料品質任務定義應該啟用網路隔離](#)
- [【SageMaker.12】SageMaker 模型偏差任務定義應該啟用網路隔離](#)
- [【SageMaker.13】SageMaker 模型品質任務定義應該啟用容器間流量加密](#)
- [【SageMaker.14】SageMaker 監控排程應該啟用網路隔離](#)
- [【SageMaker.15】SageMaker 模型偏差任務定義應該啟用容器間流量加密](#)
- [【SageMaker.17】SageMaker 功能群組離線存放區應使用 AWS KMS 金鑰加密](#)
- [【SageMaker.18】使用標準儲存的 SageMaker 功能群組線上存放區應使用 AWS KMS 金鑰加密](#)
- [【SES.3】SES 組態集應啟用 TLS 以傳送電子郵件](#)
- [【SNS.4】SNS 主題存取政策不應允許公開存取](#)
- [【SQS.3】SQS 佇列存取政策不應允許公開存取](#)
- [【SSM.4】SSM 文件不應公開](#)
- [【SSM.5】SSM 文件應加上標籤](#)
- [【StepFunctions.1】Step Functions 狀態機器應該已開啟記錄](#)
- [【StepFunctions.2】應標記 Step Functions 活動](#)
- [【Transfer.4】Transfer Family 協議應加上標籤](#)
- [【Transfer.5】Transfer Family 憑證應加上標籤](#)
- [【Transfer.6】Transfer Family 連接器應加上標籤](#)
- [【Transfer.7】轉移系列設定檔應加上標籤](#)
- [【WAF.1】應啟用 AWS WAF 傳統全域 Web ACL 記錄](#)
- [【WAF.2】AWS WAF 傳統區域規則應至少有一個條件](#)
- [【WAF.3】AWS WAF 傳統區域規則群組應至少有一個規則](#)
- [【WAF.4】AWS WAF 傳統區域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.6】AWS WAF 傳統全域規則應至少有一個條件](#)
- [【WAF.7】AWS WAF 傳統全域規則群組應至少有一個規則](#)
- [【WAF.8】AWS WAF 傳統全域 Web ACLs 應至少有一個規則或規則群組](#)
- [【WAF.10】AWS WAF Web ACLs 應至少有一個規則或規則群組](#)

- [【WAF.12】 AWS WAF 規則應啟用 CloudWatch 指標](#)

使用 CloudFormation 建立 Security Hub CSPM 資源

AWS Security Hub CSPM 與 整合 AWS CloudFormation，這項服務可協助您模型化和設定 AWS 資源，以減少建立和管理資源和基礎設施的時間。您可以建立範本來描述您想要的所有 AWS 資源（例如自動化規則），並為您 CloudFormation 佈建和設定這些資源。

使用 時 CloudFormation，您可以重複使用範本來一致且重複地設定 Security Hub CSPM 資源。描述您的資源一次，然後在多個 AWS 帳戶 和 區域中逐一佈建相同的資源。

Security Hub CSPM 和 CloudFormation 範本

若要佈建和設定 Security Hub CSPM 和相關服務的資源，您必須了解[CloudFormation 範本](#)的運作方式。範本是 JSON 或 YAML 格式的文字檔案。這些範本說明您要在 CloudFormation 堆疊中佈建的資源。

如果您不熟悉 JSON 或 YAML，您可以使用 CloudFormation 設計工具來協助您開始使用 CloudFormation 範本。如需詳細資訊，請參閱AWS CloudFormation 《使用者指南》中的[什麼是 CloudFormation 設計工具？](#)。

您可以為下列類型的 Security Hub CSPM 資源建立 CloudFormation 範本：

- 啟用 Security Hub CSPM
- 指定組織的委派 Security Hub CSPM 管理員
- 指定您的組織在 Security Hub CSPM 中的設定方式
- 啟用安全標準
- 啟用跨區域彙總
- 建立中央組態政策，並將其與帳戶、組織單位 (OUs) 或根帳戶建立關聯
- 建立自訂洞見
- 建立自動化規則
- 自訂控制參數
- 訂閱第三方產品整合

如需詳細資訊，包括資源的 JSON 和 YAML 範本範例，請參閱AWS CloudFormation 《使用者指南》中的 [AWS Security Hub CSPM 資源類型參考](#)。

進一步了解 CloudFormation

若要進一步了解 CloudFormation，請參閱下列資源：

- [AWS CloudFormation](#)
- [AWS CloudFormation 使用者指南](#)
- [CloudFormation API 參考](#)
- [AWS CloudFormation 命令列界面使用者指南](#)

使用 Amazon SNS 訂閱 Security Hub CSPM 公告

本節提供使用 Amazon Simple Notification Service (Amazon SNS) 訂閱 AWS Security Hub CSPM 公告以接收 Security Hub CSPM 通知的相關資訊。

訂閱後，您會收到下列事件的通知（請注意每個事件 `AnnouncementType` 對應的）：

- `NEW_STANDARDS_CONTROLS` – 已新增 Security Hub CSPM 控制項或標準。
- `RETIRED_STANDARDS_CONTROLS` – 現有的 Security Hub CSPM 控制項或標準已淘汰。

所有 Amazon SNS 所支援格式的通知。您可以在 Security Hub CSPM [AWS 區域 提供的所有](#) 中訂閱 [Security Hub CSPM](#) 公告。

使用者必須具有訂閱 Amazon SNS 主題的 `Subscribe` 許可。您可以使用 Amazon SNS 政策、IAM 政策或兩者來達成此目的。如需詳細資訊，請參閱《[Amazon Simple Notification Service 開發人員指南](#)》中的 [IAM 和 Amazon SNS 政策](#)。

Note

Security Hub CSPM 會將 Security Hub CSPM 服務更新的相關 Amazon SNS 公告傳送至任何訂閱的 AWS 帳戶。若要接收有關 Security Hub CSPM 調查結果的通知，請參閱 [在 Security Hub CSPM 中檢閱問題清單詳細資訊和歷史記錄](#)。

您可以訂閱 Amazon SNS 主題的 Amazon Simple Queue Service (Amazon SQS) 佇列，但必須使用位於相同區域的 Amazon SNS 主題 Amazon Resource Name (ARN)。如需詳細資訊，請參閱《[Amazon Simple Queue Service 開發人員指南](#)》中的訂閱 [Amazon SNS 主題](#) 的佇列。

您也可以使用 AWS Lambda 函數，在接收通知時叫用事件。如需詳細資訊，包括範例函數程式碼，請參閱《AWS Lambda 開發人員指南》中的[教學課程：搭配使用 AWS Lambda 與 Amazon Simple Notification Service](#)。

每個區域的 Amazon SNS 主題 ARNs 如下所示。

AWS 區域	Amazon SNS 主題 ARN
美國東部 (俄亥俄)	arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements
美國東部 (維吉尼亞北部)	arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements
美國西部 (加利佛尼亞北部)	arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements
美國西部 (奧勒岡)	arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements
非洲 (開普敦)	arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements
亞太地區 (香港)	arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements
亞太區域 (海德拉巴)	arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements
亞太地區 (雅加達)	arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements

AWS 區域	Amazon SNS 主題 ARN
亞太地區 (孟買)	arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements
亞太區域 (大阪)	arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements
亞太區域 (首爾)	arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements
亞太區域 (新加坡)	arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements
亞太地區 (雪梨)	arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements
亞太區域 (東京)	arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements
加拿大 (中部)	arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements
中國 (北京)	arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements
中國 (寧夏)	arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements

AWS 區域	Amazon SNS 主題 ARN
歐洲 (法蘭克福)	arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements
歐洲 (愛爾蘭)	arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements
歐洲 (倫敦)	arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements
歐洲 (米蘭)	arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements
Europe (Paris)	arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements
歐洲 (西班牙)	arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements
歐洲 (斯德哥爾摩)	arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements
歐洲 (蘇黎世)	arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements
以色列 (特拉維夫)	arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements

AWS 區域	Amazon SNS 主題 ARN
Middle East (Bahrain)	arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements
中東 (阿拉伯聯合大公國)	arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements
南美洲 (聖保羅)	arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements
AWS GovCloud (美國東部)	arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements
AWS GovCloud (美國西部)	arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements

訊息在[分割區](#)內的區域之間通常相同，因此您可以訂閱每個分割區中的一個區域，以接收影響該分割區中所有區域的公告。與成員帳戶相關聯的公告不會在管理員帳戶中複寫。因此，每個帳戶，包括管理員帳戶，每個公告只會有一個副本。您可以決定要使用哪個帳戶來訂閱 Security Hub CSPM 公告。

如需訂閱 Security Hub CSPM 公告的成本資訊，請參閱 [Amazon SNS 定價](#)。

訂閱 Security Hub CSPM 公告（主控台）

1. 在 <https://console.aws.amazon.com/sns/v3/home> 開啟 Amazon SNS 主控台。
2. 在區域清單中，選擇您要訂閱 Security Hub CSPM 公告的區域。此範例使用 us-west-2 區域。
3. 在導覽窗格中選擇 Subscriptions (訂閱)，然後選擇 Create subscription (建立訂閱)。
4. 在主題 ARN 方塊中輸入主題 ARN。例如 arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements。
5. 針對通訊協定，選擇您希望接收 Security Hub CSPM 公告的方式。如果您選擇電子郵件，請在端點中輸入您要用來接收公告的電子郵件地址。

6. 選擇建立訂閱。
7. 確認訂閱。例如，如果您選擇電子郵件通訊協定，Amazon SNS 會將訂閱確認訊息傳送至您提供的電子郵件。

訂閱 Security Hub CSPM 公告 (AWS CLI)

1. 執行以下命令：

```
aws sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. 確認訂閱。例如，如果您選擇電子郵件通訊協定，Amazon SNS 會將訂閱確認訊息傳送至您提供的電子郵件。

Amazon SNS 訊息格式

下列範例顯示來自 Amazon SNS 的 Security Hub CSPM 公告，說明引進新的安全控制。訊息內容會根據公告類型而有所不同，但所有公告類型的格式都相同。或者，可能會包含提供公告詳細資訊Link的欄位。

範例：新控制項的 Security Hub CSPM 公告（電子郵件通訊協定）

```
{
  "AnnouncementType": "NEW_STANDARDS_CONTROLS",
  "Title": "[New Controls] 36 new Security Hub CSPM controls added to the AWS Foundational Security Best Practices standard",
  "Description": "We have added 36 new controls to the AWS Foundational Security Best Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), CloudFormation (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift (Redshift.9), Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
```

```

Foundational Security Best Practices standard in an account and configured Security
Hub CSPM to automatically enable new controls, these controls are enabled by default.
Availability of controls can vary by Region. "
}

```

範例：新控制項的 Security Hub CSPM 公告（電子郵件 JSON 通訊協定）

```

{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":\"[New
Controls] 36 new Security Hub CSPM controls added to the AWS Foundational Security
Best Practices standard\",\"Description\":\"We have added 36 new controls to the
AWS Foundational Security Best Practices standard. These include controls for
Amazon Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), CloudFormation
(CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud
(Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR)
(ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5,
ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon
Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12,
ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3,
NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7),
Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
(SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
Foundational Security Best Practices standard in an account and configured Security
Hub CSPM to automatically enable new controls, these controls are enabled by default.
Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
    "HTHgNFRYMetCvisulgLm4CVySvK9qCXFPHQDxYl9tuCFQuIrd7Y04m4YFR28XKMgzqrF20YP
+EilipUm2S0TpEEt0TekU5bn74+YmNZfwr4aPFx0vUuQCV0shmHl37hjkilJhCg/t53QQiLFP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLI17gYKslt+jsyd/k+7k0qGm0JRDr7qhE7H
+7vaGRL0ptsQnbW8VmeYnDbahE08FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}

```

停用 Security Hub CSPM

您可以使用 AWS Security Hub CSPM 主控台或 Security Hub API 來停用 Security Hub CSPM。如果您停用 Security Hub CSPM，您可以稍後再次啟用它。

如果您的組織使用中央組態，委派的 Security Hub CSPM 管理員可以建立組態政策，以針對特定帳戶和組織單位 (OUs) 停用 Security Hub CSPM，並為其他人保持啟用 Security Hub CSPM。組態政策會影響主要區域和所有連結的區域。如需詳細資訊，請參閱[了解 Security Hub CSPM 中的中央組態](#)。

如果您停用帳戶的 Security Hub CSPM，會發生下列情況：

- 帳戶的所有 Security Hub CSPM 標準和控制項都會停用。
- Security Hub CSPM 會停止產生、更新和擷取帳戶的調查結果。
- 30 天後，Security Hub CSPM 會永久刪除帳戶的所有現有封存問題清單。無法使用 Security Hub CSPM 復原問題清單。
- 90 天後，Security Hub CSPM 會永久刪除帳戶的所有現有作用中問題清單。無法使用 Security Hub CSPM 復原問題清單。
- 90 天後，Security Hub CSPM 會永久刪除帳戶的所有現有洞見和 Security Hub CSPM 組態設定。資料和設定無法復原。

若要保留現有的問題清單，您可以在停用 Security Hub CSPM 之前，將問題清單匯出至 S3 儲存貯體。您可以搭配 Amazon EventBridge 規則使用自訂動作來執行此操作。如需詳細資訊，請參閱[使用 EventBridge 進行自動回應和修復](#)。

如果您在為帳戶停用 Security Hub CSPM 的 90 天內重新啟用 Security Hub CSPM，您可以重新取得現有作用中問題清單的存取權，以及帳戶的洞見和 Security Hub CSPM 組態設定。如果您在 30 天內重新啟用 Security Hub CSPM，您也可以重新取得帳戶現有封存問題清單的存取權。不過，現有的問題清單可能不準確，因為它們會在您停用 Security Hub CSPM 時反映您 AWS 環境的狀態。此外，當您重新啟用個別標準和控制項時，Security Hub CSPM 最初可能會針對特定 AWS 資源產生重複的問題清單，這取決於您啟用的標準和控制項。基於這些原因，我們建議您執行下列其中一項操作：

- 在您停用 Security Hub CSPM RESOLVED 之前，將所有現有問題清單的工作流程狀態變更為。如需詳細資訊，請參閱[設定問題清單的工作流程狀態](#)。
- 在停用 Security Hub CSPM 之前至少六天停用所有標準。然後，Security Hub CSPM 會盡力封存所有現有的問題清單，通常在三到五天內。如需詳細資訊，請參閱[停用標準](#)。

在下列情況中，您無法停用 Security Hub CSPM：

- 您的帳戶是組織的委派 Security Hub CSPM 管理員帳戶。如果您使用中央組態，則無法關聯停用委派管理員帳戶 Security Hub CSPM 的組態政策。其他帳戶的關聯可以成功，但 Security Hub CSPM 不會將政策套用至委派的管理員帳戶。
- 您的帳戶是透過邀請建立的 Security Hub CSPM 管理員帳戶，而且您擁有成員帳戶。您必須先取消所有成員帳戶的關聯，才能停用 Security Hub CSPM。若要了解作法，請參閱[the section called “取消成員帳戶的關聯”](#)。

成員帳戶的擁有者必須先取消與其管理員帳戶的關聯，才能停用 Security Hub CSPM。對於組織帳戶，只有管理員帳戶可以取消成員帳戶的關聯。如需詳細資訊，請參閱[the section called “取消組織成員帳戶的關聯”](#)。對於手動邀請的帳戶，管理員帳戶或成員帳戶可以取消與該帳戶的關聯。如需詳細資訊，請參閱 [the section called “取消成員帳戶的關聯”](#) 或 [the section called “取消與管理員帳戶的關聯”](#)。如果您使用中央組態，則不需要取消關聯，因為 Security Hub CSPM 管理員可以為特定成員帳戶建立停用 Security Hub CSPM 的政策。

當您停用帳戶的 Security Hub CSPM 時，只會在目前的 中停用 AWS 區域。不過，如果您使用中央組態來停用特定帳戶的 Security Hub CSPM，則會在主要區域和所有連結區域中停用。

若要停用 Security Hub CSPM，請選擇您偏好的方法並遵循步驟。

Security Hub CSPM console

請依照下列步驟，使用主控台停用 Security Hub CSPM。

停用 Security Hub CSPM

1. 在 <https://console.aws.amazon.com/securityhub/> 開啟 AWS Security Hub CSPM 主控台。
2. 在導覽窗格中，於 Settings (設定) 下選擇 General (一般)。
3. 在停用 Security Hub CSPM 區段中，選擇停用 Security Hub CSPM。
4. 出現確認提示時，請選擇停用 Security Hub CSPM。

Security Hub API

若要以程式設計方式停用 Security Hub CSPM，請使用 AWS Security Hub API 的 [DisableSecurityHub](#) 操作。或者，如果您使用的是 AWS CLI，請執行 [disable-security-hub](#) 命令。例如，下列命令會在目前的 中停用 Security Hub CSPM AWS 區域：

```
$ aws securityhub disable-security-hub
```

中的安全性 AWS Security Hub CSPM

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，該架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間共同責任。[共同責任模型](#) 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 – AWS 負責保護在 Cloud AWS 中執行 AWS 服務的基礎設施。AWS 也為您提供可安全使用的服務。在 [AWS 合規計畫](#) 中，第三方稽核員會定期測試並驗證我們的安全功效。若要進一步瞭解適用於 AWS Security Hub CSPM 的合規計畫，請參閱 [合規計畫範圍內的 AWS 服務](#)。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您的公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Security Hub CSPM 時套用共同責任模型。下列主題說明如何設定 Security Hub CSPM 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 Security Hub CSPM 資源。

主題

- [中的資料保護 AWS Security Hub CSPM](#)
- [AWS Security Hub CSPM 的 Identity and Access Management](#)
- [的合規驗證 AWS Security Hub CSPM](#)
- [AWS Security Hub 中的彈性](#)
- [中的基礎設施安全 AWS Security Hub CSPM](#)
- [AWS Security Hub CSPM 和介面 VPC 端點 \(AWS PrivateLink\)](#)

中的資料保護 AWS Security Hub CSPM

AWS [共同責任模型](#) 適用於 中的資料保護 AWS Security Hub CSPM。如此模型所述，AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱 [資料隱私權常見問答集](#)。如需歐洲資料保護的相關資訊，請參閱 [「一般資料保護法規 \(GDPR\) 中心」](#)。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《使用者指南》中的[使用 CloudTrail 追蹤](#)。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱[聯邦資訊處理標準 \(FIPS\) 140-3](#)。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Security Hub CSPM 或使用主控台 AWS CLI、API 或 AWS SDKs 的其他 AWS 服務 時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

Security Hub CSPM 是多租戶服務產品。為了確保資料保護，Security Hub CSPM 會加密靜態資料和元件服務之間傳輸中的資料。

AWS Security Hub CSPM 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證（登入）和授權（具有許可）來使用 Security Hub 資源。IAM 是您可以免費使用 AWS 服務的。

主題

- [目標對象](#)
- [使用身分驗證](#)
- [使用政策管理存取權](#)
- [Security Hub 如何與 IAM 搭配使用](#)
- [的身分型政策範例 AWS Security Hub CSPM](#)
- [的服務連結角色 AWS Security Hub CSPM](#)
- [AWS Security Hub 的 受管政策](#)
- [對 AWS Security Hub CSPM 身分和存取進行故障診斷](#)

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 [對 AWS Security Hub CSPM 身分和存取進行故障診斷](#))
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 [Security Hub 如何與 IAM 搭配使用](#))
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 [的身分型政策範例 AWS Security Hub CSPM](#))

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的[如何登入您的 AWS 帳戶](#)。

對於程式設計存取，AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的[API 請求的AWS 第 4 版簽署程序](#)。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分具有對所有 AWS 服務 和 資源的完整存取權。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的[需要根使用者憑證的任務](#)。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務 使用臨時憑證存取。

聯合身分是您企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務 憑證存取 Directory Service 。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的[什麼是 IAM Identity Center ?](#)。

IAM 使用者和群組

IAM 使用者https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的[要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取](#)。

[IAM 群組](#)會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 使用者的使用案例](#)。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過[從使用者切換到 IAM 角色（主控台）](#)或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的[擔任角色的方法](#)。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的快帳戶資源存取](#)。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS，會評估這些政策。大多數政策會以 JSON 文件 AWS 形式存放在中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的[JSON 政策概觀](#)。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的[透過客戶管理政策定義自訂 IAM 許可](#)。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的[在受管政策與內嵌政策之間選擇](#)。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。您必須在資源型政策中[指定主體](#)。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 實體許可界限](#)。
- 服務控制政策 (SCP) — 為 AWS Organizations 中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[服務控制政策](#)。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的[資源控制政策 \(RCP\)](#)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的[工作階段政策](#)。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的[政策評估邏輯](#)。

Security Hub 如何與 IAM 搭配使用

在您使用 AWS Identity and Access Management (IAM) 來管理對的存取之前 AWS Security Hub CSPM，請先了解哪些 IAM 功能可與 Security Hub CSPM 搭配使用。

您可以搭配使用的 IAM 功能 AWS Security Hub CSPM

IAM 功能	Security Hub CSPM 支援
身分型政策	是
資源型政策	否
政策動作	是

IAM 功能	Security Hub CSPM 支援
政策資源	否
政策條件索引鍵	是
存取控制清單 (ACL)	否
屬性型存取控制 (ABAC) – 政策中的標籤	是
臨時憑證	是
轉送存取工作階段 (FAS)	是
服務角色	否
服務連結角色	是

如需 Security Hub CSPM 和其他 如何與大多數 IAM 功能 AWS 服務 搭配使用的高階檢視，請參閱 [《AWS 服務 IAM 使用者指南》中的 與 IAM 搭配使用](#)。

Security Hub CSPM 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的 [透過客戶管理政策定義自訂 IAM 許可](#)。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素參考](#)。

Security Hub CSPM 支援以身分為基礎的政策。如需詳細資訊，請參閱 [的身分型政策範例 AWS Security Hub CSPM](#)。

Security Hub CSPM 的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源

的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中[指定主體](#)。委託人可以包含帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的[IAM 中的快帳戶資源存取](#)。

Security Hub CSPM 不支援以資源為基礎的政策。您無法將 IAM 政策直接連接至 Security Hub CSPM 資源。

Security Hub CSPM 的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 Action 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

Security Hub CSPM 中的政策動作在動作之前使用下列字首：

