



Benutzer-Leitfaden

AWS Application Discovery Service



AWS Application Discovery Service: Benutzer-Leitfaden

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

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS Application Discovery Service?	1
VMware Discovery	2
Database Discovery	3
Vergleichen Sie Agentless Collector und Discovery Agent	3
Annahmen	7
AWS Application Discovery Service Änderung der Verfügbarkeit	9
Einzelheiten zur Verfügbarkeit des Dienstes	9
AWS Transform Übergang	9
Häufig gestellte Fragen	10
Einrichtung	12
Melde dich an für ein AWS-Konto	12
Erstellen von IAM-Benutzern	12
Einen Non-Administrative IAM-Benutzer erstellen	12
Melden Sie sich bei Migration Hub an und wählen Sie eine Heimatregion	13
Discovery-Agent	14
Funktionsweise	14
Gesammelte Daten	15
Voraussetzungen	18
Discovery Agent wird installiert	20
Installieren von auf Linux	20
Auf Microsoft Windows installieren	24
Den Discovery Agent-Prozess verwalten	30
Verwalten Sie den Prozess unter Linux	30
Den Prozess unter Microsoft Windows verwalten	31
Discovery Agent wird deinstalliert	32
Deinstallation unter Linux	32
Deinstallation unter Microsoft Windows	33
Datenerfassung starten und beenden	34
Problembehandlung bei Discovery Agent	35
Fehlerbehebung bei Discovery Agent unter Linux	35
Problembehandlung für Discovery Agent unter Microsoft Windows	36
Kollektor ohne Agenten	38
Voraussetzungen	39
Datenperimeter konfigurieren	40

Firewall konfigurieren	40
Bereitstellen eines Collectors	42
Erstellen eines IAM-Benutzers	42
Laden Sie den Collector herunter	45
Stellen Sie den Collector bereit	45
Zugriff auf die Collector-Konsole	47
Den Collector konfigurieren	47
(Optional) Konfigurieren Sie eine statische IP-Adresse für die Collector-VM	49
(Optional) Setzen Sie die Collector-VM wieder auf DHCP zurück	55
(Optional) Konfigurieren Sie Kerberos	57
Verwenden des Moduls zur Erfassung von Netzwerkdaten	58
Einrichtung des Moduls zur Erfassung von Netzwerkdaten	59
Versuche, Netzwerkdaten zu sammeln	61
Serverstatus im Modul Netzwerkdatenerfassung	61
Verwenden des VMware Datenerfassungsmoduls	62
Einrichtung der vCenter-Datenerfassung	63
Details VMware zur Datenerfassung anzeigen	64
Steuerung des Umfangs der Datenerfassung	65
Vom Modul gesammelte Daten VMware	66
Verwenden des Moduls zur Erfassung von Datenbank- und Analysedaten	71
Unterstützte Server	72
Den AWS DMS Datensammler erstellen	73
Konfiguration der Datenweiterleitung	75
Hinzufügen Ihrer LDAP- und OS-Server	75
Entdecken Sie Ihre Datenbanken	78
Vom Datenbank- und Analysemodul gesammelte Daten	83
Gesammelte Daten anzeigen	85
Zugriff auf den Agentless Collector	86
Kollektor-Dashboard	86
Collector-Einstellungen bearbeiten	88
Bearbeiten von vCenter-Anmeldeinformationen	89
Agentless Collector wird aktualisiert	90
Fehlerbehebung	92
Reparieren Unable to retrieve manifest or certificate file error	93
Behebung von Problemen mit selbstsignierten Zertifizierungen bei der Konfiguration von WinRM-Zertifikaten	93