```
securityhub:
```

例如，若要授予使用者啟用 Security Hub CSPM 的許可，這是對應至 Security Hub CSPM API `EnableSecurityHub` 操作的動作，請在其政策中包含 `securityhub:EnableSecurityHub` 動作。政策陳述式必須包含 Action 或 NotAction 元素。Security Hub CSPM 定義自己的一組動作，描述您可以使用此服務執行的任務。

```
"Action": "securityhub:EnableSecurityHub"
```

若要在單一陳述式中指定多個動作，請用逗號分隔。例如：

```
"Action": [  
    "securityhub:EnableSecurityHub",  
    "securityhub:BatchEnableStandards"
```

您也可以使用萬用字元 (*) 指定多個動作。例如，若要指定開頭是 Get 文字的所有動作，請包含以下動作：

```
"Action": "securityhub:Get*"
```

但是，根據最佳實務，您應該定義遵循「最低權限」原則的政策。換句話說，您應建立其中只包含執行特定任務所需許可的政策。

使用者必須能夠存取 DescribeStandardsControl 操作，才能存取 BatchGetSecurityControls、BatchGetStandardsControlAssociations 和 ListStandardsControlAssociations。

使用者必須能夠存取 UpdateStandardsControls 操作，才能存取 BatchUpdateStandardsControlAssociations、和 UpdateSecurityControl。

如需 Security Hub CSPM 動作的清單，請參閱《服務授權參考》中的 [定義的動作 AWS Security Hub CSPM](#)。如需指定 Security Hub CSPM 動作的政策範例，請參閱 [的身分型政策範例 AWS Security Hub CSPM](#)。

Security Hub CSPM 的政策資源

支援政策資源：否

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 [Amazon Resource Name \(ARN\)](#) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

```
"Resource": "*"

```

Security Hub CSPM 定義下列資源類型：

- Hub (樞紐)
- 產品
- 尋找彙總工具，也稱為跨區域彙總工具
- 自動化規則
- 組態政策

您可以使用 ARNs 在政策中指定這些類型的資源。

如需 Security Hub CSPM 資源類型和每個類型的 ARN 語法清單，請參閱《服務授權參考》中的 [定義的資源類型 AWS Security Hub CSPM](#)。若要了解您可以為每種資源類型指定哪些動作，請參閱《服務

授權參考》中的 [定義的動作 AWS Security Hub CSPM](#)。如需指定資源的政策範例，請參閱 [的身分型政策範例 AWS Security Hub CSPM](#)。

Security Hub CSPM 的政策條件索引鍵

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用 [條件運算子](#) 的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 [AWS 全域條件內容索引鍵](#)。

如需 Security Hub CSPM 條件金鑰的清單，請參閱《服務授權參考》中的 [的條件金鑰 AWS Security Hub CSPM](#)。若要了解您可搭配哪些動作和資源使用條件索引鍵，請參閱 [定義的動作 AWS Security Hub CSPM](#)。如需使用條件索引鍵的政策範例，請參閱 [的身分型政策範例 AWS Security Hub CSPM](#)。

Security Hub CSPM 中的存取控制清單 (ACLs)

支援 ACL：否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Security Hub CSPM 不支援 ACLs，這表示您無法將 ACL 連接至 Security Hub CSPM 資源。

使用 Security Hub CSPM 的屬性型存取控制 (ABAC)

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的 [條件元素](#) 中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的 [使用 ABAC 授權定義許可](#)。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的 [使用屬性型存取控制 \(ABAC\)](#)。

您可以將標籤連接至 Security Hub CSPM 資源。您也可以政策的 Condition 元素中提供標籤資訊，以控制對資源的存取。

如需標記 Security Hub CSPM 資源的資訊，請參閱 [標記 Security Hub 資源](#)。如需根據標籤控制資源存取的身分型政策範例，請參閱 [的身分型政策範例 AWS Security Hub CSPM](#)。

搭配 Security Hub CSPM 使用臨時憑證

支援臨時憑證：是

臨時登入資料提供對 AWS 資源的短期存取，並在您使用聯合或切換角色時自動建立。AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM 中的臨時安全憑證與可與 IAM 搭配運作的 AWS 服務](#)。

您可以搭配聯合使用暫時憑證、擔任 IAM 角色，或是擔任跨帳戶角色。您可以透過呼叫 [AssumeRole](#) 或 [GetFederationToken](#) 等 AWS STS API 操作來取得臨時安全登入資料。

Security Hub CSPM 支援使用臨時登入資料。

轉送 Security Hub CSPM 的存取工作階段

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫的委託人許可 AWS 服務，並結合 AWS 服務請求向下游服務提出請求。如需提出 FAS 請求時的政策詳細資訊，請參閱 [轉發存取工作階段](#)。

例如，AWS 服務當您將 Security Hub CSPM 與整合時 AWS Organizations，以及當您為 Organizations 中的組織指定委派 Security Hub CSPM 管理員帳戶時，Security Hub CSPM 會向下游發出 FAS 請求。

對於其他任務，Security Hub CSPM 使用服務連結角色代表您執行動作。如需此角色的詳細資訊，請參閱 [的服務連結角色 AWS Security Hub CSPM](#)。

Security Hub CSPM 的服務角色

Security Hub CSPM 不會擔任或使用服務角色。若要代表您執行動作，Security Hub CSPM 會使用服務連結角色。如需此角色的詳細資訊，請參閱 [的服務連結角色 AWS Security Hub CSPM](#)。

Warning

變更服務角色的許可可能會在您使用 Security Hub CSPM 時產生操作問題。只有在 Security Hub CSPM 提供指引時，才能編輯服務角色。

Security Hub CSPM 的服務連結角色

支援服務連結角色：是

服務連結角色是連結至的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

Security Hub CSPM 使用服務連結角色代表您執行動作。如需此角色的詳細資訊，請參閱 [的服務連結角色 AWS Security Hub CSPM](#)。

的身分型政策範例 AWS Security Hub CSPM

根據預設，使用者和角色沒有建立或修改 Security Hub CSPM 資源的許可。他們也無法使用 AWS 管理主控台 AWS CLI 或 AWS API 執行任務。管理員必須建立 IAM 政策，授與使用者和角色在指定資源上執行特定 API 操作所需的許可。管理員接著必須將這些政策連接至需要這些許可的使用者或群組。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱 IAM 使用者指南中的 [在 JSON 索引標籤上建立政策](#)。

主題

- [政策最佳實務](#)
- [使用 Security Hub CSPM 主控台](#)
- [範例：允許使用者檢視他們自己的許可](#)
- [範例：允許使用者建立和管理組態政策](#)
- [範例：允許使用者檢視問題清單](#)
- [範例：允許使用者建立和管理自動化規則](#)

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Security Hub 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 [AWS 受管政策](#) 或 [任務職能的 AWS 受管政策](#)。

- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 [IAM 中的政策和許可](#)。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 [IAM JSON 政策元素：條件](#)。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [使用 IAM Access Analyzer 驗證政策](#)。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的 [透過 MFA 的安全 API 存取](#)。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 [IAM 安全最佳實務](#)。

使用 Security Hub CSPM 主控台

若要存取 AWS Security Hub CSPM 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視中 Security Hub CSPM 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

為了確保這些使用者和角色可以使用 Security Hub CSPM 主控台，請將下列 AWS 受管政策連接到實體。如需詳細資訊，請參閱《IAM 使用者指南》中的 [新增許可到使用者](#)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    }
  ]
}
```

```

    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}

```

範例：允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視連接到他們使用者身分的內嵌及受管政策。此政策包含在主控台或使用 或 AWS CLI AWS API 以程式設計方式完成此動作的許可。

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",

```

```

        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

範例：允許使用者建立和管理組態政策

此範例示範如何建立 IAM 政策，允許使用者建立、檢視、更新和刪除組態政策。此範例政策也允許使用者啟動、停止和檢視政策關聯。若要讓此 IAM 政策正常運作，使用者必須是組織的委派 Security Hub CSPM 管理員。

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAndUpdateConfigurationPolicy",
      "Effect": "Allow",
      "Action": [
        "securityhub:CreateConfigurationPolicy",
        "securityhub:UpdateConfigurationPolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ViewConfigurationPolicy",
      "Effect": "Allow",
      "Action": [
        "securityhub:GetConfigurationPolicy",
        "securityhub:ListConfigurationPolicies"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DeleteConfigurationPolicy",
      "Effect": "Allow",

```

```

        "Action": [
            "securityhub:DeleteConfigurationPolicy"
        ],
        "Resource": "*"
    },
    {
        "Sid": "ViewConfigurationPolicyAssociation",
        "Effect": "Allow",
        "Action": [
            "securityhub:BatchGetConfigurationPolicyAssociations",
            "securityhub:GetConfigurationPolicyAssociation",
            "securityhub:ListConfigurationPolicyAssociations"
        ],
        "Resource": "*"
    },
    {
        "Sid": "UpdateConfigurationPolicyAssociation",
        "Effect": "Allow",
        "Action": [
            "securityhub:StartConfigurationPolicyAssociation",
            "securityhub:StartConfigurationPolicyDisassociation"
        ],
        "Resource": "*"
    }
]
}

```

範例：允許使用者檢視問題清單

此範例示範如何建立 IAM 政策，允許使用者檢視 Security Hub CSPM 問題清單。

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],

```

```

        "Resource": "*"
      }
    ]
  }

```

範例：允許使用者建立和管理自動化規則

此範例示範如何建立 IAM 政策，允許使用者建立、檢視、更新和刪除 Security Hub CSPM 自動化規則。若要讓此 IAM 政策正常運作，使用者必須是 Security Hub CSPM 管理員。若要限制許可，例如，只允許使用者檢視自動化規則，您可以移除建立、更新和刪除許可。

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAndUpdateAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:CreateAutomationRule",
        "securityhub:BatchUpdateAutomationRules"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ViewAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchGetAutomationRules",
        "securityhub:ListAutomationRules"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DeleteAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchDeleteAutomationRules"
      ],
      "Resource": "*"
    }
  ]
}

```

```
}  
]  
}
```

的服務連結角色 AWS Security Hub CSPM

AWS Security Hub CSPM 使用名為 `AWSServiceRoleForSecurityHub` 的 AWS Identity and Access Management (IAM) [服務連結角色](#)。此服務連結角色是直接連結至 Security Hub CSPM 的 IAM 角色。它由 Security Hub CSPM 預先定義，並包含 Security Hub CSPM 代表您呼叫其他 AWS 服務和監控 AWS 資源所需的所有許可。Security Hub CSPM 會在提供 AWS 區域 Security Hub CSPM 的所有 `中` 使用此服務連結角色。

服務連結角色可讓您更輕鬆地設定 Security Hub CSPM，因為您不必手動新增必要的許可。Security Hub CSPM 定義其服務連結角色的許可，除非另有定義，否則只有 Security Hub CSPM 可以擔任該角色。定義的許可包括信任政策和許可政策，您無法將該許可政策連接到任何其他 IAM 實體。

若要檢閱服務連結角色的詳細資訊，您可以使用 Security Hub CSPM 主控台。在導覽窗格中，選擇設定下的一般。然後，在服務許可區段中，選擇檢視服務許可。

只有在啟用 Security Hub CSPM 的所有區域中停用 Security Hub CSPM 之後，才能刪除 Security Hub CSPM 服務連結角色。這可保護您的 Security Hub CSPM 資源，因為您不會不小心移除存取這些資源的許可。

如需有關支援服務連結角色的其他服務的資訊，請參閱 [《AWS IAM 使用者指南》中的與 IAM 搭配使用的服務](#)，並在服務連結角色欄中尋找具有是的服務。選擇有連結的是，以檢閱該服務的服務連結角色文件。

主題

- [Security Hub CSPM 的服務連結角色許可](#)
- [為 Security Hub CSPM 建立服務連結角色](#)
- [編輯 Security Hub CSPM 的服務連結角色](#)
- [刪除 Security Hub CSPM 的服務連結角色](#)

Security Hub CSPM 的服務連結角色許可

Security Hub CSPM 使用名為 `AWSServiceRoleForSecurityHub` 的服務連結角色。這是 AWS Security Hub CSPM 存取資源所需的服務連結角色。此服務連結角色可讓 Security Hub CSPM 執行任

務，例如從其他 接收問題清單，AWS 服務 並設定必要的 AWS Config 基礎設施來執行控制項的安全檢查。AWSServiceRoleForSecurityHub 服務連結角色信任 securityhub.amazonaws.com 服務來擔任該角色。

AWSServiceRoleForSecurityHub 服務連結角色使用受管政策

[AWSSecurityHubServiceRolePolicy](#)。

您必須授予許可，以允許 IAM 身分（例如角色、群組或使用者）建立、編輯或刪除服務連結角色。若要成功建立AWSServiceRoleForSecurityHub服務連結角色，您用來存取 Security Hub CSPM 的 IAM 身分必須具有必要的許可。若要授予必要許可，請將下列政策連接至 IAM 身分。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

為 Security Hub CSPM 建立服務連結角色

AWSServiceRoleForSecurityHub 服務連結角色會在您第一次啟用 Security Hub CSPM 時自動建立，或在先前未啟用該角色的區域中啟用 Security Hub CSPM。您也可以使用 IAM 主控台、IAM CLI 或 IAM API 手動建立AWSServiceRoleForSecurityHub服務連結角色。如需有關手動建立角色的詳細資訊，請參閱《IAM 使用者指南》中的[建立服務連結角色](#)。

 Important

為 Security Hub CSPM 管理員帳戶建立的服務連結角色不適用於相關聯的 Security Hub CSPM 成員帳戶。

編輯 Security Hub CSPM 的服務連結角色

Security Hub CSPM 不允許您編輯AWSServiceRoleForSecurityHub服務連結角色。因為可能有各種實體會參考服務連結角色，所以您無法在建立角色之後變更其名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的[編輯服務連結角色](#)。

刪除 Security Hub CSPM 的服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。這樣就不會有未積極監控或維護的未使用實體。

當您停用 Security Hub CSPM 時，Security Hub CSPM 不會自動為您刪除AWSServiceRoleForSecurityHub服務連結角色。如果您再次啟用 Security Hub CSPM，則服務可以再次開始使用現有的服務連結角色。如果您不再需要使用 Security Hub CSPM，您可以手動刪除服務連結角色。

 Important

刪除AWSServiceRoleForSecurityHub服務連結角色之前，您必須先在啟用該角色的所有區域中停用 Security Hub CSPM。如需詳細資訊，請參閱[停用 Security Hub CSPM](#)。如果您在嘗試刪除服務連結角色時未停用 Security Hub CSPM，則刪除會失敗。

若要刪除AWSServiceRoleForSecurityHub服務連結角色，您可以使用 IAM 主控台、IAM CLI 或 IAM API。如需詳細資訊，請參閱《IAM 使用者指南》中的[刪除服務連結角色](#)。

AWS Security Hub 的 受管政策

AWS 受管政策是由 AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住，AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的[客戶管理政策](#)，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新 AWS 受管政策中定義的許可，更新會影響政策連接的所有主體身分（使用者、群組和角色）。AWS 服務當新的啟動或新的 API 操作可供現有服務使用時，AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 [AWS 受管政策](#)。

AWS 受管政策：AWSSecurityHubFullAccess

您可將 AWSSecurityHubFullAccess 政策連接到 IAM 身分。

此政策會授予管理許可，允許委託人完整存取所有 Security Hub CSPM 動作。此政策必須連接到委託人，才能為其帳戶手動啟用 Security Hub CSPM。例如，具有這些許可的主體可以檢視和更新調查結果的狀態。他們也可以設定自訂洞見、啟用整合，以及啟用和停用標準和控制項。管理員帳戶的主體也可以管理成員帳戶。

許可詳細資訊

此政策包含以下許可：

- `securityhub` – 允許主體完整存取所有 Security Hub CSPM 動作。
- `guardduty` – 允許主體在 Amazon GuardDuty 中執行偵測器、組織管理員管理、成員帳戶管理以及全組織組態的完整生命週期管理。這包括 API 動作：`GetDetector`、`ListDetector`、`CreateDetector`、`UpdateDetector`、`DeleteDetector`、`EnableOrganizationAdminAccount`。
- `iam` – 允許主體為 Security Hub CSPM 和 Security Hub 建立服務連結角色，並取得角色、政策和政策版本。
- `inspector` – 允許主體取得帳戶狀態的相關資訊、啟用或停用、委派管理員管理，以及在 Amazon Inspector 中執行組織組態管理。這包括 API 動作：`BatchGetAccountStatus`、`Enable`、`Disable`、`EnableDelegatedAdminAccount`、`DisableDelegatedAdminAccount`。
- `pricing` – 允許主體取得 AWS 服務和產品的價目表。
- `account` – 允許主體取得帳戶區域的相關資訊，以支援 Security Hub 中的區域管理。

若要檢閱此政策的許可，請參閱《AWS 受管政策參考指南[AWSSecurityHubFullAccess](#)》中的。

AWS 受管政策：AWSSecurityHubReadOnlyAccess

您可將 AWSSecurityHubReadOnlyAccess 政策連接到 IAM 身分。

此政策授予唯讀許可，允許使用者檢視 Security Hub CSPM 中的資訊。附加此政策的委託人無法在 Security Hub CSPM 中進行任何更新。例如，具有這些許可的主體可以檢視與其帳戶相關聯的問題清

單，但無法變更問題清單的狀態。他們可以檢視洞見的結果，但無法建立或設定自訂洞見。他們無法設定控制項或產品整合。

許可詳細資訊

此政策包含以下許可：

- `securityhub` – 允許使用者執行傳回項目清單或項目詳細資訊的動作。這包括以 `Get`、`List` 或 開頭的 API 操作 `Describe`。

若要檢閱此政策的許可，請參閱《AWS 受管政策參考指南[AWSSecurityHubReadOnlyAccess](#)》中的。

AWS 受管政策：`AWSSecurityHubOrganizationsAccess`

您可將 `AWSSecurityHubOrganizationsAccess` 政策連接到 IAM 身分。

此政策授予管理許可，以啟用和管理 中組織的 Security Hub、Security Hub CSPM、Amazon GuardDuty 和 Amazon Inspector AWS Organizations。此政策的許可允許組織管理帳戶指定 Security Hub、Security Hub CSPM、Amazon GuardDuty 和 Amazon Inspector 的委派管理員帳戶。它們也允許委派的管理員帳戶將組織帳戶啟用為成員帳戶。

此政策僅提供 的許可 `AWS Organizations`。組織管理帳戶和委派管理員帳戶也需要相關聯動作的許可。您可以使用 `AWSSecurityHubFullAccess` 受管政策授予這些許可。

在管理帳戶中建立或更新委派管理員政策需要此政策中未提供的其他許可。若要執行這些動作，建議新增許可 `organizations:PutResourcePolicy` 或連接 `AWSOrganizationsFullAccess` 政策。

許可詳細資訊

此政策包含以下許可：

- `organizations:ListAccounts` – 允許主體擷取屬於組織一部分的帳戶清單。
- `organizations:DescribeOrganization` – 允許主體擷取組織的相關資訊。
- `organizations:ListRoots` – 允許主體列出組織的根目錄。
- `organizations:ListDelegatedAdministrators` – 允許主體列出組織的委派管理員。
- `organizations:ListAWSServiceAccessForOrganization` – 允許主體列出 AWS 服務 組織 使用的。

- `organizations:ListOrganizationalUnitsForParent` – 允許主體列出父 OU 的子組織單位 (OU)。
- `organizations:ListAccountsForParent` – 允許主體列出父 OU 的子帳戶。
- `organizations:ListParents` – 列出做為指定子 OUs 或帳戶直接父項的根或組織單位 (OU)。
- `organizations:DescribeAccount` – 允許主體擷取組織中帳戶的相關資訊。
- `organizations:DescribeOrganizationalUnit` – 允許主體擷取組織中 OU 的相關資訊。
- `organizations:ListPolicies` – 擷取組織中指定類型的所有政策清單。
- `organizations:ListPoliciesForTarget` – 列出直接連接到指定目標根目錄、組織單位 (OU) 或帳戶的政策。
- `organizations:ListTargetsForPolicy` – 列出指定政策連接的所有根目錄、組織單位 (OUs) 和帳戶。
- `organizations:EnableAWSServiceAccess` – 允許主體啟用與 Organizations 的整合。
- `organizations:RegisterDelegatedAdministrator` – 允許主體指定委派的管理員帳戶。
- `organizations:DeregisterDelegatedAdministrator` – 允許主體移除委派的管理員帳戶。
- `organizations:DescribePolicy` – 擷取政策的相關資訊。
- `organizations:DescribeEffectivePolicy` – 傳回指定政策類型和帳戶的有效政策內容。
- `organizations:CreatePolicy` – 建立可連接至根目錄、組織單位 (OU) 或個別 AWS 帳戶之指定類型的政策。
- `organizations:UpdatePolicy` – 使用新名稱、描述或內容更新現有政策。
- `organizations>DeletePolicy` – 從您的組織刪除指定的政策。
- `organizations:AttachPolicy` – 將政策連接至根帳戶、組織單位 (OU) 或個別帳戶。
- `organizations:DetachPolicy` – 從目標根目錄、組織單位 (OU) 或帳戶分離政策。
- `organizations:EnablePolicyType` – 在根目錄中啟用政策類型。
- `organizations:DisablePolicyType` – 在根目錄中停用組織政策類型。
- `organizations:TagResource` – 將一或多個標籤新增至指定的資源。
- `organizations:UntagResource` – 從指定的資源移除具有指定金鑰的任何標籤。
- `organizations:ListTagsForResource` – 列出連接至指定資源的標籤。
- `organizations:DescribeResourcePolicy` – 擷取資源政策的相關資訊。

若要檢閱此政策的許可，請參閱《AWS 受管政策參考指南[AWS Security Hub Organizations Access](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_aws_security_hub_organizations_access.html)》中的。

AWS 受管政策：AWSSecurityHubServiceRolePolicy

您不得將 AWSSecurityHubServiceRolePolicy 連接到 IAM 實體。此政策會連接到服務連結角色，允許 Security Hub CSPM 代表您執行動作。如需詳細資訊，請參閱[the section called “服務連結角色”](#)。

此政策會授予管理許可，允許服務連結角色執行任務，例如執行 Security Hub CSPM 控制項的安全檢查。

許可詳細資訊

此政策包含以下許可：

- `cloudtrail` – 擷取 CloudTrail 追蹤的相關資訊。
- `cloudwatch` – 擷取目前的 CloudWatch 警示。
- `logs` – 擷取 CloudWatch 日誌的指標篩選條件。
- `sns` – 擷取 SNS 主題的訂閱清單。
- `config` – 擷取組態記錄器、資源和 AWS Config 規則的相關資訊。也允許服務連結角色管理 Security Hub CSPM 服務連結組態記錄器、建立和刪除 AWS Config 規則，並根據規則執行評估。
- `iam` – 擷取和產生帳戶的登入資料報告，並建立的服務連結角色 AWS Config。
- `organizations` – 擷取組織的帳戶和組織單位 (OU) 資訊。
- `securityhub` – 擷取如何設定 Security Hub CSPM 服務、標準和控制項的相關資訊。
- `tag` – 擷取資源標籤的相關資訊。

若要檢閱此政策的許可，請參閱《AWS 受管政策參考指南[AWSSecurityHubServiceRolePolicy](#)》中的。

AWS 受管政策的 Security Hub 更新

下表提供自此服務開始追蹤這些變更以來，AWS Security Hub 和 Security Hub CSPM AWS 受管政策更新的詳細資訊。如需政策更新的自動提醒，請訂閱 [Security Hub 文件歷史記錄](#) 頁面上的 RSS 摘要。

變更	描述	Date
AWSSecurityHubServiceRolePolicy – 更新的政策	Security Hub CSPM 已更新政策，以新增管理 Security Hub	2026 年 4 月 29 日

變更	描述	Date
	CSPM 服務連結組態記錄器和建立 AWS Config 服務連結角色的許可。	
AWSSecurityHubOrganizationsAccess – 更新的政策	Security Hub 已更新政策，新增描述資源政策以支援 Security Hub 功能的許可。Security Hub 處於預覽版本，可能會有所變更。	2025 年 11 月 12 日
AWSSecurityHubFullAccess – 更新的政策	Security Hub 已更新政策，新增管理 GuardDuty、Amazon Inspector 和帳戶管理的功能，以支援 Security Hub 功能。Security Hub 處於預覽版本，可能會有所變更。	2025 年 11 月 17 日
AWSSecurityHubOrganizationsAccess – 更新現有政策	Security Hub 已將新許可新增至政策。許可允許組織管理為組織啟用和管理 Security Hub 和 Security Hub CSPM。	2025 年 6 月 17 日
AWSSecurityHubFullAccess – 更新現有政策	Security Hub CSPM 新增了新的許可，允許主體為 Security Hub 建立服務連結角色。	2025 年 6 月 17 日
AWSSecurityHubFullAccess – 更新現有政策	Security Hub CSPM 已更新政策，以取得 AWS 服務和產品的定價詳細資訊。	2024 年 4 月 24 日
AWSSecurityHubReadOnlyAccess – 更新現有政策	Security Hub CSPM 透過新增Sid欄位來更新此受管政策。	2024 年 2 月 22 日

變更	描述	Date
AWSSecurityHubFullAccess – 更新現有政策	Security Hub CSPM 已更新政策，因此可以判斷帳戶中是否啟用 Amazon GuardDuty 和 Amazon Inspector。這有助於客戶整合來自多個的安全相關資訊 AWS 服務。	2023 年 11 月 16 日
AWSSecurityHubOrganizationsAccess – 更新現有政策	Security Hub CSPM 已更新政策，授予其他許可，以允許對委派管理員功能進行 AWS Organizations 唯讀存取。這包括根目錄、組織單位 (OUs)、帳戶、組織結構和服務存取等詳細資訊。	2023 年 11 月 16 日
AWSSecurityHubServiceRolePolicy – 更新至現有政策	Security Hub CSPM 新增了 BatchGetSecurityControls 、和 UpdateSecurityControl 許可 DisassociateFromAdministratorAccount ，以讀取和更新可自訂的安全控制屬性。	2023 年 11 月 26 日
AWSSecurityHubServiceRolePolicy – 更新至現有政策	Security Hub CSPM 新增了讀取與問題清單相關資源標籤的 tag:GetResources 許可。	2023 年 11 月 7 日
AWSSecurityHubServiceRolePolicy – 更新至現有政策	Security Hub CSPM 新增 BatchGetStandardsControlAssociations 了許可，以取得有關標準中控制項啟用狀態的資訊。	2023 年 9 月 27 日

變更	描述	Date
AWSSecurityHubServiceRolePolicy – 更新至現有政策	Security Hub CSPM 新增了取得 AWS Organizations 資料以及讀取和更新 Security Hub CSPM 組態的新許可，包括標準和控制項。	2023 年 9 月 20 日
AWSSecurityHubServiceRolePolicy – 更新至現有政策	Security Hub CSPM 將現有 config:DescribeConfigRuleEvaluationStatus 許可移至政策中的不同陳述式。config:DescribeConfigRuleEvaluationStatus 許可現在會套用至所有資源。	2023 年 3 月 17 日
AWSSecurityHubServiceRolePolicy – 更新至現有政策	Security Hub CSPM 將現有 config:PutEvaluations 許可移至政策中的不同陳述式。config:PutEvaluations 許可現在會套用至所有資源。	2021 年 7 月 14 日
AWSSecurityHubServiceRolePolicy – 更新至現有政策	Security Hub CSPM 新增了允許服務連結角色將評估結果交付至其中的許可 AWS Config。	2021 年 6 月 29 日
AWSSecurityHubServiceRolePolicy – 已新增至受管政策清單	新增了受管政策 AWSSecurityHubServiceRolePolicy 的相關資訊，由 Security Hub CSPM 服務連結角色使用。	2021 年 6 月 11 日
AWSSecurityHubOrganizationsAccess – 新政策	Security Hub CSPM 新增了一項新政策，授予 Security Hub CSPM 與 Organizations 整合所需的許可。	2021 年 3 月 15 日

變更	描述	Date
Security Hub CSPM 已開始追蹤變更	Security Hub CSPM 開始追蹤其 AWS 受管政策的變更。	2021 年 3 月 15 日

對 AWS Security Hub CSPM 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 AWS Security Hub CSPM 和 IAM 時可能遇到的常見問題。

主題

- [我無權在 Security Hub CSPM 中執行動作](#)
- [我未獲得執行 iam:PassRole 的授權](#)
- [我想要以程式設計方式存取 Security Hub CSPM](#)
- [我是管理員，想要允許其他人存取 Security Hub CSPM](#)
- [我想要允許以外的人員 AWS 帳戶 存取我的 Security Hub CSPM 資源](#)

我無權在 Security Hub CSPM 中執行動作

如果 AWS 管理主控台 告知您無權執行 動作，則必須聯絡您的管理員尋求協助。您的管理員是為您提供簽署憑證的人員。

當使用者mateojackson嘗試使用主控台檢視###的詳細資訊，但沒有securityhub:*GetWidget*許可時，會發生下列範例錯誤。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
securityhub:GetWidget on resource: my-example-widget
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 *my-example-widget* 動作存取 securityhub:*GetWidget* 資源。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行 iam:PassRole動作，您的政策必須更新，以允許您將角色傳遞至 Security Hub。

有些 AWS 服務 可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM marymajor 使用者嘗試使用主控台在 Security Hub 中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要以程式設計方式存取 Security Hub CSPM

如果使用者想要與 AWS 外部互動，則需要程式設計存取 AWS 管理主控台。授予程式設計存取權的方式取決於正在存取的使用者類型 AWS。

若要授予使用者程式設計存取權，請選擇下列其中一個選項。

哪個使用者需要程式設計存取權？	到	根據
IAM	(建議) 使用主控台登入資料做為臨時登入資料，以簽署對 AWS CLI、AWS SDKs 程式設計請求。AWS APIs	請依照您要使用的介面所提供的指示操作。 - 如需 AWS CLI，請參閱 AWS Command Line Interface 《使用者指南》中的 登入以進行 AWS 本機開發。 - AWS SDKs 請參閱 AWS SDKs 和工具參考指南中的 登入以進行 AWS 本機開發。
人力資源身分 (IAM Identity Center 中管理的使用者)	使用暫時登入資料簽署對 AWS CLI、AWS SDKs 程式設計請求。AWS APIs	請依照您要使用的介面所提供的指示操作。 如需 AWS CLI，請參閱 AWS Command Line Interface 《使用者指南》中的 設定 AWS CLI 要使用 AWS IAM Identity Center 的。

哪個使用者需要程式設計存取權？	到	根據
		AWS SDKs、工具和 AWS APIs，請參閱 AWS SDK 和工具參考指南中的 SDKs IAM Identity Center 身分驗證。
IAM	使用暫時登入資料簽署對 AWS CLI、AWS SDKs 程式設計請求。AWS APIs	遵循《IAM 使用者指南》中 將臨時登入資料與 AWS 資源搭配使用 的指示。
IAM	(不建議使用) 使用長期憑證簽署對 AWS CLI、AWS SDKs 程式設計請求。AWS APIs	請依照您要使用的介面所提供的指示操作。 - 如需 AWS CLI，請參閱 AWS Command Line Interface 《使用者指南》中的 使用 IAM 使用者憑證進行身分驗證。 - AWS SDKs 和工具，請參閱 AWS SDKs 和工具參考指南中的 使用長期憑證進行身分驗證。 - 對於 AWS APIs，請參閱《IAM 使用者指南》中的 管理 IAM 使用者的存取金鑰。

我是管理員，想要允許其他人存取 Security Hub CSPM

若要提供存取權，請新增權限至您的使用者、群組或角色：

- 中的使用者和群組 AWS IAM Identity Center：

建立權限合集。請按照《AWS IAM Identity Center 使用者指南》中的 [建立權限合集](#) 說明進行操作。

- 透過身分提供者在 IAM 中管理的使用者：

建立聯合身分的角色。遵循《IAM 使用者指南》的 [為第三方身分提供者 \(聯合\) 建立角色](#) 中的指示。

- IAM 使用者：
 - 建立您的使用者可擔任的角色。請按照《IAM 使用者指南》的[為 IAM 使用者建立角色](#)中的指示。
 - (不建議) 將政策直接附加至使用者，或將使用者新增至使用者群組。請遵循《IAM 使用者指南》的[新增許可到使用者 \(主控台\)](#) 中的指示。

我想要允許 以外的人員 AWS 帳戶 存取我的 Security Hub CSPM 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Security Hub 是否支援這些功能，請參閱 [Security Hub 如何與 IAM 搭配使用](#)。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《IAM 使用者指南》中的[在您擁有 AWS 帳戶 的另一個 IAM 使用者中提供存取權](#)。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的[將存取權提供給第三方 AWS 帳戶 擁有](#)。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的[將存取權提供給在外部進行身分驗證的使用者 \(聯合身分\)](#)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 [IAM 中的跨帳戶資源存取](#)。

的合規驗證 AWS Security Hub CSPM

若要了解 AWS 服務 是否在特定合規計劃範圍內，請參閱[AWS 服務 合規計劃範圍內](#)然後選擇您感興趣的合規計劃。如需一般資訊，請參閱[AWS 合規計劃](#)。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱[下載報告 in AWS Artifact](#)

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 [AWS 安全文件](#)。

AWS Security Hub 中的彈性

AWS 全球基礎設施是以 AWS 區域 和可用區域為基礎建置。區域提供多個分開且隔離的實際可用區域，並以低延遲、高輸送量和高度備援網路連線相互連結。透過可用區域，您可以設計與操作的應用

程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱 [AWS 全球基礎設施](#)。

中的基礎設施安全 AWS Security Hub CSPM

作為受管服務，AWS Security Hub CSPM 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及如何 AWS 保護基礎設施的資訊，請參閱[AWS 雲端安全](#)。若要使用基礎設施安全的最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的[基礎設施保護](#)。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 Security Hub CSPM。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

AWS Security Hub CSPM 和介面 VPC 端點 (AWS PrivateLink)

您可以建立介面 VPC 端點，AWS Security Hub CSPM 在 VPC 和 之間建立私有連線。介面端點採用[AWS PrivateLink](#)技術，可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線的情況下，私下存取 Security Hub CSPM APIs。VPC 中的執行個體不需要公有 IP 地址，即可與 Security Hub CSPM APIs 通訊。VPC 和 Security Hub CSPM 之間的流量不會離開 Amazon 網路。

每個介面端點都是由您子網路中的一或多個[彈性網路介面](#)表示。如需詳細資訊，請參閱 [《Amazon Virtual Private Cloud 指南》](#) 中的 [AWS 服務 使用介面 VPC 端點存取](#)。Amazon Virtual Private Cloud

Security Hub CSPM VPC 端點的考量事項

設定 Security Hub CSPM 的介面 VPC 端點之前，請務必檢閱 [Amazon Virtual Private Cloud 指南](#) 中的先決條件和其他資訊。

Security Hub CSPM 支援從您的 VPC 呼叫其所有 API 動作。

為 Security Hub CSPM 建立介面 VPC 端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 為 Security Hub CSPM 服務建立 VPC 端點AWS CLI。如需詳細資訊，請參閱 [《Amazon Virtual Private Cloud 指南》](#) 中的[建立 VPC 端點](#)。

使用下列服務名稱建立 Security Hub CSPM 的 VPC 端點：

`com.amazonaws.region.securityhub`

其中 *region* 是適用的區域代碼 AWS 區域。

如果您為端點啟用私有 DNS，您可以使用區域的預設 DNS 名稱向 Security Hub CSPM 提出 API 請求，例如，美國東部 `securityhub.us-east-1.amazonaws.com`（維吉尼亞北部）區域。

為 Security Hub CSPM 建立 VPC 端點政策

您可以將端點政策連接至控制 Security Hub CSPM 存取的 VPC 端點。此政策會指定下列資訊：

- 可執行動作的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《Amazon Virtual Private Cloud 指南》中的[使用端點政策控制對 VPC 端點的存取](#)。

範例：Security Hub CSPM 動作的 VPC 端點政策

以下是 Security Hub CSPM 的端點政策範例。連接到端點時，此政策會授予所有資源上所有委託人的所列 Security Hub CSPM 動作的存取權。

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "securityhub:getFindings",
        "securityhub:getEnabledStandards",
        "securityhub:getInsights"
      ],
      "Resource": "*"
    }
  ]
}
```

共用子網路

無法在與您共用的子網路中建立、描述、修改或刪除 VPC 端點。不過，可以在與您共用的子網路中使用 VPC 端點。如需 VPC 共用的相關資訊，請參閱《Amazon Virtual Private Cloud 指南》中的[與其他帳戶共用 VPC 子網路](#)。

使用 CloudTrail 記錄 Security Hub API 呼叫

AWS Security Hub CSPM 已與整合 AWS CloudTrail，此服務提供由使用者、角色或 Security Hub CSPM 中的 AWS 服務所採取之動作的記錄。CloudTrail 會將 Security Hub CSPM 的 API 呼叫擷取為事件。擷取的呼叫包括來自 Security Hub CSPM 主控台的呼叫，以及對 Security Hub CSPM API 操作的程式碼呼叫。如果您建立追蹤，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Security Hub CSPM 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台內的 Event history (事件歷史記錄) 檢視最新事件。您可以使用 CloudTrail 收集的資訊，判斷向 Security Hub CSPM 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，包括如何設定及啟用，請參閱[《AWS CloudTrail 使用者指南》](#)。

CloudTrail 中的 Security Hub CSPM 資訊

當您建立帳戶 AWS 帳戶時，您的上會啟用 CloudTrail。當 Security Hub CSPM 中發生支援的事件活動時，該活動會與事件歷史記錄中的其他 AWS 服務事件一起記錄在 CloudTrail 事件中。您可以檢視、搜尋和下載帳戶的最新事件。如需詳細資訊，請參閱[使用 CloudTrail 事件歷史記錄檢視事件](#)。

若要持續記錄您帳戶中的事件，包括 Security Hub CSPM 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。根據預設，在主控台建立線索時，該線索會套用到所有 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- [建立追蹤的概觀](#)
- [CloudTrail 支援的服務和整合](#)
- [設定 CloudTrail 的 Amazon SNS 通知](#)
- [接收多個區域的 CloudTrail 日誌檔案](#)和[接收多個帳戶的 CloudTrail 日誌檔案](#)

Security Hub CSPM 支援將所有 Security Hub CSPM API 動作記錄為 CloudTrail 日誌中的事件。若要檢視 Security Hub CSPM 操作的清單，請參閱[Security Hub CSPM API 參考](#)。

將下列動作的活動記錄到 CloudTrail 時，`responseElements` 會設為 `null`。這可確保敏感資訊不包含在 CloudTrail 日誌中。

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求
- 提出該請求時，是否使用了特定角色或聯合身分使用者的臨時安全憑證
- 請求是否由其他 AWS 服務提出

如需詳細資訊，請參閱 [CloudTrail userIdentity 元素](#)。

範例：Security Hub CSPM 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例顯示的是展示 `CreateInsight` 動作的 CloudTrail 日誌項目。在本範例中，建立了名為 `Test Insight` 的洞見。此 `ResourceId` 屬性指定為 `Group by` (分組依據) 彙整工具，而且此洞見不指定任何選用篩選條件。如需洞見的詳細資訊，請參閱在 [Security Hub CSPM 中檢視洞見](#)。

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAJK6U5DS22IAVUI7BW",
    "arn": "arn:aws:iam::012345678901:user/TestUser",
    "accountId": "012345678901",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "TestUser"
  },
}
```



```
"eventTime": "2018-11-25T01:02:18Z",
"eventSource": "securityhub.amazonaws.com",
"eventName": "CreateInsight",
"awsRegion": "us-west-2",
"sourceIPAddress": "205.251.233.179",
"userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
"requestParameters": {
  "Filters": {},
  "ResultField": "ResourceId",
  "Name": "Test Insight"
},
"responseElements": {
  "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
},
"requestID": "c0ffffccd-f04d-11e8-93fc-ddcd14710066",
"eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "012345678901"
}
```

標記 Security Hub 資源

標籤是選用的標籤，您可以定義和指派給 AWS 資源，包括特定類型的 AWS Security Hub CSPM 資源。標籤可協助您以不同方式識別、分類和管理資源，例如透過用途、擁有者、環境或其他條件。例如，您可以使用標籤來區分資源、識別支援特定合規要求或工作流程的資源，或分配成本。

您可以將標籤新增至下列類型的 Security Hub CSPM 資源：

- 自動化規則
- 組態政策
- Hub 資源

標記基本概念

資源最多可以擁有 50 個標籤。每個標籤皆包含由您定義的必要「標籤金鑰」與選用「標籤值」。標籤索引鍵是一般標籤，可做為更特定標籤值的類別。標籤值是標籤金鑰的描述項。

例如，如果您為不同的環境建立不同的自動化規則（一組適用於測試帳戶的自動化規則，另一組則適用於生產帳戶），您可以將Environment標籤金鑰指派給這些規則。相關聯的標籤值可能Test適用於與測試帳戶相關聯的規則，也可能Prod適用於與生產帳戶和 OUs 相關聯的規則。

當您定義標籤並將其指派給 AWS Security Hub CSPM 資源時，請記住下列事項：

- 每個資源的上限為 50 個標籤。
- 對於每個資源，每個標籤索引鍵必須是唯一的，而且只能有一個標籤值。
- 標籤鍵與值皆區分大小寫。最佳實務是，建議您定義將標籤大寫的策略，並在整個資源中一致地實作該策略。
- 標籤索引鍵最多可有 128 個 UTF-8 字元。標籤值最多可有 256 個 UTF-8 字元。字元可以是字母、數字、空格或下列符號：_ . : / = + - @
- 字aws:首保留供使用 AWS。您無法在定義的任何標籤索引鍵或值中使用它。此外，您無法變更或移除使用此字首的標籤索引鍵或值。使用此字首的標籤不會計入每個資源 50 個標籤的配額。
- 您指派的任何標籤僅適用於您的 AWS 帳戶，且僅適用於您指派標籤 AWS 區域的。
- 如果您使用 Security Hub CSPM 將標籤指派給資源，則標籤只會套用至在適用的 Security Hub CSPM 中直接存放的資源 AWS 區域。它們不會套用至 Security Hub CSPM 為您在其他中建立、使用或維護的任何相關支援資源 AWS 服務。例如，如果您將標籤指派給更新與 Amazon Simple

Storage Service (Amazon S3) 相關調查結果的自動化規則，則標籤只會套用至指定區域的 Security Hub CSPM 中的自動化規則。它們不會套用至您的 S3 儲存貯體。若要同時將標籤指派給相關聯的資源，您可以使用 AWS Resource Groups 或 AWS 服務 來存放資源，例如 Amazon S3 用於 S3 儲存貯體。將標籤指派給相關聯的資源，可協助您識別 Security Hub CSPM 資源的支援資源。

- 如果您刪除資源，也會刪除指派給資源的任何標籤。

Important

請勿在標籤中存放機密或其他類型的敏感資料。標籤可從許多 存取 AWS 服務，包括 AWS 帳單與成本管理。它們不適用於敏感資料。

若要新增和管理 Security Hub CSPM 資源的標籤，您可以使用 Security Hub CSPM 主控台、Security Hub CSPM API 或 AWS Resource Groups 標記 API。使用 Security Hub CSPM，您可以在建立資源時將標籤新增至資源。您也可以新增和管理個別現有資源的標籤。透過資源群組，您可以大量新增和管理跨越多個現有資源的標籤 AWS 服務，包括 Security Hub CSPM。

如需其他標記提示和最佳實務，請參閱 [《標記 AWS 資源使用者指南》](#) 中的標記您的 AWS 資源。

在 IAM 政策中使用標籤

開始標記資源後，您可以在 AWS Identity and Access Management (IAM) 政策中定義以標籤為基礎的資源層級許可。透過以這種方式使用標籤，您可以實作精細控制 中的哪些使用者和角色 AWS 帳戶 具有建立和標記資源的許可，以及哪些使用者和角色具有更普遍地新增、編輯和移除標籤的許可。若要根據標籤控制存取，您可以在 IAM 政策 [的條件元素](#) 中使用 [標籤相關條件索引鍵](#)。

例如，您可以建立 IAM 政策，以允許使用者完整存取所有 AWS Security Hub CSPM 資源，如果資源的 Owner 標籤指定其使用者名稱：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ModifyResourceIfOwner",
      "Effect": "Allow",
      "Action": "securityhub:*",
```

```
        "Resource": "*",
        "Condition": {
            "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
                "${aws:username}"
            }
        }
    ]
}
```

如果您定義標籤型、資源層級許可，則許可會立即生效。這表示您的資源一旦建立就會更安全，而且您可以快速開始強制使用新資源的標籤。您也可以使用資源層級許可，以控制哪些標籤金鑰和值可以與新的和現有的資源相關聯。如需詳細資訊，請參閱《IAM 使用者指南》中的[使用標籤控制對 AWS 資源的存取](#)。