Behebung des Problems, das Agentless Collector AWS während der Installation nicht erreichen kann	94
Behebung von Problemen mit selbstsignierten Zertifizierungen beim Herstellen einer Verbindung zum Proxyhost	96
Suche nach fehlerhaften Collectors	96
Behebung von Problemen mit IP-Adressen	97
Behebung von Problemen mit vCenter-Anmeldeinformationen	98
Behebung von Problemen bei der Datenweiterleitung	99
Behebung von Verbindungsproblemen	99
Unterstützung eigenständiger ESX-Hosts	101
Den AWS -Support kontaktieren	101
Daten in Migration Hub importieren	103
Unterstützte Importformate	104
RVTools	104
Migration Hub Hub-Importvorlage	104
Importberechtigungen einrichten	110
Ihre Importdatei auf Amazon S3 hochladen	114
Importieren von Daten	115
Nachverfolgung Ihrer Migration Hub Hub-Importanfragen	117
Daten anzeigen und untersuchen	120
Gesammelte Daten anzeigen	120
Passende Logik	121
Erkundung von Daten in Athena	122
Datenexploration einschalten	122
Erkundung von Daten	124
Visualisieren von Daten	126
Verwenden vordefinierter Abfragen	126
Daten mit der Migration Hub Hub-Konsole ermitteln	135
Daten im Dashboard anzeigen	135
Datensammler starten und stoppen	136
Datensammler sortieren	137
Server anzeigen	142
Server sortieren	142
Server taggen	143
Serverdaten werden exportiert	144
Server gruppieren	147

Verwenden der API zum Abfragen entdeckter Elemente	148
Verwenden der DescribeConfigurations Aktion	148
Die ListConfigurations Aktion verwenden	152
Letztendliche Datenkonsistenz	167
AWS PrivateLink	169
Überlegungen	169
Erstellen eines Schnittstellenendpunkts	169
Erstellen einer Endpunktrichtlinie	170
Verwenden des VPC-Endpunkts für den Agentless Collector und den AWS Application Discovery Agent	172
Sicherheit	173
Identitäts- und Zugriffsverwaltung	174
Zielgruppe	174
Authentifizierung mit Identitäten	175
Verwalten des Zugriffs mit Richtlinien	176
Wie AWS Application Discovery Service funktioniert mit IAM	178
AWS verwaltete Richtlinien	181
Beispiele für identitätsbasierte Richtlinien	186
Servicebezogene Rollen verstehen und verwenden	194
Fehlersuche bei IAM	202
Protokollierung von CloudTrail-API-Aufrufen mit	203
Informationen zum Application Discovery Service in CloudTrail	204
Grundlegendes zu den Protokolldateieinträgen des Application Discovery Service	205
ARN-Formate	207
Kontingente	208
Fehlerbehebung	209
Stoppen Sie die Datenerfassung durch Datenerkundung	209
Entfernen Sie die bei der Datenerkundung gesammelten Daten	210
Beheben Sie häufig auftretende Probleme bei der Datenexploration in Amazon Athena	212
Die Datenexploration in Amazon Athena kann nicht initiiert werden, da serviceverknüpfte Rollen erforderlich sind AWS Ressourcen können nicht erstellt werden	212
Neue Agentendaten werden in Amazon Athena nicht angezeigt	212
Sie verfügen nicht über ausreichende Berechtigungen für den Zugriff auf Amazon S3, Amazon Data Firehose oder AWS Glue	214
Fehlerbehebung bei fehlgeschlagenen Datensätzen	214
Dokumentverlauf	217

AWS Glossar 223

..... CCXXIV

Was ist AWS Application Discovery Service?

AWS Application Discovery Service hilft Ihnen bei der Planung Ihrer Migration zur AWS Cloud, indem es Nutzungs- und Konfigurationsdaten über Ihre lokalen Server und Datenbanken sammelt. Der Application Discovery Service ist in AWS Database Migration Service Fleet Advisor integriert. AWS Migration Hub vereinfacht Ihre Migrationsverfolgung, da es Ihre Migrationsstatusinformationen in einer einzigen Konsole zusammenfasst. Sie können die erkannten Server anzeigen, sie zu Anwendungen gruppieren und dann den Migrationsstatus jeder Anwendung von der Migration Hub Konsole in Ihrer Heimatregion aus verfolgen. Sie können DMS Fleet Advisor verwenden, um die Migrationsoptionen für Datenbank-Workloads zu bewerten.

Alle erkannten Daten werden in Ihrer Heimatregion gespeichert. AWS Migration Hub Daher müssen Sie Ihre Heimatregion in der Migration Hub Konsole oder mit CLI-Befehlen festlegen, bevor Sie Erkennungs- und Migrationsaktivitäten durchführen. Ihre Daten können zur Analyse in Microsoft Excel oder AWS Analysetools wie Amazon Athena und Amazon Quick exportiert werden.