將標籤新增至 Security Hub CSPM 資源

標籤是您可以定義和指派給 AWS 資源的標籤，包括特定類型的 AWS Security Hub CSPM 資源。透過使用標籤，您可以以不同的方式識別、分類和管理資源，例如透過用途、擁有者、環境或其他條件。例如，您可以使用標籤來：套用政策、配置成本、區分資源版本，或識別支援特定合規要求或工作流程的資源。

您可以將標籤新增至下列類型的 Security Hub CSPM 資源：

- 自動化規則
- 組態政策
- Hub 資源

資源最多可以擁有 50 個標籤。每個標籤都包含必要的標籤索引鍵和選用的標籤值。標籤索引鍵是一般標籤，可做為更特定標籤值的類別。標籤值是標籤金鑰的描述項。如需標記選項和需求的詳細資訊，請參閱[標記基本概念](#)。

若要將標籤新增至 Security Hub CSPM 資源，您可以使用 Security Hub CSPM 主控台或 Security Hub CSPM API。不過，主控台不支援將標籤新增至 Hub 資源。

新增標籤後，您可以編輯標籤並變更標籤索引鍵或標籤值。

若要同時新增或編輯多個 Security Hub CSPM 資源的標籤，請使用[AWS Resource Groups 標記 API](#)的標記操作。

Important

將標籤新增至資源可能會影響對資源的存取。將標籤新增至資源之前，請檢閱任何可能使用標籤來控制資源存取的 AWS Identity and Access Management (IAM) 政策。

Console

將標籤新增至 Security Hub CSPM 資源（主控台）

當您建立自動化規則或組態政策時，Security Hub CSPM 主控台會提供新增標籤的選項。您可以在標籤區段中提供標籤索引鍵和標籤值。

Security Hub CSPM API

將標籤新增至 Security Hub CSPM 資源 (API)

若要以程式設計方式建立資源並新增一或多個標籤，請針對您要建立的資源類型使用適當的操作：

- 若要建立組態政策並將其新增一或多個標籤，請叫用 [CreateConfigurationPolicy](#) API，或者，如果您使用的是 AWS CLI，請執行 [create-configuration-policy](#) 命令。
- 若要建立自動化規則並將其新增一或多個標籤，請叫用 [CreateAutomationRule](#) API，或者，如果您使用的是 AWS CLI，請執行 [create-automation-rule](#) 命令。
- 若要啟用 Security Hub CSPM 並將一或多個標籤新增至 Hub 資源，請叫用 [EnableSecurityHub](#) API，或者，如果您使用的是 AWS Command Line Interface (AWS CLI)，請執行 [enable-security-hub](#) 命令。

在您的請求中，使用 `tags` 參數指定要新增至資源的每個標籤的標籤索引鍵和選用標籤值。`tags` 參數指定物件陣列。每個物件都會指定標籤索引鍵及其相關聯的標籤值。

若要將一或多個標籤新增至現有資源，請使用 Security Hub CSPM API 的 [TagResource](#) 操作，或者，如果您使用的是 AWS CLI，請執行 [tag-resource](#) 命令。在請求中，指定您要新增標籤之資源的 Amazon Resource Name (ARN)。使用 `tags` 參數為要新增的每個標籤指定標籤索引鍵 (key) 和選用標籤值 (value)。`tags` 參數會指定物件陣列、每個標籤索引鍵一個物件及其相關聯的標籤值。

例如，下列 AWS CLI 命令會將標籤值為 `Prod` 的 `Environment` 索引鍵新增至指定的組態政策。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (\) 行接續字元來改善可讀性。

CLI 命令範例：

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Environment":"Prod"}'
```

其中：

- **resource-arn** 指定要新增標籤之組態政策的 ARN。
- **Environment** 是要新增至規則之標籤的標籤索引鍵。
- **Prod** 是指定標籤索引鍵 () 的標籤值 **Environment**。

在下列範例中，命令會將數個標籤新增至組態政策。

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Environment":"Prod", "CostCenter":"12345", "Owner":"jane-doe"}'
```

對於tags陣列中的每個物件，都需要 key和 value引數。不過，value引數的值可以是空字串。如果您不想將標籤值與標籤索引鍵建立關聯，請不要為value引數指定值。例如，下列命令會新增沒有關聯Owner標籤值的標籤金鑰：

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Owner":""}'
```

如果標記操作成功，Security Hub CSPM 會傳回空的 HTTP 200 回應。否則，Security Hub CSPM 會傳回 HTTP 4xx 或 500 回應，指出操作失敗的原因。

編輯 Security Hub CSPM 資源的標籤

隨著環境或需求隨時間變更，您可以評估 AWS Security Hub CSPM 資源的現有標籤，並視需要變更標籤。標籤是您定義並指派給一或多個 AWS 資源的標籤，包括特定類型的 Macie 資源。每個標籤都包含必要的標籤索引鍵和選用的標籤值。標籤索引鍵是一般標籤，可做為更特定標籤值的類別。標籤值是標籤金鑰的描述項。

標籤可協助您以不同方式識別、分類和管理資源，例如透過用途、擁有者、環境或其他條件。例如，您可以使用標籤來：套用政策、配置成本、區分資源版本，或識別支援特定合規要求或工作流程的資源。

您可以將標籤新增至下列類型的 Security Hub CSPM 資源：

- 自動化規則
- 組態政策
- Hub 資源

若要編輯 Security Hub CSPM 資源的標籤索引鍵或標籤值，您可以使用 Security Hub CSPM API。Security Hub CSPM 主控台目前不支援標籤編輯。

Important

編輯資源的標籤可能會影響對資源的存取。在編輯資源的標籤之前，請檢閱任何可能使用標籤來控制資源存取的 AWS Identity and Access Management (IAM) 政策。

Security Hub CSPM API

編輯 Security Hub CSPM 資源 (API) 的標籤

當您以程式設計方式編輯資源的標籤時，會以新的值覆寫現有的標籤。因此，編輯標籤的最佳方式取決於您要編輯標籤索引鍵、標籤值或兩者。若要編輯標籤金鑰，[請移除目前的標籤並新增標籤](#)。

若要編輯或移除與標籤金鑰相關聯的標籤值，請使用 Security Hub CSPM API 的 [TagResource](#) 操作覆寫現有的值。如果您使用的是 AWS CLI，請執行 [tag-resource](#) 命令。在您的請求中，指定您要編輯或移除其標籤值之資源的 Amazon Resource Name (ARN)。

若要編輯標籤值，請使用 `tags` 參數來指定您要變更其標籤值的標籤索引鍵。您也應該指定金鑰的新標籤值。例如，下列 AWS CLI 命令 `ProdTest` 會將指派給指定自動化規則的標籤金鑰的 `Environment` 標籤值從 `變更為`。此範例已針對 Linux、macOS 或 Unix 格式化，並使用反斜線 (`\`) 行接續字元來改善可讀性。

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```

其中：

- `resource-arn` 指定組態政策的 ARN。
- `Environment` 是與要變更的標籤值相關聯的標籤索引鍵。
- `Test` 是指定標籤索引鍵 () 的新標籤值 `Environment`。

若要從標籤索引鍵移除標籤值，請勿在 `tags` 參數中指定索引鍵 `value` 引數的值。例如：

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags '{"Owner":""}'
```

如果操作成功，Security Hub CSPM 會傳回空的 HTTP 200 回應。否則，Security Hub CSPM 會傳回 HTTP 4xx 或 500 回應，指出操作失敗的原因。

檢閱 Security Hub CSPM 資源的標籤

新增或編輯 AWS Security Hub CSPM 資源的標籤後，您可以檢視資源目前擁有的標籤索引鍵和標籤值。標籤是您定義並指派給一或多個 AWS 資源的標籤，包括特定類型的 Macie 資源。每個標籤都包含必要的標籤索引鍵和選用的標籤值。標籤索引鍵是一般標籤，可做為更特定標籤值的類別。標籤值是標籤金鑰的描述項。

標籤可協助您以不同方式識別、分類和管理資源，例如透過用途、擁有者、環境或其他條件。例如，您可以使用標籤來：套用政策、配置成本、區分資源版本，或識別支援特定合規要求或工作流程的資源。

您可以將標籤新增至下列類型的 Security Hub CSPM 資源：

- 自動化規則
- 組態政策
- Hub 資源

您可以使用 Security Hub CSPM 主控台或 Security Hub CSPM API 來檢閱 Security Hub CSPM 自動化規則或組態政策的標籤。主控台不支援檢閱 Hub 資源的標籤。您可以透過程式設計方式檢閱任何資源的標籤。

若要同時檢閱多個 Security Hub CSPM 資源的標籤，請使用 [AWS Resource Groups 標記 API](#) 的標記操作。

Console

檢閱 Security Hub CSPM 資源的標籤（主控台）

1. 使用 Security Hub CSPM 管理員的登入資料，開啟位於 <https://console.aws.amazon.com/securityhub/> 的 AWS Security Hub CSPM 主控台。
2. 根據您要新增標籤的資源類型，執行下列其中一項操作：
 - 若要檢閱自動化規則的標籤，請在導覽窗格中選擇自動化。然後，選擇自動化規則。
 - 若要檢閱組態政策的標籤，請在導覽窗格中選擇組態。然後，在政策索引標籤上，選取組態政策旁的選項。側邊面板隨即開啟，顯示指派給政策的標籤數量。您可以展開標籤標頭，以查看標籤索引鍵和標籤值。

標籤區段會列出目前指派給資源的所有標籤。

Security Hub CSPM API

檢閱 Security Hub CSPM 資源 (API) 的標籤

若要擷取和檢閱現有資源的標籤，請叫用 [ListTagsForResource](#) API。在您的請求中，使用 `resourceArn` 參數來指定資源的 Amazon Resource Name (ARN)。

如果您使用的是 AWS CLI，請執行 [list-tags-for-resource](#) 命令，並使用 `resource-arn` 參數來指定資源的 ARN。例如：

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

如果操作成功，Security Hub CSPM 會傳回tags陣列。陣列中的每個物件都會指定目前指派給資源的標籤（包括標籤索引鍵和標籤值）。例如：

```
{
  "tags": [
    {
      "key": "Environment",
      "value": "Prod"
    },
    {
      "key": "CostCenter",
      "value": "12345"
    }
  ],
}
```

```
{
  {
    "key": "Owner",
    "value": ""
  }
}
```

其中 Environment、CostCenter 和 Owner 是指派給資源的標籤金鑰。Prod 是與標籤金鑰相關聯的 Environment 標籤值。12345 是與標籤金鑰相關聯的 CostCenter 標籤值。Owner 標籤索引鍵沒有相關聯的標籤值。

若要擷取具有標籤的所有 Security Hub CSPM 資源清單，以及指派給每個資源的所有標籤，請使用 AWS Resource Groups 標記 API 的 [GetResources](#) 操作。在您的請求中，將 ResourceTypeFilters 參數的值設定為 securityhub。若要使用執行此操作 AWS CLI，請執行 [get-resources](#) 命令，並將 resource-type-filters 參數的值設定為 securityhub。例如：

```
$ aws resourcegroupstaggingapi get-resources --resource-type-filters "securityhub"
```

如果操作成功，資源群組會傳回 ResourceTagMappingList 陣列。陣列為每個具有標籤的 Security Hub CSPM 資源包含一個物件。每個物件都會指定 Security Hub CSPM 資源的 ARN，以及指派給資源的標籤索引鍵和值。

從 Security Hub CSPM 資源移除標籤

如果您將標籤新增至 AWS Security Hub CSPM 資源，您之後可以移除一或多個標籤。標籤是您定義和指派給 AWS 資源的標籤，包括特定類型的 Security Hub CSPM 資源。您可以從下列類型的 Security Hub CSPM 資源新增、編輯和移除標籤：自動化規則、組態政策和資源Hub。

若要從個別 AWS Security Hub CSPM 資源移除標籤，您可以使用 Security Hub CSPM API。Security Hub CSPM 主控台目前不支援標籤移除。

若要同時從多個 Security Hub CSPM 資源中移除標籤，請使用 [AWS Resource Groups 標記 API](#) 的標記操作。

Important

從資源移除標籤可能會影響對資源的存取。移除標籤之前，請檢閱任何可能使用該標籤來控制資源存取的 AWS Identity and Access Management (IAM) 政策。

Security Hub CSPM API

從 Security Hub CSPM 資源 (API) 移除標籤

若要以程式設計方式從資源移除一或多個標籤，請使用 Security Hub CSPM API 的 [UntagResource](#) 操作。在您的請求中，使用 `resourceArn` 參數來指定要從中移除標籤之資源的 Amazon Resource Name (ARN)。使用 `tagKeys` 參數來指定要移除之標籤的標籤索引鍵。若要移除多個標籤，請附加要移除之每個標籤的 `tagKeys` 參數和引數，並以 ampersand (&) 分隔，例如 `tagKeys=key1&tagKeys=key2`。若要僅從資源移除特定標籤值（而非標籤索引鍵），[請編輯標籤](#)，而不是移除標籤。

如果您使用的是 AWS CLI，請執行 [untag-resource](#) 命令，從資源中移除一或多個標籤。針對 `resource-arn` 參數，指定要從中移除標籤之資源的 ARN。使用 `tag-keys` 參數指定要移除之標籤的標籤索引鍵。例如，下列命令會從指定的組態政策中移除 `Environment` 標籤（包括標籤索引鍵和標籤值）：

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

其中 `resource-arn` 指定要從中移除標籤之組態政策的 ARN，且 `Environment` 是要移除之標籤的標籤索引鍵。

若要從資源移除多個標籤，請新增每個額外的標籤索引鍵做為 `tag-keys` 參數的引數。例如：

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

如果操作成功，Security Hub CSPM 會傳回空的 HTTP 200 回應。否則，Security Hub CSPM 會傳回 HTTP 4xx 或 500 回應，指出操作失敗的原因。

Security Hub 的配額

您的 AWS 帳戶 具有特定預設配額，先前稱為每個配額的限制 AWS 服務。這些配額是您帳戶的 服務資源或操作數量上限。本主題連結至適用於您 帳戶的 AWS Security Hub 資源和操作的配額。除非另有說明，否則每個配額都適用於您的 帳戶 AWS 區域。

有些配額可以增加，有些則無法增加。若要請求提高配額，請使用 [Service Quotas 主控台](#)。若要了解如何請求提高配額，請參閱 [《Service Quotas 使用者指南》中的請求提高配額](#)。Service Quotas 如果 Service Quotas 主控台上沒有配額，請使用 上的 [服務限制增加表單](#) AWS Support Center Console 來請求增加配額。

最大配額

如需適用於 AWS Security Hub 資源的配額清單，請參閱《》中的 [AWS Security Hub 端點和配額](#) AWS 一般參考。

費率配額

如需適用於 AWS Security Hub API 操作的配額清單，請參閱 [AWS Security Hub API 參考](#)。

如果您在 [Security Hub CSPM 中設定跨區域彙總](#)，則一次對連結區域BatchImportFindings和彙總區域的呼叫和BatchUpdateFindings影響。GetFindings 操作會從連結的區域和彙總區域擷取問題清單。不過，BatchEnableStandards和 UpdateStandardsControl操作是區域特定的。

AWS Security Hub 使用者指南的文件歷史記錄

下表說明自上次發行 AWS Security Hub 和 Security Hub CSPM 以來文件的重要變更。針對新版 Security Hub CSPM 控制項，日期會指定控制項何時開始在支援的 中使用 AWS 區域。在所有支援的區域中，控制項可能需要 1-2 週才能使用。如需現有控制項之重大變更的詳細資訊，請參閱 [Security Hub CSPM 控制項的變更日誌](#)。

若要接收 AWS Security Hub 使用者指南的更新通知，您可以訂閱 RSS 摘要。

變更	描述	日期
未使用的存取調查結果	Security Hub 新增了從 IAM Access Analyzer 產生和顯示未使用存取問題清單的功能 了解 Security Hub 中未使用的存取問題清單	2026 年 5 月 19 日
新的安全控制	Security Hub CSPM 發佈了五個新的控制項。某些控制項支援 AWS 基礎安全最佳實務 (FSBP) 標準。大多數控制項支援 NIST SP 800-53 修訂版 5 要求。 - 對於 AWS FSBP 標準，適用控制項IDs 為：BedrockAgentCore.5 和 BedrockAgentCore.6。 - 對於 NIST SP 800-53 修訂版 5，適用控制項IDs 為：BedrockAgentCore.3、BedrockAgentCore.4 和 SageMaker.18。	2026 年 5 月 15 日
受管政策的更新 – AWS SecurityHubServiceRolePolicy	Security Hub CSPM 已更新名為的 AWS 受管政策 AWS SecurityHubServ	2026 年 4 月 29 日

iceRolePolicy 。更新新增了管理 Security Hub CSPM 服務連結組態記錄器和建立 AWS Config 服務連結角色的許可。

新的安全控制

Security Hub CSPM 發佈了[AWS 針對基礎安全最佳實務 \(FSBP\) 標準](#)的四個新控制項。新的控制項包括：[BedrockAgentCore.1](#)、[BedrockAgentCore.2](#)、[RDS.51](#) 和 [SageMaker.19](#)。

新的安全控制

Security Hub CSPM 針對[AWS 基礎安全最佳實務 \(FSBP\) 標準](#)發佈了五個新控制項。新的控制項包括：[APIGateway.11](#)、[EC2.183](#)、[EKS.9](#)、[SageMaker.16](#) 和 [SageMaker.17](#)。

安全標準和控制項的更新

我們已淘汰 AppSync.1 和 AppSync.6 控制項，並將其從[AWS 基礎安全最佳實務 \(FSBP\) 標準](#)中移除。AWS AppSync 現在為所有目前和未來的 API 快取提供預設加密。

安全標準和控制項的更新

我們已淘汰 ECS.1 控制項，並從[AWS 基礎安全最佳實務 \(FSBP\) 標準](#)和 [NIST SP 800-53 修訂版 5 標準](#)中移除控制項。

新的安全控制

Security Hub CSPM 發佈了 [AWS 針對基礎安全最佳實務 \(FSBP\) 標準](#) 的十一個新控制項。新的控制項包括：[APIGateway.10](#)、[ELB.21](#)、[ELB.22](#)、[RDS.50](#)、[SageMaker.9](#) [SageMaker.10](#) [SageMaker.11](#) [SageMaker.12](#) [SageMaker.13](#) [SageMaker.14](#) 和 [SageMaker.15](#)。

安全標準和控制項的更新

我們已淘汰 MQ.3 控制項，並從所有適用標準中移除控制項。由於 Amazon MQ 要求自動次要版本升級，我們已淘汰控制。

先前，此控制項適用於 [AWS 基礎安全最佳實務 \(FSBP\) 標準](#)、[NIST SP 800-53 修訂版 5 標準](#) 和 [PCI DSS 4.0.1 版標準](#)。

成本估算器文件的更新

將詳細資訊新增至 Security Hub 成本估算器文件，說明如何授予跨帳戶存取權，以便在管理帳戶以外的帳戶中進行預估。

新的安全控制

Security Hub CSPM 針對 [AWS 基礎安全最佳實務 \(FSBP\) 標準](#) 發佈了五個新控制項。新的控制項為：[CloudFormation.4](#)、[CloudFront.17](#)、[ECS.19](#)、[ECS.20](#) 和 [ECS.21](#)。

安全標準和控制項的更新	由於 Amazon MQ 對自動次要版本升級的要求，我們計劃在 2026 年 1 月 12 日淘汰 MQ.3 並從所有適用標準中移除控制權。目前，控制項適用於 AWS 基礎安全最佳實務 (FSBP) 標準 、 NIST SP 800-53 修訂版 5 標準 和 PCI DSS 4.0.1 版標準 。	2025 年 12 月 12 日
更新服務受管標準的內容： AWS Control Tower	更新了 服務受管標準的內容 ： AWS Control Tower 提供在標準中建立、檢視和停用控制項的改善指引 AWS Control Tower。	2025 年 12 月 8 日
新的安全控制	Security Hub CSPM 針對 AWS 基礎安全最佳實務 (FSBP) 標準 發佈了七項新控制。新的控制項包括： Cognito.4 、 Cognito.5 、 Cognito.6 、 EC2.182 、 CloudFormation.3 、 ECS.18 和 SES.3 。	2025 年 12 月 8 日
更新 Security Hub 一般可用性的內容	新增內容以支援 AWS Security Hub 的一般可用性版本	2025 年 12 月 2 日
已更新 Security Hub 的內容	新增 趨勢 和 區域彙總 的內容。這些變更支援 Security Hub 預覽版本。	2025 年 11 月 21 日

[受管政策的更新 – AWSSecurityHubV2ServiceRolePolicy](#)

Security Hub 已更新名為 [的AWS 受管政策](#) [AWSSecurityHubV2ServiceRolePolicy](#) 。這些更新新增了 Amazon Elastic Container Registry、Amazon CloudWatch 和 AWS Lambda 的計量功能 AWS Identity and Access Management ，以支援 Security Hub 功能。這些更新也新增了對全域 AWS Config 記錄器的支援。這些變更支援 Security Hub 預覽版本。

2025 年 11 月 17 日

[受管政策的更新 – AWSSecurityHubOrganizationsAccess](#)

Security Hub 已更新名為 [的AWS 受管政策](#) [AWSSecurityHubOrganizationsAccess](#) 。更新新增了許可，以描述支援 Security Hub 功能的資源政策。這些變更支援 Security Hub 預覽版本。

2025 年 11 月 17 日

[受管政策的更新 – AWSSecurityHubFullAccess](#)

Security Hub 已更新名為 [的AWS 受管政策](#) [AWSSecurityHubFullAccess](#) 。這些更新新增了有關管理 GuardDuty、Amazon Inspector 和帳戶管理的功能，以支援 Security Hub 功能。這些變更支援 Security Hub 預覽版本。

2025 年 11 月 17 日

[安全性控制項的更新](#)

我們變更了 10 Security Hub CSPM 控制項的嚴重性：CloudFront.7、CloudTrail.5、ELB.7、GuardDuty.7、MQ.3、OpenSearch.10、RDS.7、ServiceCatalog.1、SNS.4 和 SQS.3。如需變更的明細，請參閱 [Security Hub CSPM 控制項的變更日誌](#)。

2025 年 11 月 13 日

[新的安全控制](#)

Security Hub CSPM 發佈了六項 [AWS 新的基礎安全最佳實務 \(FSBP\) 標準](#) 控制項。新的控制項包括：[Cognito.3](#)、[DMS.13](#)、[EC2.181](#)、[RDS.43](#)、[RDS.47](#) 和 [RDS.48](#)。

2025 年 10 月 28 日

[新的安全標準](#)

Security Hub CSPM 現在提供符合 CIS AWS Foundations Benchmark v5.0.0 [的安全標準](#)。這個新標準包含 40 個現有的安全控制。控制項會執行自動檢查，評估特定資源是否符合架構定義的部分需求。

2025 年 10 月 16 日

[新的第三方整合](#)

Elastic 是一種新的 [第三方整合](#)，可以從 Security Hub CSPM 接收問題清單。

2025 年 10 月 3 日

安全標準和控制的更新

我們已淘汰 Redshift.9 和 RedshiftServerless.7 控制項，並將其從所有適用標準中移除。我們因為固有的 Amazon Redshift 限制而淘汰這些控制項，這些限制無法有效修復控制項的問題 FAILED 清單。

2025 年 9 月 24 日

先前，這些控制項適用於 [AWS 基礎安全最佳實務 \(FSBP\) 標準](#) 和 [NIST SP 800-53 修訂版 5 標準](#)。Redshift.9 控制項也套用至 [AWS Control Tower 服務受管標準](#)。

區域可用性

Security Hub CSPM 現已在亞太區域（紐西蘭）區域提供。如需 Security Hub CSPM 目前可用 AWS 區域位置的完整清單，請參閱《》中的 [AWS Security Hub 端點和配額](#) AWS 一般參考。

2025 年 9 月 19 日

新的安全控制

Security Hub CSPM 發佈了兩個 [AWS 新的基礎安全最佳實務 \(FSBP\) 標準](#) 控制項：[CloudFront.16](#) 和 [RDS.46](#)。

2025 年 9 月 3 日

區域可用性

[AWS 資源標記標準](#) 現已在亞太區域（泰國）和墨西哥（中部）區域提供。

2025 年 8 月 29 日

[安全標準和控制項的更新](#)

由於 Amazon Redshift 的限制，我們計劃在 2025 年 9 月 15 日淘汰 Redshift.9 和 RedshiftServerless.7 控制項，並將其從所有適用標準中移除。目前，這些控制項適用於[AWS 基礎安全最佳實務 \(FSBP\) 標準](#)和[NIST SP 800-53 修訂版 5 標準](#)。Redshift.9 控制項也適用於[AWS Control Tower 服務受管標準](#)。

2025 年 8 月 15 日

[ASFF 中的新資源詳細資訊物件](#)

[AWS 安全調查結果格式 \(ASFF\)](#) 現在包含 CodeRepository 資源物件。此物件提供連線至 AWS 資源的外部程式碼儲存庫詳細資訊，並設定 Amazon Inspector 掃描漏洞。

2025 年 8 月 1 日

[區域可用性](#)

Security Hub CSPM 現已在亞太區域（台北）區域提供。如需 Security Hub CSPM 目前可用 AWS 區域位置的完整清單，請參閱《》中的[AWS Security Hub 端點和配額](#)AWS 一般參考。

2025 年 7 月 23 日

[新的第三方整合](#)

Dynatrace 是一種新的[第三方整合](#)，可以從 Security Hub CSPM 接收問題清單。

2025 年 7 月 18 日

新的安全控制

Security Hub CSPM 發佈了 13 個新控制項。大多數控制項都支援 [AWS 基礎安全最佳實務 \(FSBP\)](#) 標準。某些控制項支援 [NIST SP 800-53 修訂版 5](#) 要求。

2025 年 7 月 15 日

- 對於 AWS FSBP 標準，適用控制項IDs 為：[CloudFront.15](#)、[Cognito.2](#)、[EC2.180](#)、[ELB.18](#)、[MSK.4](#)、[MSK.5](#)、[MSK.6](#)、[RDS.45](#)、[Redshift.18](#)、[S3.25](#)、[SSM.6](#) 和 [SSM.7](#)。
- 對於 NIST SP 800-53 修訂版 5，適用控制項IDs 為：[Lambda.7](#) 和 [RDS.45](#)。

控制問題清單的產生更新

為了協助您追蹤合規變更，當個別資源的合規狀態發生變更時，Security Hub CSPM 現在會 [更新現有的控制調查結果](#)，而不是產生新的調查結果。這表示您可以使用個別調查結果提供的資料，根據特定控制項追蹤特定資源的合規變更。

2025 年 7 月 3 日

安全標準和控制項的更新

我們已從 PCI DSS v4.0.1 標準移除 IAM.13 控制。 <https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html> 我們也從 NIST SP 800-171 修訂版 2 標準中移除 IAM.17 控制項。這些標準不會明確要求這些控制項提供的檢查。我們也針對檢查 IAM 密碼政策的特定控制項更新了這些標準的相關需求詳細資訊：IAM.7，以及透過 IAM.17 的 IAM.10。

2025 年 6 月 30 日

問題清單保留的更新

Security Hub CSPM 現在將[封存的問題清單存放](#) 30 天，而不是 90 天，這可以減少問題清單的雜訊。如需長期保留，您可以使用[具有 Amazon EventBridge 規則的自訂動作](#)，將問題清單匯出至 S3 儲存貯體。

2025 年 6 月 20 日

現有 受管政策的更新

Security Hub CSPM 已將新許可新增至名為的[AWS 受管政策](#) `AWSecurityHubOrganizationsAccess`。許可允許組織管理在組織內啟用和管理 Security Hub 和 Security Hub CSPM。Security Hub CSPM 也將新許可新增至名為的 AWS 受管政策 `AWSecurityHubFullAccess`。許可允許主體為 Security Hub 建立服務連結角色。

2025 年 6 月 18 日

Security Hub 的公有預覽版本和新的受管政策

AWS Security Hub 的公開預覽版本和 [AWS Security Hub 使用者指南](#)。此版本包含新的 [AWS 受管政策](#) `AWSecurityHubV2ServiceRolePolicy`。此政策允許 Security Hub 代表客戶管理客戶組織中的 AWS Config 規則和 Security Hub 資源。Security Hub 處於預覽版本，可能會有所變更。

2025 年 6 月 17 日

安全標準和控制項的更新

我們已從 PCI DSS v4.0.1 標準中移除 [IAM.10 控制項](#)。
<https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html> 此控制項會檢查 IAM 使用者的帳戶密碼政策是否符合最低需求，包括至少 7 個字元的密碼長度。PCI DSS v4.0.1 現在需要密碼至少 8 個字元。IAM.10 控制項會繼續套用至具有不同密碼需求的 PCI DSS v3.2.1 標準。

2025 年 5 月 30 日

新的安全標準

Security Hub CSPM 現在提供符合 NIST SP 800-171 修訂版 2 網路安全和合規架構的 [安全標準](#)。此新標準包含超過 60 個現有的安全控制。這些控制項會執行自動檢查，評估特定 AWS 服務和資源是否符合架構定義的部分需求。

2025 年 5 月 29 日

安全性控制項的更新

Security Hub CSPM 在所有 中 復原了下列控制項的版本 AWS 區域：【RDS.46】 RDS 資料庫執行個體不應部署在具有網際網路閘道路由的公有子網路中。先前，此控制項支援 AWS 基礎安全最佳實務 (FSBP) 標準。

2025 年 5 月 8 日

新的安全控制

Security Hub CSPM 發佈了 9 個新控制項。大多數控制項都支援 [AWS 基礎安全最佳實務 \(FSBP\)](#) 標準。某些控制項支援 [NIST SP 800-53 修訂版 5](#) 要求。

2025 年 5 月 7 日

- 對於 AWS FSBP 標準，適用控制項IDs 為：[DocumentD B.6](#)、[RDS.44](#)、[RedshiftServerless.2](#)、[RedshiftServerless.3](#)、[RedshiftServerless.5](#)、[RedshiftServerless.6](#) 和 [RedshiftServerless.7](#) (已淘汰)。
- 對於 NIST SP 800-53 修訂版 5，適用控制項IDs 為：[CloudTrail.10](#)、[RedshiftServerless.4](#) 和 [RedshiftServerless.7](#) (已淘汰)。

新的安全控制

Security Hub CSPM 發佈了 24 個新控制項。大多數控制項支援 [AWS 基礎安全最佳實務 \(FSBP\)](#) 或 [AWS 資源標記標準](#)。某些控制項支援 [NIST SP 800-53 修訂版 5](#) 要求。

2025 年 4 月 16 日

- 對於 AWS FSBP 標準，適用控制項IDs 為：[EC2.173](#)、[RDS.41](#)、[RDS.42](#) 和 [SageMaker.8](#)。
- 對於 AWS 資源標記標準，適用控制項IDs 為：[Amplify.1](#)、[Amplify.2](#)、[Batch.4](#)、[DataSync.2](#)、[EC2.174](#)、[EC2.175](#)、[EC2.176](#)、[EC2.177](#)、[EC2.178](#)、[EC2.179](#)、[F1.17](#)、[SageMaker.6](#)、[SageMaker.7](#)、[SSM.5](#)、[Transfer.4](#)、[Transfer.5](#)、[Transfer.6](#) 和 [Transfer.7](#)。
- 對於 NIST SP 800-53 修訂版 5，適用控制項IDs 為：[ECS.17](#) 和 [RDS.42](#)。

新的安全控制

Security Hub CSPM 發佈了 [AWS 針對基礎安全最佳實務標準](#) 的四個新控制項。控制項包括：

2025 年 3 月 18 日

- [the section called “【FSx.3\] FSx for OpenZFS 檔案系統應設定為異地同步備份部署”](#)
- [the section called “【FSx.4\] FSx for NetApp ONTAP 檔案系統應設定為異地同步備份部署”](#)
- [the section called “【FSx.5\] FSx for Windows File Server 檔案系統應設定為異地同步備份部署”](#)
- [the section called “【RedshiftServerless.1\] Amazon Redshift Serverless 工作群組應使用增強型 VPC 路由”](#)

安全標準和控制項的更新

我們已從 AWS 基礎 [安全最佳實務標準](#) 移除 [RDS.18 安全控制](#)，並自動檢查 NIST SP 800-53 修訂版 5 要求。由於 Amazon EC2-Classical 網路已淘汰，因此 Amazon Relational Database Service (Amazon RDS) 執行個體無法再部署在 VPC 外部。控制項仍是 [AWS Control Tower 服務受管標準](#) 的一部分。

2025 年 3 月 7 日

控制問題清單的更新

如果控制項檢查的資源類型未在中開啟[資源錄製](#)，Security Hub AWS Config CSPM 現在會產生已啟用控制項的問題WARNING清單。這可協助您識別和解決安全控制檢查中潛在的組態差距。

2025 年 2 月 25 日

新的安全控制

Security Hub CSPM 發佈了 11 個新控制項。控制項包括：

- the section called “【Connect.2】 Connect Customer 執行個體應啟用 CloudWatch 記錄”
- the section called “【ECR.5】 ECR 儲存庫應使用客戶受管加密 AWS KMS keys”
- the section called “【ELB.17】 具有接聽程式的應用程式和 Network Load Balancer 應使用建議的安全政策”
- the section called “【Glue.4】 AWS Glue Spark 任務應在支援的 版本上執行 AWS Glue”
- the section called “【GuardDuty.11] 應啟用 GuardDuty 執行期監控”
- the section called “【GuardDuty.12] 應啟用 GuardDuty ECS 執行期監控”
- the section called “【GuardDuty.13] 應啟用 GuardDuty EC2 執行期監控”
- the section called “【NetworkFirewall.10] 網路防火牆防火牆應啟用子網路變更保護”

- [the section called “【RDS.40】 RDS for SQL Server 資料庫執行個體應將日誌發佈至 CloudWatch Logs”](#)
- [the section called “【SQS.3】 SQS 佇列存取政策不應允許公開存取”](#)
- [the section called “【Transfer.3】 Transfer Family 連接器應該已啟用記錄”](#)

[新的安全控制](#)

Security Hub CSPM 發佈了 [AWS 資源標記標準的 37 個新控制項](#)。Security Hub CSPM 也發行了下列新控制項：

2025 年 1 月 22 日

- [the section called “【EMR.3】 Amazon EMR 安全組態應靜態加密”](#)
- [the section called “【EMR.4】 Amazon EMR 安全組態應在傳輸中加密”](#)
- [the section called “【SageMaker.5】 SageMaker 模型應該啟用網路隔離”](#)

[新的安全控制](#)

Security Hub CSPM 發佈的 [EC2.172 EC2 VPC 封鎖公開存取設定應封鎖網際網路閘道流量](#)。

2025 年 1 月 15 日

[新的安全控制](#)

下列新的 Security Hub CSPM 控制項可供使用。

2024 年 12 月 17 日

- [the section called “【Cognito.1】 Cognito 使用者集區應以標準身分驗證的完整功能強制執行模式啟用威脅防護”](#)
- [the section called “【RDS.38】 RDS for PostgreSQL 資料庫執行個體應在傳輸中加密”](#)
- [the section called “【RDS.39】 RDS for MySQL 資料庫執行個體應在傳輸中加密”](#)
- [the section called “【Redshift.16】 Redshift 叢集子網路群組應具有來自多個可用區域的子網路”](#)

[Security Hub CSPM 支援 PCI DSS v4.0.1](#)

Security Hub CSPM 現在支援支付卡產業資料安全標準 (PCI DSS) 的 4.0.1 版。如需標準及其適用的控制項的詳細資訊，請參閱 [Security Hub CSPM 中的 PCI DSS](#)。

2024 年 12 月 11 日

[Security Hub CSPM 會收到 GuardDuty 攻擊序列調查結果](#)

Security Hub CSPM 現在會從 Amazon GuardDuty 延伸威脅偵測收到攻擊序列調查結果。攻擊序列調查結果詳細資訊可在 AWS 安全調查結果格式 (ASFF) 的 [偵測](#) 物件中取得。

2024 年 12 月 1 日

[新 中支援的 Security Hub CSPM AWS 區域](#)

Security Hub CSPM 現已在亞太區域（馬來西亞）區域提供。有些安全控制具有區域限制。如需此區域無法使用的控制項清單，請參閱 [Security Hub CSPM 控制項的區域限制](#)。

2024 年 11 月 22 日

[Config.1 的變更](#)

Security Hub CSPM 將 Config.1 控制項的嚴重性從 提高MEDIUM為 CRITICAL，並為失敗的 Config.1 調查結果新增新的狀態碼和狀態原因。如需變更的詳細資訊，請參閱 [Security Hub CSPM 控制項變更日誌](#) 中 2024 年 11 月 20 日的項目。

2024 年 11 月 20 日

新的安全控制

2024 年 11 月 15 日

下列新的 Security Hub CSPM 控制項可供使用。這些控制項是 AWS 基礎安全最佳實務和 NIST SP 800-53 第 5 版的一部分，它們會評估您管理的虛擬私有雲端 (VPC) 是否具有 AWS 服務 或 AWS 資源的介面 VPC 端點。

- [the section called “【EC2.55】 VPCs應使用 ECR API 的介面端點進行設定”](#)
- [the section called “【EC2.56】 VPCs應使用 Docker 登錄檔的介面端點進行設定”](#)
- [the section called “【EC2.57】 VPCs應使用 Systems Manager 的介面端點進行設定”](#)
- [the section called “【EC2.58】 VPCs應使用 Systems Manager Incident Manager Contacts 的介面端點進行設定”](#)
- [the section called “【EC2.60】 VPCs應使用 Systems Manager Incident Manager 的介面端點進行設定”](#)

新的安全控制

下列新的 Security Hub CSPM 控制項可供使用。

2024 年 10 月 18 日

- [the section called “【AppSync.1】AWS AppSync API 快取應靜態加密”](#)
- [the section called “【AppSync.6】AWS AppSync API 快取應在傳輸中加密”](#)
- [the section called “【EC2.170】EC2 啟動範本應使用執行個體中繼資料服務第 2 版 \(IMDSv2\)”](#)
- [the section called “【EC2.171】EC2 VPN 連線應該已啟用記錄”](#)
- [the section called “【EFS.8】EFS 檔案系統應靜態加密”](#)
- [the section called “【KMS.5】不應公開存取 KMS 金鑰”](#)
- [the section called “【SNS.4】SNS 主題存取政策不應允許公開存取”](#)

新的安全控制

下列新的 Security Hub CSPM 控制項可供使用。 2024 年 10 月 3 日

- [the section called “【ECS.16】 ECS 任務集不應自動指派公有 IP 地址”](#)
- [the section called “【GuardDuty.7】應啟用 GuardDuty EKS 執行期監控”](#)
- [the section called “【Kinesis.3】 Kinesis 串流應具有足夠的資料保留期”](#)
- [the section called “【MSK.3】 MSK Connect 連接器應在傳輸中加密”](#)
- [the section called “【RDS.36】 RDS for PostgreSQL 資料庫執行個體應將日誌發佈至 CloudWatch Logs”](#)
- [the section called “【RDS.37】 Aurora PostgreSQL 資料庫叢集應將日誌發佈至 CloudWatch Logs”](#)
- [the section called “【S3.24】 S3 多區域存取點應啟用封鎖公開存取設定”](#)

新的安全控制

下列新的 Security Hub CSPM 控制項可供使用。

2024 年 8 月 30 日

- [the section called “【Athena.4】 Athena 工作群組應該已啟用記錄”](#)
- [the section called “【CodeBuild.7】 CodeBuild 報告群組匯出應靜態加密”](#)
- [the section called “【DataSync.1】 DataSync 任務應該已啟用記錄”](#)
- [the section called “【EFS.7】 EFS 檔案系統應該啟用自動備份”](#)
- Glue.2 (已淘汰)
- [the section called “【Glue.3】 AWS Glue 機器學習轉換應該靜態加密”](#)
- [the section called “【WorkSpaces.1】 應靜態加密 WorkSpaces 使用者磁碟區”](#)
- [the section called “【WorkSpaces.2】 WorkSpaces 根磁碟區應靜態加密”](#)

新的問題清單面板

Security Hub CSPM 主控台上的 [新調查結果面板](#) 可協助您快速對調查結果採取行動、檢閱資源詳細資訊和調查結果歷史記錄，以及尋找有關調查結果的其他相關資訊。

2024 年 8 月 16 日

[Config.1 控制項的更新](#)

[Config.1 控制項](#)會檢查 AWS Config 是否已啟用、使用服務連結角色，以及記錄已啟用控制項的資源。Security Hub CSPM 新增了名為的自訂控制參數 `includeConfigServiceLinkedRoleCheck`。透過將此參數設定為 `false`，您可以選擇不檢查是否 AWS Config 使用服務連結角色。

2024 年 8 月 15 日

[指定沒有連結區域的主區域](#)

您現在可以建立問題清單彙總工具並建立主要區域，而無需 AWS 區域 將任何 連結至主要區域。這可讓您啟用[中央組態](#)，而無需指定連結的區域。

2024 年 7 月 25 日

[選取更多區域中可用的控制項](#)

下列控制項現在可在其他 中使用 AWS 區域，包括美國東部（維吉尼亞北部）和美國東部（俄亥俄）。

2024 年 7 月 15 日

- [the section called “【DataFirehose.1】 Firehose 交付串流應靜態加密”](#)
- [the section called “【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權”](#)
- [the section called “【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制”](#)
- [the section called “【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS”](#)
- [the section called “【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密”](#)
- [the section called “【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯”](#)
- [the section called “【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密”](#)
- [the section called “【FSx.2】 FSx for Lustre 檔案系統應設定為將標籤複製到備份”](#)
- [the section called “【MQ.2】 ActiveMQ 代理](#)

程式應將稽核日誌串流至 CloudWatch”

- the section called “【MQ.3】 Amazon MQ 代理程式應該啟用自動次要版本升級”
- the section called “【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點”
- the section called “【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠”
- the section called “【SageMaker.4】 SageMaker 端點生產變體的初始執行個體計數應大於 1”
- the section called “【Service Catalog.1】 Service Catalog 產品組合只能在 AWS 組織內共用”
- the section called “【Transfer.2】 Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線”

新的安全控制

可使用下列新的 Security Hub CSPM 控制項：

2024 年 7 月 11 日

- [the section called “【GuardDuty.5】應啟用 GuardDuty EKS 稽核日誌監控”](#)
- [the section called “【GuardDuty.6】應啟用 GuardDuty Lambda 保護”](#)
- [the section called “【GuardDuty.8】應啟用 EC2 的 GuardDuty 惡意軟體防護”](#)
- [the section called “【GuardDuty.9】應啟用 GuardDuty RDS 保護”](#)
- [the section called “【GuardDuty.10】應啟用 GuardDuty S3 保護”](#)
- [the section called “【Inspector or.1】應啟用 Amazon Inspector EC2 掃描”](#)
- [the section called “【Inspector or.2】應啟用 Amazon Inspector ECR 掃描”](#)
- [the section called “【Inspector or.3】應啟用 Amazon Inspector Lambda 程式碼掃描”](#)
- [the section called “【Inspector or.4】應啟用 Amazon Inspector Lambda 標準掃描”](#)

CIS AWS Foundations Benchmark 3.0.0 版的發行

Security Hub CSPM 發佈
Center for Internet Security
(CIS) AWS Foundations
Benchmark v3.0.0。此版本包
含下列新控制項，以及數個現
有控制項的映射。

2024 年 5 月 13 日

- the section called
“【EC2.53】 EC2 安全群組
不應允許從 0.0.0.0/0 傳入遠
端伺服器管理連接埠”
- the section called
“【EC2.54】 EC2 安全群組
不應允許從 ::/0 傳入遠端
伺服器管理連接埠”
- the section called
“【IAM.26】 應移除在 IAM
中管理的過期 SSL/TLS 憑
證”
- the section called
“【IAM.27】 IAM 身分不應
連接 AWSCloudShellFullA
ccess 政策”
- the section called
“【IAM.28】 應啟用 IAM
Access Analyzer 外部存取分
析器”
- the section called
“【S3.22】 S3 一般用途儲存
貯體應記錄物件層級寫入事
件”
- the section called
“【S3.23】 S3 一般用途儲存
貯體應記錄物件層級讀取事
件”