Mit dem Application Discovery Service APIs können Sie die Systemleistungs- und Nutzungsdaten für Ihre erkannten Server exportieren. Geben Sie diese Daten in Ihr Kostenmodell ein, um die Kosten für den Betrieb dieser Server zu berechnen AWS. Darüber hinaus können Sie Daten über die Netzwerkverbindungen exportieren, die zwischen Servern bestehen. Auf diese Weise können Sie die Netzwerkabhängigkeiten zwischen Servern leichter bestimmen und sie zur Planung der Migration in Anwendungen gruppieren.

Note

Ihre Heimatregion muss eingerichtet werden, AWS Migration Hub bevor Sie mit dem Ermittlungsprozess beginnen, da Ihre Daten in Ihrer Heimatregion gespeichert werden. Weitere Informationen zur Arbeit mit einer Heimatregion finden Sie unter [Heimatregion](#).

Der Application Discovery Service bietet drei Möglichkeiten, Daten über Ihre lokalen Server zu ermitteln und zu sammeln:

- Die agentenlose Erkennung kann durchgeführt werden, indem Sie den Application Discovery Service Agentless Collector (Agentless Collector) (OVA-Datei) über Ihr vCenter bereitstellen. VMware Nachdem Agentless Collector konfiguriert wurde, identifiziert er virtuelle Maschinen (VMs) und Hosts, die mit vCenter verknüpft sind. Agentless Collector sammelt die folgenden

statischen Konfigurationsdaten: Server-Hostnamen, IP-Adressen, MAC-Adressen, Zuweisungen von Festplattenressourcen, Versionen der Datenbank-Engine und Datenbankschemas. Darüber hinaus sammelt es die Nutzungsdaten für jede VM und Datenbank und stellt die durchschnittliche und maximale Auslastung für Kennzahlen wie CPU, RAM und Festplatten-I/O bereit.

- Die agentenbasierte Erkennung kann durchgeführt werden, indem Sie den AWS Application Discovery Agent (Discovery Agent) auf jedem Ihrer Server VMs und auf Ihren physischen Servern einsetzen. Das Installationsprogramm für den Agenten ist für Windows- und für Linux-Betriebssysteme verfügbar. Es sammelt statische Konfigurationsdaten, detaillierte Zeitreihendaten der Systemleistung, ein- und ausgehende Netzwerkverbindungen sowie derzeit ausgeführte Prozesse.
- Der dateibasierte Import ermöglicht es Ihnen, Details Ihrer lokalen Umgebung direkt in Migration Hub zu importieren, ohne den Agentless Collector oder Discovery Agent zu verwenden, sodass Sie die Migrationsbewertung und -planung direkt anhand Ihrer importierten Daten durchführen können. Die aufgenommenen Daten hängen von den bereitgestellten Daten ab.

Der Application Discovery Service lässt sich in die Anwendungserkennungslösungen von AWS Partner Network (APN) -Partnern integrieren. Mit diesen Drittanbieterlösungen können Sie Details zu Ihrer lokalen Umgebung direkt in Migration Hub importieren, ohne einen Collector oder Discovery Agent ohne Agenten verwenden zu müssen. Anwendungserkennungstools von Drittanbietern können den AWS Application Discovery Service abfragen und mithilfe der öffentlichen API in die Application Discovery Service Service-Datenbank schreiben. Auf diese Weise können Sie Daten in den Migration Hub importieren und aufrufen, damit Sie Anwendungen mit Servern verknüpfen und Migrationen verfolgen können.

VMware Discovery

Wenn Sie virtuelle Maschinen (VMs) haben, die in der VMware vCenter-Umgebung ausgeführt werden, können Sie den Agentless Collector verwenden, um Systeminformationen zu sammeln, ohne auf jeder VM einen Agenten installieren zu müssen. Stattdessen laden Sie diese lokale Appliance in vCenter und lassen sie alle ihre Hosts erkennen und VMs

Agentless Collector erfasst Informationen zur Systemleistung und zur Ressourcenauslastung für jede VM, die im vCenter ausgeführt wird, unabhängig davon, welches Betriebssystem verwendet wird. Es kann jedoch nicht in jede einzelne VM „hineinschauen“ und kann daher nicht herausfinden, welche Prozesse auf jeder VM ausgeführt werden oder welche Netzwerkverbindungen bestehen. VMs Wenn Sie diesen Detaillierungsgrad benötigen und sich einige Ihrer vorhandenen VMs Daten genauer

ansehen möchten, um Sie bei der Planung Ihrer Migration zu unterstützen, können Sie den Discovery Agent daher nach Bedarf installieren.

Außerdem können Sie bei VMs Hosted on VMware sowohl den Agentless Collector als auch den Discovery Agent verwenden, um die Erkennung gleichzeitig durchzuführen. Einzelheiten zu den genauen Datentypen, die jedes Discovery-Tool sammelt, finden Sie unter [Verwenden des VMware vCenter Agentless Collector-Datenerfassungsmoduls](#).

Database Discovery

Wenn Sie in Ihrer lokalen Umgebung über Datenbank- und Analyseserver verfügen, können Sie den Agentless Collector verwenden, um diese Server zu ermitteln und zu inventarisieren. Anschließend können Sie Leistungsmetriken für jeden Datenbankserver sammeln, ohne Agentless Collector auf jedem Computer in Ihrer Umgebung installieren zu müssen.

Das Datenbank- und Analysedatenerfassungsmodul von Agentless Collector erfasst Metadaten und Leistungskennzahlen, die Einblicke in Ihre Dateninfrastruktur bieten. Das Modul zur Erfassung von Datenbank- und Analysedaten verwendet LDAP in Microsoft Active Directory, um Informationen über das Betriebssystem, die Datenbank und die Analyseserver in Ihrem Netzwerk zu sammeln. Anschließend führt das Datenerfassungsmodul in regelmäßigen Abständen Abfragen aus, um die tatsächliche Auslastung der CPU-, Arbeitsspeicher- und Festplattenkapazität für die Datenbanken und Analyseserver zu erfassen. Einzelheiten zu den gesammelten Messwerten finden Sie unter [Vom Datenbank- und Analysemodul gesammelte Daten](#).

Nachdem Agentless Collector die Datenerfassung aus Ihrer Umgebung abgeschlossen hat, können Sie die AWS DMS Konsole für weitere Analysen und zur Planung Ihrer Migration verwenden. Um beispielsweise ein optimales Migrationsziel in der auszuwählen AWS Cloud, können Sie Zielempfehlungen für Ihre Quelldatenbanken generieren. Weitere Informationen finden Sie unter [Verwenden des Datenbank- und Analysedatenerfassungsmoduls](#).

Vergleichen Sie Agentless Collector und Discovery Agent

Die folgende Tabelle bietet einen schnellen Vergleich der Datenerfassungsmethoden, die von Application Discovery Service unterstützt werden.

	Agentenloser Collector	Discovery-Agent	Vorlage für Migration Hub	RVTools exportieren
Supported server types				
VMware virtuelle Maschine	Ja	Ja	Ja	Ja
Physischer Server	Nein	Ja	Ja	Ja
Deployment				
Pro Server	Nein	Ja	–	Nein
Pro vCenter	Ja	Nein	–	Ja
Pro Rechenzentrum im selben Netzwerk	Nein	Nein	–	Nein
Collected data				
Daten zum Serverprofil (statische Konfiguration)	Ja	Ja	Ja	Ja
Metriken zur Serverauslastung von Hypervisor (CPU, RAM usw.)	Ja	Ja	Ja	Nein
Metriken zur Serverauslastung vom	Ja	Ja	Ja	Nein

	Agentenloser Collector	Discovery-Agent	Vorlage für Migration Hub	RVTools exportieren
Server (CPU, RAM usw.)				
Server-Netzwerkverbindungen (nur TCP)	Ja	Ja	Nein	Nein
Ausgeführte Prozesse	Nein	Ja	Nein	Nein
Erfassung intervall	-60 Minuten	-15 Sekunden	Einzelner Schnappschuss	Einzelner Snapshot
Server data use cases				
Serverdaten in Migration Hub anzeigen	Ja	Ja	Nur Profil	Nein
Generieren Sie eine Amazon EC2 Empfehlung auf der Grundlage des Serverprofils	Ja	Ja	Ja	Ja
Generieren Sie Amazon EC2 Empfehlungen auf der Grundlage von Nutzungsdaten	Ja	Ja	Ja	Nein