新的安全控制

可使用下列新的 Security Hub CSPM 控制項：

2024 年 5 月 3 日

- [the section called “【DataFirehose.1】 Firehose 交付串流應靜態加密”](#)
- [the section called “【DMS.10】 Neptune 資料庫的 DMS 端點應啟用 IAM 授權”](#)
- [the section called “【DMS.11】 MongoDB 的 DMS 端點應啟用身分驗證機制”](#)
- [the section called “【DMS.12】 Redis OSS 的 DMS 端點應該已啟用 TLS”](#)
- [the section called “【DynamoDB.7】 DynamoDB Accelerator 叢集應在傳輸中加密”](#)
- [the section called “【EFS.6】 EFS 掛載目標不應與在啟動時指派公有 IP 地址的子網路相關聯”](#)
- [the section called “【EKS.3】 EKS 叢集應使用加密的 Kubernetes 秘密”](#)
- [the section called “【FSx.2】 FSx for Lustre 檔案系統應設定為將標籤複製到備份”](#)
- [the section called “【MQ.2】 ActiveMQ 代理程式應將稽核日誌串流至 CloudWatch”](#)

- [the section called “【MQ.3】 Amazon MQ 代理程式應該啟用自動次要版本升級”](#)
- [the section called “【Opensearch.11】 OpenSearch 網域應至少具有三個專用主節點”](#)
- [the section called “【Redshift.15】 Redshift 安全群組應僅允許從受限原始伺服器傳入叢集連接埠”](#)
- [the section called “【SageMaker.4】 SageMaker 端點生產變體的初始執行個體計數應大於 1”](#)
- [the section called “【Service Catalog.1】 Service Catalog 產品組合只能在 AWS 組織內共用”](#)
- [the section called “【Transfer.2】 Transfer Family 伺服器不應使用 FTP 通訊協定進行端點連線”](#)

[AWS 資源標記標準](#)

Security Hub CSPM [AWS 的資源標記標準](#) 現已正式推出，以及適用於標準的新控制項。

2024 年 4 月 30 日

[現有 受管政策的更新](#)

Security Hub CSPM 已更新名為的 [AWS 受管政策](#) `AmazonSecurityHubFullAccess`，以取得 AWS 服務 和 產品的定價詳細資訊。

2024 年 4 月 24 日

控制參數的內容內組態	如果您使用中央組態，您現在可以從 Security Hub CSPM 主控台上控制項的詳細資訊頁面，在 內容中設定控制項參數 。	2024 年 3 月 29 日
現有 受管政策的更新	Security Hub CSPM AWSSecurityHubReadOnlyAccess 透過新增Sid欄位來更新名為的 AWS 受管政策 。	2024 年 2 月 22 日
新的安全控制	控制項【Macie.2】應啟用的 Macie 自動化敏感資料探索 現已可用。如需此控制項的區域限制，請參閱 依區域的控制項可用性 。	2024 年 2 月 19 日
Security Hub CSPM 可在加拿大西部（卡加利）使用	Security Hub CSPM 現已在加拿大西部（卡加利）提供。所有 Security Hub CSPM 功能現在都可在此區域使用，但某些安全控制除外。如需詳細資訊，請參閱 依區域控制可用性 。	2023 年 12 月 20 日

新的安全控制

可使用下列新的 Security Hub CSPM 控制項：

2023 年 12 月 14 日

- [the section called “【Backup.1】 AWS Backup 復原點應靜態加密”](#)
- [the section called “【DynamoDB.6】 DynamoDB 資料表應該已啟用刪除保護”](#)
- [the section called “【EC2.51】 EC2 Client VPN 端點應該啟用用戶端連線記錄”](#)
- [the section called “【EKS.8】 EKS 叢集應該啟用稽核記錄”](#)
- [the section called “【EMR.2】 應啟用 Amazon EMR 封鎖公開存取設定”](#)
- [the section called “【FSx.1】 FSx for OpenZFS 檔案系統應設定為將標籤複製到備份和磁碟區”](#)
- [the section called “【Macie.1】 應啟用 Amazon Macie”](#)
- [the section called “【MSK.2】 MSK 叢集應已設定增強型監控”](#)
- [the section called “【Neptune.9】 Neptune 資料庫叢集應部署在多個可用區域”](#)

- [the section called “【NetworkFirewall.1】網路防火牆防火牆應部署在多個可用區域”](#)
- [the section called “【NetworkFirewall.2】應啟用網路防火牆記錄”](#)
- [the section called “【Opensearch.10】OpenSearch 網域應已安裝最新的軟體更新”](#)
- [the section called “【PCA.1】應停用 AWS 私有 CA 根憑證授權單位”](#)
- [the section called “【S3.19】S3 存取點應啟用封鎖公開存取設定”](#)
- [the section called “【S3.20】S3 一般用途儲存貯體應啟用 MFA 刪除”](#)

[尋找擴充功能](#)

Security Hub CSPM 將新的調查結果欄位 `AwsAccountName`、`ApplicationArn` 和 `ApplicationName` 新增至 AWS 安全調查結果格式 (ASFF)。

2023 年 11 月 27 日

[摘要儀表板的增強功能](#)

您現在可以在 Security Hub CSPM 主控台的摘要頁面上存取更多儀表板小工具，儲存儀表板篩選條件集以快速專注於特定安全問題，並自訂儀表板配置。

2023 年 11 月 27 日

[中央組態](#)

中央組態現已可用。使用中央組態，Security Hub CSPM 委派管理員可以跨多個組織帳戶、組織單位 (OUs) 和區域設定 Security Hub CSPM、標準和控制。

2023 年 11 月 27 日

[受管政策的更新項目](#)

Security Hub CSPM 為AWSSecurityHubServiceRolePolicy 受管政策新增了新的許可，允許 Security Hub CSPM 讀取和更新可自訂的安全控制屬性。

2023 年 11 月 26 日

[自訂控制參數](#)

您現在可以自訂特定 Security Hub CSPM 控制項的參數值。這可以對特定控制項提出更符合您業務需求和安全期望的問題清單。

2023 年 11 月 26 日

[受管政策的更新](#)

Security Hub CSPM 更新了AWSSecurityHubFullAccess 和AWSSecurityHubOrganizationsAccess 受管政策，分別允許您使用 Security Hub CSPM 功能以及與的整合 AWS Organizations。

2023 年 11 月 16 日

新增至服務受管標準的現有安全控制：AWS Control Tower

下列現有的 Security Hub CSPM 控制項已新增至服務受管標準：AWS Control Tower。

2023 年 11 月 14 日

- ACM.2
- AppSync.5
- CloudTrail.6
- DMS.9
- DocumentDB.3
- DynamoDB.3
- EC2.23
- EKS.1
- ElastiCache.3
- ElastiCache.4
- ElastiCache.5
- ElastiCache.6
- EventBridge.3
- KMS.4
- Lambda.3
- MQ.5
- MQ.6
- MSK.1
- RDS.12
- RDS.15
- S3.17

受管政策的更新項目

Security Hub CSPM 將新的標記許可新增至AWSSecurityHubServiceRolePolicy 受管政策，以允許 Security Hub CSPM 讀取與問題清單相關的資源標籤。

2023 年 11 月 7 日

新的安全控制

可使用下列新的 Security Hub CSPM 控制項：

2023 年 10 月 10 日

- [the section called “【AppSync.5】 AWS AppSync GraphQL APIs 不應使用 API 金鑰進行身分驗證”](#)
- [the section called “【DMS.6】 DMS 複寫執行個體應啟用自動次要版本升級”](#)
- [the section called “【DMS.7】 目標資料庫的 DMS 複寫任務應該已啟用記錄”](#)
- [the section called “【DMS.8】 來源資料庫的 DMS 複寫任務應該已啟用記錄”](#)
- [the section called “【DMS.9】 DMS 端點應使用 SSL”](#)
- [the section called “【DocumentDB.3】 Amazon DocumentDB 手動叢集快照不應公開”](#)
- [the section called “【DocumentDB.4】 Amazon DocumentDB 叢集應將稽核日誌發佈至 CloudWatch Logs”](#)
- [the section called “【DocumentDB.5】 Amazon](#)

DocumentDB 叢集應該啟用刪除保護”

- the section called “【ECS.9】 ECS 任務定義應具有記錄組態”
- the section called “【EventBridge.3】 EventBridge 自訂事件匯流排應連接以資源為基礎的政策”
- the section called “【EventBridge.4】 EventBridge 全域端點應啟用事件複寫”
- the section called “【MSK.1】 MSK 叢集應在代理程式節點之間傳輸時加密”
- the section called “【MQ.5】 ActiveMQ 代理程式應使用作用中/待命部署模式”
- the section called “【MQ.6】 RabbitMQ 代理程式應使用叢集部署模式”
- the section called “【NetworkFirewall.9】 網路防火牆防火牆應啟用刪除保護”
- the section called “【RDS.34】 Aurora MySQL 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs”
- the section called “【RDS.35】 RDS 資料庫叢集應該啟用自動次要版本升級”

- [the section called “【Route53.2】 Route 53 公有託管區域應記錄 DNS 查詢”](#)
- [the section called “【WAF.12】 AWS WAF 規則應啟用 CloudWatch 指標”](#)

[受管政策的更新項目](#)

Security Hub CSPM 將新的 Organizations 動作新增至AWSSecurityHubServiceRolePolicy 受管政策，以允許 Security Hub CSPM 擷取帳戶和組織單位 (OU) 資訊。我們也新增了新的 Security Hub CSPM 動作，允許 Security Hub CSPM 讀取和更新服務組態，包括標準和控制項。

2023 年 9 月 27 日

新增至服務受管標準的現有安全控制：AWS Control Tower

2023 年 9 月 26 日

下列現有的 Security Hub CSPM 控制項已新增至服務受管標準：AWS Control Tower。

- the section called
“【Athena.1】Athena 工作群組應靜態加密”
- the section called
“【DocumentDB.1】Amazon DocumentDB 叢集應靜態加密”
- the section called
“【DocumentDB.2】Amazon DocumentDB 叢集應具有足夠的備份保留期”
- the section called
“【Neptune.1】Neptune 資料庫叢集應靜態加密”
- the section called
“【Neptune.2】Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs”
- the section called
“【Neptune.3】Neptune 資料庫叢集快照不應公開”
- the section called
“【Neptune.4】Neptune 資料庫叢集應啟用刪除保護”
- the section called
“【Neptune.5】Neptune 資料庫叢集應該啟用自動備份”
- the section called
“【Neptune.6】Neptune 資料庫叢集快照應靜態加密”

- [the section called “【Neptune.7】 Neptune 資料庫叢集應該啟用 IAM 資料庫身分驗證”](#)
- [the section called “【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照”](#)
- [the section called “【RDS.27】 RDS 資料庫叢集應靜態加密”](#)

[中可用的合併控制項檢視和合併控制項問題清單 AWS GovCloud \(US\)](#)

合併控制項檢視和合併控制項調查結果現在可在 中 使用 AWS GovCloud (US) Region。Security Hub CSPM 主控台的控制項頁面會顯示跨標準的所有控制項。每個控制項在標準之間都有相同的控制 ID。當您開啟合併控制問題清單時，即使控制項適用於多個啟用的標準，您也會收到每個安全檢查的單一問題清單。

2023 年 9 月 6 日

[中國區域提供的合併控制項檢視和合併控制項調查結果](#)

合併控制項檢視和合併控制項調查結果現在可於中國區域使用。Security Hub CSPM 主控台的控制項頁面會顯示跨標準的所有控制項。每個控制項在標準之間都有相同的控制 ID。當您開啟合併控制問題清單時，即使控制項適用於多個啟用的標準，您也會收到每個安全檢查的單一問題清單。

2023 年 8 月 28 日

[以色列（特拉維夫）區域提供 Security Hub CSPM](#)

Security Hub CSPM 現已在以色列（特拉維夫）提供。所有 Security Hub CSPM 功能現在都可在此區域使用，但某些安全控制除外。如需詳細資訊，請參閱[依區域控制可用性](#)。

2023 年 8 月 8 日

新的安全控制

可使用下列新的 Security Hub CSPM 控制項：

2023 年 7 月 28 日

- [the section called “【Athena.1】 Athena 工作群組應靜態加密”](#)
- [the section called “【DocumentDB.1】 Amazon DocumentDB 叢集應靜態加密”](#)
- [the section called “【DocumentDB.2】 Amazon DocumentDB 叢集應具有足夠的備份保留期”](#)
- [the section called “【Neptune.1】 Neptune 資料庫叢集應靜態加密”](#)
- [the section called “【Neptune.2】 Neptune 資料庫叢集應將稽核日誌發佈至 CloudWatch Logs”](#)
- [the section called “【Neptune.3】 Neptune 資料庫叢集快照不應公開”](#)
- [the section called “【Neptune.4】 Neptune 資料庫叢集應啟用刪除保護”](#)
- [the section called “【Neptune.5】 Neptune 資料庫叢集應該啟用自動備份”](#)
- [the section called “【Neptune.6】 Neptune 資料庫叢集快照應靜態加密”](#)
- [the section called “【Neptune.7】 Neptune 資](#)

[料庫叢集應該啟用 IAM 資料庫身分驗證”](#)

- [the section called “【Neptune.8】 Neptune 資料庫叢集應設定為將標籤複製到快照”](#)
- [the section called “【RDS.27】 RDS 資料庫叢集應靜態加密”](#)

[自動化規則條件的新運算子](#)

您現在可以將 CONTAINS 和 NOT_CONTAINS 比較運算子用於自動化規則映射和字串條件。

2023 年 7 月 25 日

[自動化規則](#)

Security Hub CSPM 現在提供自動化規則，可根據您指定的條件自動更新問題清單。

2023 年 6 月 13 日

[新的第三方整合](#)

Snyk 是一種新的第三方整合，可將問題清單傳送至 Security Hub CSPM。

2023 年 6 月 12 日

新增至服務受管標準的現有安全控制：AWS Control Tower

2023 年 6 月 12 日

下列現有的 Security Hub CSPM 控制項已新增至服務受管標準：AWS Control Tower。

- the section called “【Account.1】應針對提供安全性聯絡資訊 AWS 帳戶”
- the section called “【APIGateway.8】API Gateway 路由應指定授權類型”
- the section called “【APIGateway.9】應為 API Gateway V2 階段設定存取記錄”
- the section called “【CodeBuild.3】CodeBuild S3 日誌應加密”
- the section called “【EC2.25】Amazon EC2 啟動範本不應將公IPs 指派給網路介面”
- the section called “【ELB.1】Application Load Balancer 應設定為將所有 HTTP 請求重新導向至 HTTPS”
- the section called “【Redshift.10】應靜態加密 Redshift 叢集”
- the section called “【SageMaker.2】應在自訂 VPC 中啟動 SageMaker 筆記本執行個體”

- [the section called “【SageMaker.3】使用者不應擁有 SageMaker 筆記本執行個體的根存取權”](#)
- [the section called “【WAF.10】AWS WAF Web ACLs 應至少有一個規則或規則群組”](#)

[新的安全控制](#)

可使用下列新的 Security Hub CSPM 控制項：

2023 年 6 月 6 日

- [the section called “【ACM.2】由 ACM 管理的 RSA 憑證應使用至少 2,048 位元的金鑰長度”](#)
- [the section called “【AppSync.2】AWS AppSync 應該啟用欄位層級記錄”](#)
- [the section called “【CloudFront.13】CloudFront 分佈應使用原始存取控制”](#)
- [the section called “【Elastic Beanstalk.3】Elastic Beanstalk 應將日誌串流至 CloudWatch”](#)
- [the section called “【S3.17】S3 一般用途儲存貯體應使用靜態加密 AWS KMS keys”](#)
- [the section called “【StepFunctions.1】Step Functions 狀態機器應該已開啟記錄”](#)

[亞太區域（墨爾本）提供 Security Hub CSPM](#)

Security Hub CSPM 現已在亞太區域（墨爾本）提供。所有 Security Hub CSPM 功能現在都可在此區域使用，但某些安全控制除外。如需詳細資訊，請參閱[依區域控制可用性](#)。

2023 年 5 月 25 日

[尋找歷史記錄](#)

Security Hub CSPM 現在可以追蹤過去 90 天內的問題清單歷史記錄。

2023 年 5 月 4 日

[新的安全控制](#)

可使用下列新的 Security Hub CSPM 控制項：

2023 年 3 月 29 日

- [the section called “【EKS.1】不應公開存取 EKS 叢集端點”](#)
- [the section called “【ELB.16】Application Load Balancer 應與 AWS WAF Web ACL 建立關聯”](#)
- [the section called “【Redshift.10】應靜態加密 Redshift 叢集”](#)
- [the section called “【S3.15】S3 一般用途儲存貯體應啟用物件鎖定”](#)

[擴展對合併控制問題清單的支援](#)

[v2 AWS .0.0 上的自動化安全回應](#)現在支援合併的控制問題清單。

2023 年 3 月 24 日

[Security Hub CSPM 可在新中使用 AWS 區域](#)

Security Hub CSPM 現已在亞太區域（海德拉巴）、歐洲（西班牙）和歐洲（蘇黎世）提供。這些區域中可用的控制項存在限制。

2023 年 3 月 21 日

[受管政策的更新](#)

Security Hub CSPM 已更新AWSSecurityHubServiceRolePolicy 受管政策中的現有許可。

2023 年 3 月 17 日

NIST 800-53 標準的新安全控制

Security Hub CSPM 已新增下列適用於 NIST 800-53 標準的安全控制：

2023 年 3 月 3 日

- the section called
“【Account.2】 AWS 帳戶
應該是 AWS Organizations
組織的一部分”
- the section called
“【CloudWatch.15]
CloudWatch 警示應已設定指
定的動作”
- the section called
“【CloudWatch.16]
CloudWatch 日誌群組應保留
一段指定的時間”
- the section called
“【CloudWatch.17] 應啟用
CloudWatch 警示動作”
- the section called
“【DynamoDB.4]
DynamoDB 資料表應存在於
備份計畫中”
- the section called
“【EC2.28】 備份計畫應涵
蓋 EBS 磁碟區”
- EC2.29 – EC2 執行個體應在 VPC 中啟動（已淘汰）
- the section called
“【RDS.26】 RDS 資料庫執
行個體應受備份計劃保護”
- the section called
“【S3.14】 S3 一般用途儲存
貯體應該已啟用版本控制”

- [the section called “【WAF.11】應該啟用 AWS WAF Web ACL 記錄”](#)

[國家標準技術研究所 \(NIST\) 800-53 修訂版 5](#)

Security Hub CSPM 現在支援具有超過 200 個適用安全控制的 NIST 800-53 修訂版 5 標準。

2023 年 2 月 28 日

[合併控制項檢視和控制問題清單](#)

隨著合併控制項檢視的發行，Security Hub CSPM 主控台的控制項頁面會顯示跨標準的所有控制項。每個控制項在標準之間都有相同的控制 ID。當您開啟合併控制問題清單時，即使控制項適用於多個啟用的標準，您也會收到每個安全檢查的單一問題清單。

2023 年 2 月 23 日

新的安全控制

下列新的 Security Hub CSPM 控制項可供使用。有些控制項具有區域限制。

2023 年 2 月 16 日

- [the section called “【Elasticache.1\] Elasticache \(Redis OSS\) 叢集應該啟用自動備份”](#)
- [the section called “【Elasticache.2\] Elasticache 叢集應該啟用自動次要版本升級”](#)
- [the section called “【Elasticache.3\] Elasticache 複寫群組應該啟用自動容錯移轉”](#)
- [the section called “【Elasticache.4\] Elasticache 複寫群組應靜態加密”](#)
- [the section called “【Elasticache.5\] Elasticache 複寫群組應在傳輸中加密”](#)
- [the section called “【Elasticache.6\] 舊版的 Elasticache \(Redis OSS\) 複寫群組應該已啟用 Redis OSS AUTH”](#)
- [the section called “【Elasticache.7\] Elasticache 叢集不應使用預設子網路群組”](#)

新的 ASFF 欄位

Security Hub CSPM 已將 ProductFields.ArchivalReasons:0/Description 和 ProductFields.ArchivalReasons:0/ReasonCode 新增至 AWS 安全調查結果格式 (ASFF)。

2023 年 2 月 8 日

新的 ASFF 欄位	Security Hub CSPM 已將 Compliance.AssociatedStandards 和 Compliance.SecurityControlId 新增至 AWS Security Finding Format (ASFF)。	2023 年 1 月 31 日
漏洞詳細資訊現已推出	您現在可以在 Security Hub CSPM 主控台中查看漏洞詳細資訊，了解 Amazon Inspector 傳送給 Security Hub CSPM 的問題清單。	2023 年 1 月 14 日
Security Hub CSPM 可在中東（阿拉伯聯合大公國）使用	Security Hub CSPM 現已在中東（阿拉伯聯合大公國）提供。有些控制項具有區域限制。	2023 年 1 月 12 日
新增與 的第三方整合 MetricStream	Security Hub CSPM 現在支援在中國和 以外的MetricStream 所有區域中與 進行第三方整合 AWS GovCloud (US)。	2023 年 1 月 11 日
提高組織帳戶限制	Security Hub CSPM 現在支援每個區域每個 Security Hub CSPM 管理員帳戶最多 11,000 個成員帳戶。	2022 年 12 月 27 日
ElasticBeanstalk.3 復原	Security Hub CSPM 復原了控制項 【ElasticBeanstalk.3] Elastic Beanstalk 應該從所有區域中的 FSBP 標準將日誌串流到 CloudWatch。	2022 年 12 月 21 日
Security Hub CSPM 新增了新的安全控制	新的 Security Hub CSPM 控制項可供已啟用 FSBP 標準的客戶使用。有些控制項具有 區域限制 。	2022 年 12 月 15 日

即將推出功能的指引	Security Hub CSPM 計劃發佈兩個新功能：合併控制檢視和合併控制問題清單。這些即將推出的功能可能會影響依賴控制調查結果欄位和值的現有工作流程。	2022 年 12 月 9 日
Amazon Security Lake 整合現已推出	Security Lake 現在透過接收 Security Hub CSPM 調查結果來與 Security Hub CSPM 整合。	2022 年 11 月 29 日
支援服務受管標準：AWS Control Tower	Security Hub CSPM 支援稱為 Service-Managed Standard 的新安全標準 AWS Control Tower。AWS Control Tower 管理此標準。	2022 年 11 月 28 日
CIS AWS Foundations Benchmark 1.4.0 版現已在中國區域提供	Security Hub CSPM 現在在中國區域支援 CIS AWS Foundations Benchmark 1.4.0 版。	2022 年 11 月 18 日
Jira Service Management Cloud 整合現已推出	Jira Service Management Cloud 現在會在所有可用區域中接收 Security Hub CSPM 調查結果，但中國區域除外。	2022 年 11 月 17 日
AWS IoT Device Defender 整合現已推出	AWS IoT Device Defender 現在會將問題清單傳送至所有可用區域中的 Security Hub CSPM。	2022 年 11 月 17 日
支援 CIS AWS Foundations Benchmark 1.4.0 版	Security Hub CSPM 現在提供支援 CIS AWS Foundations Benchmark v1.4.0 的安全控制。此標準適用於所有可用區域，但中國區域除外。	2022 年 11 月 9 日

支援 中的 Security Hub CSPM 公告 AWS GovCloud (US)	您現在可以使用 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 中的 Amazon Simple Notification Service (Amazon SNS) 訂閱 Security Hub CSPM 公告，以接收有關 Security Hub CSPM 的通知。	2022 年 10 月 3 日
AWS Security Hub CSPM 新增了新的安全控制	新的 Security Hub CSPM 控制 AutoScaling.9 可供已啟用 FSBP 標準的客戶使用。控制項可能有 區域限制 。	2022 年 9 月 1 日
訂閱 Security Hub CSPM 公告	您現在可以使用 Amazon Simple Notification Service (Amazon SNS) 訂閱 Security Hub CSPM 公告，以接收有關 Security Hub CSPM 的通知。	2022 年 8 月 29 日
跨區域彙總的區域擴展	跨區域彙總現在可用於 問題清單、問題清單更新和洞見 AWS GovCloud (US)。	2022 年 8 月 2 日
新的第三方產品整合	Fortinet - FortiCNP 是接收 Security Hub CSPM 調查結果的第三方整合，而 JFrog 是將調查結果傳送至 Security Hub CSPM 的第三方整合。	2022 年 7 月 26 日
EC2.27 已淘汰	Security Hub CSPM 已淘汰 EC2.27 - 執行 EC2 執行個體不應使用金鑰對，這是基礎安全最佳實務 (FSBP) 標準中的 AWS 先前控制項。	2022 年 7 月 20 日

Lambda.2 不再支援 python3.6	Security Hub CSPM 不再支援 python3.6 作為 Lambda.2 的參數 - Lambda 函數應使用支援的執行期，這是 AWS 基礎安全最佳實務 (FSBP) 標準中的控制項。	2022 年 7 月 19 日
AWS Security Hub CSPM 新增了新的安全控制	新的 Security Hub CSPM 控制項可供已啟用 FSBP 標準的客戶使用。有些控制項具有 區域限制 。	2022 年 6 月 22 日
AWS Security Hub CSPM 支援新區域	Security Hub CSPM 現已在亞太區域（雅加達）提供。某些控制項不適用於此區域。	2022 年 6 月 7 日
改善 AWS Security Hub CSPM 與 之間的整合 AWS Config	Security Hub CSPM 使用者可以將 AWS Config 規則評估的結果視為 Security Hub CSPM 中的調查結果。	2022 年 6 月 6 日
新增選擇退出自動啟用標準的功能	對於已與整合的使用者 AWS Organizations，此功能可讓您登入 Security Hub CSPM 管理員帳戶，並從自動啟用的標準中選擇新的成員帳戶。	2022 年 4 月 25 日
擴展的跨區域彙總	新增跨區域彙總以控制狀態和安全性分數。	2022 年 4 月 20 日
CompanyName 和 ProductName 現在是頂層屬性	新增了新的最上層屬性，用於設定與自訂整合相關聯的公司和產品名稱	2022 年 4 月 1 日
將新控制項新增至 AWS 基礎安全最佳實務標準	將 5 個新控制項新增至 AWS 基礎安全最佳實務標準。	2022 年 3 月 31 日

新增資源詳細資訊物件至 ASFF	已將AwsRdsDbSecurityGroup 資源類型新增至 ASFF。	2022 年 3 月 25 日
在 ASFF 中新增其他資源詳細資訊	新增其他詳細資訊至 AwsAutoScalingScalingGroup 、 AwsRedshiftCluster 、 AwsElasticLoadBalancer 和 AwsCodeBuildProject 。	2022 年 3 月 25 日
將新控制項新增至 AWS 基礎安全最佳實務標準	將 15 個新控制項新增至 AWS 基礎安全最佳實務標準。	2022 年 3 月 16 日
將新控制項新增至 AWS 基礎安全最佳實務標準和支付卡產業資料安全標準 (PCI DSS)	將 Amazon OpenSearch Service、Amazon RDS、Amazon EC2、Elastic Load Balancing 和 CloudFront AWS 的新控制項新增至基礎安全最佳實務標準。也為 PCI DSS 新增了兩個新的 OpenSearch Service 控制項。	2022 年 2 月 15 日
已將新欄位新增至 ASFF	新增欄位：範例。	2022 年 1 月 26 日
新增與 的整合 AWS Health	AWS Health 使用service-to-service事件傳訊，將問題清單傳送至 Security Hub CSPM。	2022 年 1 月 19 日
新增與 的整合 AWS Trusted Advisor	Trusted Advisor 會將檢查結果作為 Security Hub CSPM 調查結果傳送至 Security Hub CSPM。Security Hub CSPM 會將其 AWS 基礎安全最佳實務檢查的結果傳送至 Trusted Advisor。	2022 年 1 月 18 日

[更新 ASFF 中的資源詳細資訊物件](#)

新增了 MixedInstancesPolicy 和 AvailabilityZones 至 AwsAutoScalingAutoScalingGroup 。已新增 MetadataOptions 到 AwsAutoScalingLaunchConfiguration 。已新增 BucketVersioningConfiguration 到 AwsS3Bucket 。

2021 年 12 月 20 日

[更新 ASFF 文件的輸出](#)

ASFF 屬性的說明先前是在單一主題中。每個最上層物件和每個資源詳細資訊物件現在都位於自己的主題中。ASFF 語法主題包含這些主題的連結。

2021 年 12 月 20 日

[已將新的資源詳細資訊物件新增至的 ASFF AWS Network Firewall](#)

針對 AWS Network Firewall 新增下列資源詳細資訊物件：AwsNetworkFirewallFirewall 、 AwsNetworkFirewallPolicy 和 AwsNetworkFirewallRuleGroup 。

2021 年 12 月 20 日

[新增對新版本 Amazon Inspector 的支援](#)

Security Hub CSPM 已與新版本的 Amazon Inspector 以及 Amazon Inspector Classic 整合。Amazon Inspector 會將問題清單傳送至 Security Hub CSPM。

2021 年 11 月 29 日

[變更 EC2.19 的嚴重性](#)

EC2.19 的嚴重性（安全群組不應允許無限制存取高風險的連接埠）從高變更為嚴重。

2021 年 11 月 17 日

與 的新整合 Sonrai Dig	Security Hub CSPM 現在提供與 的整合Sonrai Dig。 Sonrai Dig會監控雲端環境以識別安全風險。 Sonrai Dig會將問題清單傳送至 Security Hub CSPM。	2021 年 11 月 12 日
更新 CIS 2.1 和 CloudTrail.1 控制項的檢查	除了檢查至少一個多區域 CloudTrail 線索已就地，CIS 2.1 和 CloudTrail.1 現在也會檢查至少一個多區域 CloudTrail 線索中的 ExcludeManagementEventSources 參數是否為空。	2021 年 11 月 9 日
新增對 VPC 端點的支援	Security Hub CSPM 現在已與整合 AWS PrivateLink，並支援 VPC 端點。	2021 年 11 月 3 日
將控制項新增至 AWS 基礎安全最佳實務標準	新增 Elastic Load Balancing (ELB.2 和 ELB.8) 和 AWS Systems Manager (SSM.4) 的新控制項。	2021 年 11 月 2 日
已將連接埠新增至 EC2.19 控制項的檢查	EC2.19 現在也會檢查安全群組是否不允許無限制存取下列連接埠：3000 (Go、Node.js 和 Ruby Web 開發架構)、5000 (Python Web 開發架構)、8088 (舊版 HTTP 連接埠) 和 8888 (替代 HTTP 連接埠)	2021 年 10 月 27 日

[新增與 Logz.io Cloud SIEM 的整合](#)

Logz.io 是雲端 SIEM 的供應商，可提供日誌和事件資料的進階相互關聯，以協助安全團隊即時偵測、分析和回應安全威脅。Logz.io 會收到 Security Hub CSPM 的問題清單。

2021 年 10 月 25 日

[新增對問題清單跨區域彙總的支援](#)

跨區域彙總可讓您檢視所有調查結果，而無需變更區域。管理員帳戶選擇彙總區域和連結的區域。管理員帳戶及其成員帳戶的問題清單會從連結的區域彙總到彙總區域。

2021 年 10 月 20 日

[更新 ASFF 中的資源詳細資訊物件](#)

已將檢視器憑證詳細資訊新增至 `AwsCloudFrontDistribution`。已新增其他詳細資訊至 `AwsCodeBuildProject`。已將負載平衡器屬性新增至 `AwsElasticLoadBalancer`。已將 S3 儲存貯體擁有者帳戶識別符新增至 `AwsS3Bucket`。

2021 年 10 月 8 日

[新增資源詳細資訊物件至 ASFF](#)

已將下列新資源詳細資訊物件新增至 ASFF：`AwsEc2VpcEndpointService`、`AwsEcrRepository`、`AwsEksCluster`、`AwsOpenSearchServiceDomain`、`AwsWafRateBasedRule`、`AwsWafRegionalRateBasedRule`、`AwsXrayEncryptionConfig`

2021 年 10 月 8 日

從 Lambda.2 控制項中移除已取代的執行時間	在 AWS 基礎安全最佳實務標準中，從 【Lambda.2】 Lambda 函數移除 dotnetcore2.1 執行期應使用支援的執行期。	2021 年 10 月 6 日
檢查點整合的新名稱	與 Check Point Dome9 Arc 的整合現在是 Check Point CloudGuard Posture Management。整合 ARN 並未變更。	2021 年 10 月 1 日
已移除與 Alcide 的整合	與 Alcide kAudit 的整合已停止。	2021 年 9 月 30 日
變更 EC2.19 的嚴重性	【EC2.19】 安全群組的嚴重性不應允許無限制存取高風險的連接埠，從中變更為高。	2021 年 9 月 30 日
中國區域 AWS Organizations 現在支援與整合	中國（北京）和中國（寧夏）現在支援 Security Hub CSPM 與 Organizations 的整合。	2021 年 9 月 20 日
S3.1 和 PCI.S3.6 控制項的新 AWS Config 規則	S3.1 和 PCI.S3.6 都確認已啟用 Amazon S3 封鎖公開存取設定。這些控制項的 AWS Config 規則會從 變更為 s3-account-level-public-access-blocks s3-account-level-public-access-blocks-periodic。	2021 年 9 月 14 日

[從 Lambda.2 控制項中移除已取代的執行時間](#)

在 AWS 基礎安全最佳實務標準中，從 **【Lambda.2】** Lambda 函數移除 nodejs10.x 和 ruby2.5 執行時間，應使用支援的執行時間。

2021 年 9 月 13 日

[變更 CIS 2.2 控制項的嚴重性](#)

在 CIS AWS Foundations Benchmark 標準中，2.2 的嚴重性。– 確保 CloudTrail 日誌檔案驗證已啟用，從低變更為中。

2021 年 9 月 13 日

[更新 AWS 基礎安全最佳實務標準中的 ECS.1、Lambda.2 和 SSM.1](#)

在 AWS 基礎安全最佳實務標準中，ECS.1 現在具有設定為的 `SkipInactiveTaskDefinitions` 參數。true 這可確保控制項只會檢查作用中的任務定義。對於 Lambda.2，已將 Python 3.9 新增至執行時間清單。SSM.1 現在會檢查已停止和執行中的執行個體。

2021 年 9 月 7 日

[PCI.Lambda.2 控制項現在排除 Lambda@Edge 資源](#)

在支付卡產業資料安全標準 (PCI DSS) 標準中，PCI.Lambda.2 控制項現在會排除 Lambda@Edge 資源。

2021 年 9 月 7 日

[新增與的整合 HackerOne Vulnerability Intelligence](#)

Security Hub CSPM 現在提供與的整合 HackerOne Vulnerability Intelligence。整合會將問題清單傳送至 Security Hub CSPM。

2021 年 9 月 7 日

[更新 ASFF 中的資源詳細資訊物件](#)

對於 `AwsKmsKey`，已新增 `KeyRotationStatus`。
對於 `AwsS3Bucket`，已新增 `AccessControlList`、`BucketNotificationConfiguration`、`BucketLoggingConfiguration` 和 `BucketWebsiteConfiguration`。

2021 年 9 月 2 日

[新增資源詳細資訊物件至 ASFF](#)

已將下列新資源詳細資訊物件新增至 ASFF：`AwsAutoScalingLaunchConfiguration`、`AwsEc2VpnConnection` 和 `AwsEcrContainerImage`。

2021 年 9 月 2 日

[在 ASFF 中將詳細資訊新增至 Vulnerabilities 物件](#)

在 `Cvss` 中，新增了 `Adjustments` 和 `Source`。
在 `VulnerablePackages`，新增檔案路徑和套件管理員。

2021 年 9 月 2 日

[中國區域現在支援 Systems Manager Explorer 和 OpsCenter 整合](#)

中國（北京）和中國（寧夏）現在支援 Security Hub CSPM 與 SSM Explorer 和 OpsCenter 整合。

2021 年 8 月 31 日

[淘汰 Lambda.4 控制項](#)

Security Hub CSPM 正在淘汰控制項 **【Lambda.4】**。Lambda 函數應該設定無效字母佇列。控制項淘汰時，不會再顯示在主控台上，而且 Security Hub CSPM 不會對其執行檢查。

2021 年 8 月 31 日

淘汰 PCI.EC2.3 控制項	Security Hub CSPM 正在淘汰控制項【PCI.EC2.3】應該移除未使用的 EC2 安全群組。控制項淘汰時，不會再顯示在主控台上，而且 Security Hub CSPM 不會對其執行檢查。	2021 年 8 月 27 日
變更 Security Hub CSPM 將調查結果傳送至自訂動作的方式	當您將問題清單傳送至自訂動作時，Security Hub CSPM 現在會在個別 Security Hub Findings - Custom Action 事件中傳送每個問題清單。	2021 年 8 月 20 日
新增自訂 Lambda 執行時間的新合規狀態原因代碼	新增新的 LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE 合規狀態原因代碼。此原因代碼表示 Security Hub CSPM 無法對自訂 Lambda 執行時間執行檢查。	2021 年 8 月 20 日
AWS Firewall Manager 中國區域現在支援 整合	中國（北京）和中國（寧夏）現在支援 Security Hub CSPM 與 Firewall Manager 的整合。	2021 年 8 月 19 日
與 Caveonix Cloud 和 的新整合 Forcepoint Cloud Security Gateway	Security Hub CSPM 現在提供與 Caveonix Cloud 和 的整合 Forcepoint Cloud Security Gateway。兩個整合都會將問題清單傳送至 Security Hub CSPM。	2021 年 8 月 10 日

[已將新的 ProductName 、
CompanyName 和 Region 屬性新增至 ASFF](#)

已將 ProductName 、 CompanyName 和 Region 欄位新增至 ASFF 的最上層。這些欄位會自動填入，除了自訂產品整合之外，無法使用 BatchImportFindings 或更新BatchUpdateFindings 。在 主控台上，尋找篩選條件會使用這些新欄位。在 API 中， CompanyName 和 ProductName 篩選條件會使用 下的屬性ProductFields 。

2021 年 7 月 23 日

[在 ASFF 中新增和更新資源詳細資訊物件](#)

新增了新的AwsRdsEventSubscription 資源類型和資源詳細資訊。新增資源類型的AwsEcsService 資源詳細資訊。已將屬性新增至AwsElasticsearchDomain 資源詳細資訊物件。

2021 年 7 月 23 日

[將控制項新增至 AWS 基礎安全最佳實務標準](#)

新增了 Amazon API Gateway (APIGateway.5)、Amazon EC2 (EC2.19)、Amazon ECS (ECS.2)、Elastic Load Balancing (ELB.7)、Amazon OpenSearch Service (ES.5 到 ES.8)、Amazon RDS (RDS.16 到 RDS.23)、Amazon Redshift (Redshift.4) 和 Amazon SQS (SQS.1) 的新控制項。

2021 年 7 月 20 日

[在服務連結角色受管政策中移動許可](#)

在受管政策中移動 `config:PutEvaluations` 許可 `AWSSecurityHubServiceRolePolicy`，以便將其套用至所有資源。

2021 年 7 月 14 日

[將控制項新增至 AWS 基礎安全最佳實務標準](#)

新增了 Amazon API Gateway (APIGateway.4)、Amazon CloudFront (CloudFront.5 和 CloudFront.6)、Amazon EC2 (EC2.17 和 EC2.18)、Amazon ECS (ECS.1)、Amazon OpenSearch Service (ES.4)、AWS Identity and Access Management (IAM.21)、Amazon RDS (RDS.15) 和 Amazon S3 (S3.8) 的新控制項。

2021 年 7 月 8 日

[新增控制問題清單的新合規狀態原因代碼](#)

`INTERNAL_SERVICE_ERROR` 表示發生未知錯誤。
`SNS_TOPIC_CROSS_ACCOUNT` 表示 SNS 主題是由不同的帳戶所擁有。
`SNS_TOPIC_INVALID` 表示相關聯的 SNS 主題無效。

2021 年 7 月 6 日

[在聊天應用程式中新增與 Amazon Q Developer 的整合](#)

在聊天應用程式中新增與 Amazon Q Developer 的整合。Security Hub CSPM 會在聊天應用程式中將調查結果傳送至 Amazon Q Developer。

2021 年 6 月 30 日

[已將新許可新增至服務連結角色受管政策](#)

已將新許可新增至 受管政策AWSecurityHubServiceRolePolicy，以允許服務連結角色將評估結果交付至其中 AWS Config。

2021 年 6 月 29 日

[ASFF 中新增和更新的資源詳細資訊物件](#)

新增 ECS 叢集和 ECS 任務定義的資源詳細資訊物件。更新 EC2 執行個體物件以列出相關聯的網路介面。新增 API Gateway V2 階段的用戶端憑證 ID。新增 S3 儲存貯體的生命週期組態。

2021 年 6 月 24 日

[更新彙總控制狀態和標準安全分數的計算](#)

Security Hub CSPM 現在每 24 小時計算一次整體控制狀態和標準安全分數。對於管理員帳戶，分數現在會反映每個帳戶是否啟用或停用每個控制項。

2021 年 6 月 23 日

[更新有關暫停帳戶之 Security Hub CSPM 處理的資訊](#)

新增 Security Hub CSPM 如何處理在 中暫停的帳戶的相關資訊 AWS。

2021 年 6 月 23 日

[新增標籤以顯示個別管理員帳戶的啟用和停用控制項](#)

對於管理員帳戶，標準詳細資訊頁面上的主要標籤包含跨帳戶彙總的資訊。此帳戶啟用的新帳戶和此帳戶停用索引標籤會列出個別管理員帳戶啟用或停用的帳戶。

2021 年 6 月 23 日

[已java8.a12 新增至 的參數 Lambda.2](#)

在 AWS 基礎安全最佳實務標準中，已java8.a12 新增至Lambda.2控制項支援的執行時間。

2021 年 6 月 8 日

[與 MicroFocus ArcSight 和 NETSCOUT 網路調查員的新整合](#)

新增與 MicroFocus ArcSight 和 NETSCOUT 網路調查員的整合。MicroFocus ArcSight 會從 Security Hub CSPM 接收問題清單。NETSCOUT 網路調查人員會將問題清單傳送至 Security Hub CSPM。

2021 年 6 月 7 日

[新增的詳細資訊 AWSSecurityHubServiceRolePolicy](#)

已更新 受管政策區段，以新增現有 受管政策 的詳細資訊 AWSSecurityHubServiceRolePolicy，供 Security Hub CSPM 服務連結角色使用。

2021 年 6 月 4 日

[與 Jira Service Management 的新整合](#)

適用於 Jira 的 AWS Service Management Connector 會將問題清單傳送至 Jira，並使用它們來建立 Jira 問題。更新 Jira 問題時，也會更新 Security Hub CSPM 中的對應調查結果。

2021 年 5 月 26 日

[更新亞太區域（大阪）區域的支援控制清單](#)

更新 CIS AWS Foundations 標準和支付卡產業資料安全標準 (PCI DSS)，以指出亞太區域（大阪）不支援的控制項。

2021 年 5 月 21 日

[與雲端 Sysdig Secure 的新整合](#)

新增與 Sysdig Secure for cloud 的整合。整合會將問題清單傳送至 Security Hub CSPM。

2021 年 5 月 14 日

[已將控制項新增至 AWS 基礎安全最佳實務標準](#)

新增了 Amazon API Gateway (APIGateway.2 和 APIGateway.3), AWS CloudTrail (CloudTrail.4 和 CloudTrail.5), Amazon EC2 (EC2.15 和 EC2.16)、 AWS Elastic Beanstalk (ElasticBeanstalk.1 和 ElasticBeanstalk.2), AWS Lambda (Lambda.4)、 Amazon RDS (RDS.12 – RDS.14)、 Amazon Redshift (Redshift.7) AWS Secrets Manager (SecretsManager.3 和 SecretsManager.4), 和 AWS WAF (WAF.1) 的新控制項。

2021 年 5 月 10 日

[GuardDuty 和 Amazon RDS 控制項的更新](#)

將 GuardDuty.1 和 的嚴重性 PCI.GuardDuty.1 從中變更為高。已將 databaseEngines 參數新增至 RDS.8。

2021 年 5 月 4 日

[已將新資源詳細資訊新增至 ASFF](#)

在 Resources.Details 中，新增了 Amazon EC2 網路 ACLs、 Amazon EC2 子網路和 AWS Elastic Beanstalk 環境的新資源詳細資訊物件。

2021 年 5 月 3 日

[新增主控台欄位，以提供 Amazon EventBridge 規則的篩選條件值](#)

Security Hub CSPM EventBridge 規則的新預先定義篩選模式提供主控台欄位，您可以用來指定篩選值。

2021 年 4 月 30 日

[新增與 AWS Systems Manager Explorer 和 OpsCenter 的整合](#)

Security Hub CSPM 現在支援與 Systems Manager Explorer 和 OpsCenter 整合。整合會從 Security Hub CSPM 接收調查結果，並在 Security Hub CSPM 中更新這些調查結果。

2021 年 4 月 26 日

[產品整合的新類型](#)

新的整合類型 UPDATE_FINDINGS_IN_SECURITY_HUB 表示產品整合會更新從 Security Hub CSPM 收到的調查結果。

2021 年 4 月 22 日

[已將「主帳戶」一詞變更為「管理員帳戶」。](#)

「主帳戶」一詞變更為「管理員帳戶」。術語也會在 Security Hub CSPM 主控台和 API 中變更。

2021 年 4 月 22 日

[更新 APIGateway.1 以將 HTTP 取代為 Websocket](#)

更新 APIGateway.1. 控制項現在會檢查 Websocket API 執行記錄，而不是 HTTP API 執行記錄。

2021 年 4 月 9 日

[北京和寧夏現在支援 Amazon GuardDuty 整合](#)

中國（北京）和中國（寧夏）區域現在支援 Security Hub CSPM 與 GuardDuty 整合。

2021 年 4 月 5 日

[已nodejs14.x 新增至 Lambda.2 控制項支援的執行時間](#)

基礎安全最佳實務標準中的 Lambda.2 控制項現在支援nodejs14.x 執行期。

2021 年 3 月 30 日

[Security Hub CSPM 已在亞太區域（大阪）推出](#)

Security Hub CSPM 現已在亞太區域（大阪）區域提供。

2021 年 3 月 29 日

[新增調查結果提供者欄位至調查結果詳細資訊](#)

在調查結果詳細資訊面板上，新的調查結果提供者欄位區段包含調查結果提供者值，用於可信度、重要性、相關調查結果、嚴重性和類型。

2021 年 3 月 24 日

[新增從 Amazon Macie 接收敏感問題清單的選項](#)

與 Macie 的整合現在可以設定為將敏感問題清單傳送至 Security Hub CSPM。

2021 年 3 月 23 日

[轉換為 AWS Organizations 以進行帳戶管理](#)

對於具有成員帳戶之現有管理員帳戶的客戶，新增了有關如何透過邀請從管理帳戶變更為使用 Organizations 管理帳戶的新資訊。

2021 年 3 月 22 日

[ASFF 中的新物件，以取得 Amazon S3 公有存取區塊組態的相關資訊](#)

在 `Resources`，新的 `AwsS3AccountPublicAccessBlock` 資源類型和詳細資訊物件提供帳戶 Amazon S3 公開存取區塊組態的相關資訊。在 `AwsS3Bucket` 資源詳細資訊物件中，`PublicAccessBlockConfiguration` 物件會提供 S3 儲存體的公有存取區塊組態。

2021 年 3 月 18 日

ASFF 中的新物件，以允許調查結果提供者更新特定欄位	ASFF 中的新FindingProviderFields 物件用於BatchImportFindings 提供 Confidence 、 Criticality 、 Severity、 RelatedFindings 和 的值Types。應該只使用更新原始欄位BatchUpdateFindings 。	2021 年 3 月 18 日
ASFF 中資源的新DataClassification 物件	ASFF 中的新Resources .DataClassification 物件用於提供有關資源上偵測到的敏感資料的資訊。	2021 年 3 月 18 日
將CONFIG_RETURNS_NOT_APPLICABLE 值新增至可用的合規狀態碼	針對NOT_AVAILABLE 合規狀態，已移除原因代碼，RESOURCE_NO_LONGER_EXISTS 並新增原因代碼 CONFIG_RETURNS_NOT_APPLICABLE 。	2021 年 3 月 16 日
用於與 整合的新受管政策 AWS Organizations	新的 受管政策 AWSSecurityHubOrganizations Access 提供組織管理帳戶和委派 Security Hub CSPM 管理員帳戶所需的 Organizations 許可。	2021 年 3 月 15 日
已移至安全性章節的受管政策和服務連結角色資訊	受管政策的相關資訊會經過修訂和擴充。受管政策資訊和服務連結角色的資訊都已移至安全章節。	2021 年 3 月 15 日
修訂 CIS 1.1 和 CIS 3.1 – CIS 3.14 控制項的嚴重性	CIS 1.1 和 CIS 3.1 – CIS 3.14 控制項的嚴重性已變更為低。	2021 年 3 月 3 日

已移除 RDS.11 控制項	從基礎安全最佳實務標準中移除 RDS.11 控制項。	2021 年 3 月 3 日
已更新 Turbot 的整合	Turbot 整合已更新為傳送和接收問題清單。	2021 年 2 月 26 日
已將控制項新增至基礎安全最佳實務標準	新增了 Amazon API Gateway (APIGateway.1)、Amazon EC2 (EC2.9 和 EC2.10)、Amazon Elastic File System (EFS.2)、Amazon OpenSearch Service (ES.2 和 ES.3)、Elastic Load Balancing (ELB.6) 和 AWS Key Management Service (AWS KMS) (KMS.3) 的新控制項。	2021 年 2 月 11 日
已將選用ProductArn 篩選條件新增至 DescribeProducts API	DescribeProducts API 操作現在包含選用ProductArn 參數。ProductArn 參數用於識別要傳回詳細資訊的特定產品整合。	2021 年 2 月 3 日
雲端儲存安全與適用於 Amazon S3 的防毒新整合	與適用於 Amazon S3 的防毒整合會將病毒掃描結果作為調查結果傳送至 Security Hub CSPM。	2021 年 1 月 27 日
更新管理員帳戶的安全分數計算程序	對於管理員帳戶，Security Hub CSPM 使用單獨的程序來計算安全分數。新程序可確保分數包含針對成員帳戶啟用但針對管理員帳戶停用的控制項。	2021 年 1 月 21 日

[ASFF 中的新欄位和物件](#)

新增了新Action物件，以追蹤針對資源發生的動作。已將欄位新增至 AwsEc2NetworkInterface 物件，以追蹤 DNS 名稱和 IP 地址。已將新AwsSsmPatchCompliance 物件新增至資源詳細資訊。

2021 年 1 月 21 日

[將控制項新增至基礎安全最佳實務標準](#)

新增了 Amazon CloudFront (CloudFront.1 到 CloudFront.4),、Amazon DynamoDB (DynamoDB.1 到 DynamoDB.3),Elastic Load Balancing (ELB.3 到 ELB.5)、Amazon RDS (RDS.9 到 RDS.11)、Amazon Redshift (Redshift.1 到 Redshift.3 和 Redshift.6) 和 Amazon SNS (SNS.1) 的新控制項。

2021 年 1 月 15 日

[工作流程狀態會根據記錄狀態或合規狀態重設](#)

NOTIFIED RESOLVED NEW 如果封存的問題清單處於作用中狀態，或者問題清單的合規狀態從變更為 WARNING、或 FAILED，Security Hub CSPM 會自動將工作流程狀態從 或重設PASSED為 NOT_AVAILABLE。這些變更表示需要額外調查。

2021 年 1 月 7 日

[新增控制型問題清單 ProductFields 的資訊](#)

對於從控制項產生的問題清單，新增 AWS 了安全性問題清單格式 (ASFF) 中ProductFields 物件內容的相關資訊。

2020 年 12 月 29 日

受管洞察的更新	已變更洞見 5 的標題。新增了新的洞見 32，用於檢查是否有可疑活動的 IAM 使用者。	2020 年 12 月 22 日
IAM.7 和 Lambda.1 控制項的更新	在 AWS 基礎安全最佳實務標準中，已更新 IAM.7 的參數。更新 Lambda.1 的標題和描述。	2020 年 12 月 22 日
擴展與 ServiceNow ITSM 的整合	ServiceNow ITSM 整合可讓使用者在收到 Security Hub CSPM 調查結果時自動建立事件或問題。這些事件或問題的更新會導致 Security Hub CSPM 中的調查結果更新。	2020 年 12 月 11 日
與 AWS Audit Manager 的新整合	Security Hub CSPM 現在提供與 AWS Audit Manager 的整合。整合可讓 Audit Manager 從 Security Hub CSPM 接收以控制為基礎的調查結果。	2020 年 12 月 8 日
與 Aqua Security Kube-bench 的新整合	Security Hub CSPM 新增了與 Aqua Security Kube-bench 的整合。整合會將問題清單傳送至 Security Hub CSPM。	2020 年 11 月 24 日
雲端託管人現已在中國區域提供	與 Cloud Custodian 的整合現已在中國（北京）和中國（寧夏）區域提供。	2020 年 11 月 24 日

[BatchImportFindings 現在可以用來更新其他欄位](#)

先前，您無法使用 BatchImportFindings 更新 Confidence、Criticality、Severity、RelatedFindings 和 Types 欄位。現在，如果這些欄位尚未由更新BatchUpdateFindings，則可以由更新BatchImportFindings。一旦由更新BatchUpdateFindings，就無法由更新BatchImportFindings。

2020 年 11 月 24 日

[Security Hub CSPM 現在已與 整合 AWS Organizations](#)

客戶現在可以使用其 Organizations 帳戶組態來管理成員帳戶。組織管理帳戶會指定 Security Hub CSPM 管理員帳戶，其會決定要在 Security Hub CSPM 中啟用哪些組織帳戶。手動邀請程序仍然可用於不屬於組織的帳戶。

2020 年 11 月 23 日

[已移除大量控制項的個別調查 結果清單格式](#)

有大量問題清單時，控制項的問題清單不會再使用問題清單頁面格式。

2020 年 11 月 19 日

[全新和更新的第三方整合](#)

Security Hub CSPM 現在支援與 cloudtamer.io、3COR ESec、Prowler 和 StackRox Kubernetes Security 整合。IBM QRadar 不再傳送問題清單。它只會接收問題清單。

2020 年 10 月 30 日

[新增從控制項詳細資訊頁面下載問題清單的選項。](#)

在控制項詳細資訊頁面上，新的下載選項可讓您將調查結果清單下載至 .csv 檔案。下載的清單會遵守清單中的任何篩選條件。如果您選取特定問題清單，則下載的清單只會包含這些問題清單。

2020 年 10 月 26 日

[新增從標準詳細資訊頁面下載控制項清單的選項。](#)

在標準詳細資訊頁面上，新的下載選項可讓您將控制清單下載至 .csv 檔案。下載的清單會遵守清單中的任何篩選條件。如果您選取特定控制項，則下載的清單只會包含該控制項。

2020 年 10 月 26 日

[全新和更新的合作夥伴整合](#)

Security Hub CSPM 現在已與 ThreatModeler 整合。更新了下列合作夥伴整合，以反映其新產品名稱。Twistlock Enterprise Edition 現在是 Palo Alto Networks - Prisma 雲端運算。同樣來自 Palo Alto Networks 的 Demisto 現在是 Cortex XSOAR，而 Redlock 現在是 Prisma Cloud Enterprise。

2020 年 10 月 23 日

[Security Hub CSPM 在中國（北京）和中國（寧夏）推出](#)

Security Hub CSPM 現已在中國（北京）和中國（寧夏）區域提供。

2020 年 10 月 21 日

[ASFF 屬性和第三方整合的修訂格式](#)

[ASFF 屬性](#)和[合作夥伴整合](#)的清單現在使用清單型格式，而不是資料表。ASFF 語法、屬性和類型分類現在位於不同的主題中。

2020 年 10 月 15 日

重新設計的標準詳細資訊頁面	已啟用標準的標準詳細資訊頁面現在會顯示控制項的標籤式清單。標籤會根據控制項狀態篩選控制項清單。	2020 年 10 月 7 日
將 CloudWatch Events 取代為 EventBridge	將 Amazon CloudWatch Events 的參考取代為 Amazon EventBridge。	2020 年 10 月 1 日
與 Bluehexon for AWS、Alcid e kAudit 和 Palo Alto Networks VM-Series 的新整合。	Security Hub CSPM 現在已與 Blue Hexagon for AWS、Alcid e kAudit 和 Palo Alto Networks VM-Series 整合。適用於 AWS 和 kAudit 的藍色六角形會將問題清單傳送至 Security Hub CSPM。VM 系列會從 Security Hub CSPM 接收問題清單。	2020 年 9 月 30 日
在 ASFF 中新增和更新的資源詳細資訊物件	新增 AwsApiGatewayRestApi 、AwsApiGatewayStage 、AwsApiGatewayV2Api 、AwsApiGatewayV2Stage 、AwsCertificateManagerCertificate 、AwsElasticLoadBalancing 、AwsIamGroup 、和的新Resources .Details 物件AwsRedshiftCluster 。已將詳細資訊新增至 AwsCloudFrontDistribution 、AwsIamRole 和 AwsIamAccessKey 物件。	2020 年 9 月 30 日

[ASFF ResourceRole 中資源的新屬性，用於追蹤資源是演員還是目標。](#)

資源的 ResourceRole 屬性會指出資源是調查結果活動的目標還是調查結果活動的執行者。有效值為 ACTOR 和 TARGET。

2020 年 9 月 30 日

[已將 AWS Systems Manager 修補程式管理員新增至可用的 AWS 服務整合](#)

AWS Systems Manager 修補程式管理員現在已與 Security Hub CSPM 整合。當客戶機群中的執行個體不符合其修補程式合規標準時，修補程式管理員會將問題清單傳送至 Security Hub CSPM。

2020 年 9 月 22 日

[將新控制項新增至 AWS 基礎安全最佳實務標準](#)

新增下列服務的新控制項：
Amazon EC2 (EC2.7 和 EC2.8)、Amazon EMR (EMR.1)、IAM (IAM.8)、Amazon RDS (RDS.4 到 RDS.8)、Amazon S3 (S3.6) 和 AWS Secrets Manager (SecretsManager.1 和 SecretsManager.2)。

2020 年 9 月 15 日

[IAM 政策的新內容索引鍵，用於控制對 BatchUpdateFindings 欄位的存取](#)

IAM 政策現在可以設定為在使用時限制對欄位和欄位值的存取 BatchUpdateFindings。

2020 年 9 月 10 日

[擴展 BatchUpdateFindings 成員帳戶的存取權](#)

根據預設，成員帳戶現在擁有與 BatchUpdateFindings 管理員帳戶相同的存取權。

2020 年 9 月 10 日

[基礎安全最佳實務標準 AWS KMS 中的 新控制項](#)

將兩個新的控制項 (KMS.1 和 KMS.2) 新增至基礎安全最佳實務標準。新的控制項會檢查 IAM 政策是否限制對 AWS KMS 解密動作的存取。

2020 年 9 月 9 日

[已移除控制項的帳戶層級調查結果](#)

Security Hub CSPM 不再為控制項產生帳戶層級的問題清單。只會產生資源層級的問題清單。

2020 年 9 月 1 日

[ASFF 中的新PatchSummary物件](#)

已將PatchSummary 物件新增至 ASFF。PatchSummary 物件提供有關相對於所選合規標準之資源修補程式合規的資訊。

2020 年 9 月 1 日

[重新設計的控制項詳細資訊頁面](#)

控制項的詳細資訊頁面已重新設計。控制項調查結果清單提供索引標籤，可讓您根據合規狀態快速篩選清單。您也可以快速查看隱藏的問題清單。每個項目都可以存取有關問題清單資源、AWS Config 規則和問題清單備註的其他詳細資訊。

2020 年 8 月 28 日

[問題清單的新篩選條件選項](#)

對於問題清單篩選條件，您可以使用 不是篩選條件來尋找欄位值不等於篩選條件值的問題清單。您可以使用 開頭不是 來尋找欄位值開頭不是指定篩選條件值的問題清單。

2020 年 8 月 28 日

[ASFF 中的新資源詳細資訊物件](#)

新增下列資源類型的
新Resources.Details 物件：
AwsDynamoDbTable、AwsEc2Eip、
AwsIamPolicy、AwsIamUser、
AwsRdsDbCluster、AwsRdsDbClusterSnapshot、
AwsRdsDbSnapshot、
AwsSecretsManagerSecret

2020 年 8 月 18 日

[與 RSA Archer 的新整合](#)

Security Hub CSPM 現在已與 RSA Archer 整合。RSA Archer 會收到 Security Hub CSPM 的問題清單。

2020 年 8 月 18 日

[AwsKmsKey 的新描述欄位](#)

已將 Description 欄位新增至下的 AwsKmsKey 物件Resources.Details。

2020 年 8 月 18 日

[新增欄位至 AwsRdsDbInstance](#)

已將數個屬性新增至下的 AwsRdsDbInstance 物件Resources.Details。

2020 年 8 月 18 日

[更新 Security Hub CSPM 如何判斷控制項的整體狀態](#)

對於沒有調查結果的控制項，狀態為無資料而非未知。控制狀態包括帳戶層級和資源層級調查結果。控制狀態不會使用問題清單的工作流程狀態，除了忽略隱藏的問題清單。

2020 年 8 月 13 日

[更新 Security Hub CSPM 如何計算標準的安全性分數](#)

計算標準的安全分數時，Security Hub CSPM 現在會忽略狀態為無資料的控制項。安全性分數是傳遞控制項與啟用控制項的比例，不包括沒有資料的控制項。

2020 年 8 月 13 日

[在已啟用的標準中自動啟用新控制項的新選項](#)

新增設定選項，以在已啟用的標準中自動啟用新的控制項。您也可以使用 UpdateSecurityHubConfiguration API 操作來設定此選項。

2020 年 7 月 31 日

[支付卡產業資料安全標準 \(PCI DSS\) 標準的新控制項](#)

已將新控制項新增至 PCI DSS 標準。新控制項的識別符包括 PCI.DMS.1、PCI.EC2.5、PCI.EC2.6、PCI.ELBV2.1、PCI.GuardDuty.1、PCI.IAM.7、PCI.IAM.8、PCI.S3.5、PCI.S3.6、PCI.SageMaker.1、PCI.SSM.2 和 PCI.SSM.3。

2020 年 7 月 29 日

[基礎安全最佳實務標準的新控制和更新控制](#)

已將新控制項新增至基礎安全最佳實務標準。新控制項的識別符為 AutoScaling.1、DMS.1、EC2.4、EC2.6、S3.5 和 SSM.3。更新 ACM.1 的標題，並將 daysToExpiration 參數的值變更為 30。

2020 年 7 月 29 日

[ASFF 中的新 Vulnerabilities 物件](#)

新增 Vulnerabilities 物件，提供與調查結果相關聯之漏洞的相關資訊。

2020 年 7 月 1 日

ASFF for Auto Scaling 群組、EC2 磁碟區和 EC2 VPCs 中的新Resource.Details 物件	已將 AwsAutoScalingAutoScalingGroup 、 AWSEc2Volume 和 AwsEc2Vpc 物件新增至 Resource.Details 。	2020 年 7 月 1 日
ASFF 中的新NetworkPath 物件	新增 NetworkPath 物件，提供與問題清單相關的網路路徑資訊。	2020 年 7 月 1 日
在 Compliance.Status 為時自動解析問題清單 PASSED	對於控制項的問題清單，如果 Compliance.Status 是 PASSED，則 Security Hub CSPM 會自動Workflow.Status 設定為 RESOLVED。	2020 年 6 月 24 日
AWS Command Line Interface 範例	新增數個 Security Hub AWS CLI CSPM 任務的語法和範例。包括啟用 Security Hub CSPM、管理洞察、管理標準和控制、管理產品整合，以及停用 Security Hub CSPM。	2020 年 6 月 24 日
ASFF 中的新Severity.Original 屬性	已新增 Severity.Original 屬性，這是尋找提供者的原始嚴重性。這會取代已取代的 Severity.Product 屬性。	2020 年 5 月 20 日
ASFF 中的新Compliance.StatusReasons 物件，以取得控制項狀態的詳細資訊	已新增 Compliance.StatusReasons 物件，可為控制項目前狀態提供其他內容。	2020 年 5 月 20 日
新的 AWS 基礎安全最佳實務標準	新增了 AWS 新的基礎安全最佳實務標準，這是一組控制項，可偵測您部署的帳戶和資源何時偏離安全最佳實務。	2020 年 4 月 22 日

[更新問題清單工作流程狀態的新主控台選項](#)

新增使用 Security Hub 主控台或 API 來設定問題清單工作流程狀態的相關資訊。

2020 年 4 月 16 日

[用於客戶更新問題清單的新 BatchUpdateFindings API](#)

新增使用 BatchUpdateFindings 來更新與調查問題清單程序相關資訊的資訊。BatchUpdateFindings 已取代 UpdateFindings，後者已遭到取代。

2020 年 4 月 16 日

[AWS 安全性調查結果格式 \(ASFF\) 的更新](#)

新增了數個新的資源類型。新增了 Label 屬性到 Severity 物件。Label 的用途是取代 Normalized 欄位。新增了 Workflow 物件來追蹤調查問題清單的程序。Workflow 包含 Status 屬性，該屬性會取代現有的 Workflowstate 屬性。

2020 年 3 月 12 日

[整合頁面的更新](#)

更新以反映 Integrations (整合) 頁面的更新 對於每個整合，頁面現在會顯示整合類別，以及每個整合是否將調查結果傳送至 Security Hub CSPM 或從中接收調查結果。此頁面也會提供啟用各個整合所需進行的特定步驟。

2020 年 2 月 26 日

[新的第三方產品整合](#)

新增下列新產品整合：
Cloud Custodian、FireEye Helix、Forcepoint CASB、Forcepoint DLP、Forcepoint NGFW、Rackspace Cloud Native Security 和 Vectra.ai Cognito Detect。

2020 年 2 月 21 日

支付卡產業資料安全標準 (PCI DSS) 的新安全標準	已新增支付卡產業資料安全標準 (PCI DSS) 的 Security Hub CSPM 安全標準。啟用此標準時，Security Hub CSPM 會對與 PCI DSS 要求相關的控制項執行自動檢查。	2020 年 2 月 13 日
AWS 安全性調查結果格式 (ASFF) 的更新	新增 標準控制項相關需求 的欄位。新增 新的資源類型和新的資源詳細資訊 。ASFF 現在也允許你提供最多 32 個資源。	2020 年 2 月 5 日
停用個別安全標準控制項的新選項	新增如何控制是否啟用每個個別安全標準控制項的資訊。	2020 年 1 月 15 日
Security Hub CSPM 概念的更新	更新了一些描述，並將新術語新增至 Security Hub CSPM 概念 。	2019 年 9 月 21 日
AWS Security Hub CSPM 一般可用性版本	內容更新以反映測試期間對 Security Hub CSPM 所做的改進。	2019 年 6 月 25 日
新增 CIS AWS Foundations 檢查的修復步驟	已將修補步驟新增至 Security AWS Hub CSPM 中支援的安全標準 。	2019 年 4 月 15 日
AWS Security Hub CSPM 的 Beta 版	已發佈 AWS Security Hub CSPM 使用者指南的 Beta 版。	2018 年 11 月 18 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。