	Agentenloser Collector	Discovery-Agent	Vorlage für Migration Hub	RVTools exportieren
Export der aktuellen Nutzungs- Snapshot-Daten	Ja	Ja	Ja	Nein
Export von Nutzungsdaten aus Zeitreihen	Nein	Ja	Nein	Nein
Network data use cases				
Visualisierung im Migration Hub	Ja	Ja	Nein	Nein
Export nach Amazon Athena zur weiteren Erkundung	Nein	Ja	Nein	Nein
In eine CSV- Datei exportieren	Nein	Ja	Nein	Nein
Database use cases				
Daten des Datenbank serverprofils (statische Konfiguration)	Ja	Nein	Nein	Nein
Unterstützte Datenbank- Engines	Oracle, SQL Server, MySQL, PostgreSQL	Keine	Keine	Keine

	Agentenloser Collector	Discovery-Agent	Vorlage für Migration Hub	RVTools exportieren
Komplexität und Duplikate des Datenbank schemas	Ja	Nein	Nein	Nein
Objekte des Datenbank schemas	Ja	Nein	Nein	Nein
Plattform support				
Unterstützte Betriebssysteme	Jedes Betriebss- ystem, das in VMware Center v5.5 oder neueren Versionen läuft	Jeder Linux- oder Windows-S erver	Jeder Linux- oder Windows-S erver	Jeder Linux-Ser- ver, Windows- Server oder VMware v5.5 oder neuere Versionen

Annahmen

Für die Verwendung von Application Discovery Service wird Folgendes vorausgesetzt:

- Sie haben sich für angemeldet AWS. Weitere Informationen finden Sie unter [Application Discovery Service einrichten](#).
- Sie haben eine Heimatregion des Migration Hub ausgewählt. Weitere Informationen finden Sie in [der Dokumentation zu den Heimatregionen](#).

Folgendes ist zu erwarten:

- Die Heimatregion des Migration Hub ist die einzige Region, in der Application Discovery Service Ihre Ermittlungs- und Planungsdaten speichert.
- Discovery Agents, Konnektoren und Importe können nur in der von Ihnen ausgewählten Migration Hub-Heimatregion verwendet werden.

- Eine Liste der AWS Regionen, in denen Sie den Application Discovery Service verwenden können, finden Sie unter [Allgemeine Amazon Web Services-Referenz](#).

AWS Application Discovery Service Änderung der Verfügbarkeit

Nach reiflicher Überlegung haben wir beschlossen, ab dem 7. November 2025 für Neukunden AWS Application Discovery Service zu schließen. Wenn Sie den Service nutzen möchten, melden Sie sich vor diesem Datum an. Bestandskunden können den Service weiterhin wie gewohnt nutzen.

Dieses Thema enthält Informationen zur Änderung der Verfügbarkeit und Anleitungen für die Umstellung auf AWS Transform.

Einzelheiten zur Verfügbarkeit des Dienstes

Der Application Discovery Service nimmt ab dem 7. November 2025 keine neuen Kunden mehr an. AWS Transform ist unser agentischer KI-Service der nächsten Generation, der ähnliche Funktionen und erweiterte Funktionen zur Erkennung und Bewertung von virtuellen Rechnern bietet. Bestandskunden des Application Discovery Service können den Service weiterhin nutzen, um ihre laufenden Discovery-Projekte abzuschließen, die in der Regel einen Lebenszyklus von 4 Monaten haben. Die Kernfunktionen des Service für die Erkennung und Erfassung von Daten über lokale Server und Anwendungen sind jetzt AWS Transform mit verbesserten Funktionen verfügbar, sodass für den Kunden kein Umstellungsaufwand erforderlich ist.

Bis zum 7. November 2025 werden wir die Sicherheit und Zuverlässigkeit des Application Discovery Service weiterhin gewährleisten. Wir werden dem Service zwar keine neuen Funktionen hinzufügen, sind aber weiterhin bestrebt, Sicherheitsupdates bereitzustellen und die Serviceverfügbarkeit aufrechtzuerhalten, um sicherzustellen, dass Ihre laufenden Migrationsprojekte weiterhin reibungslos ablaufen. Unser Fokus liegt auf der Sicherstellung einer stabilen Umgebung, in der Bestandskunden ihre laufenden Migrationsinitiativen abschließen und uns gleichzeitig auf die erweiterten Funktionen vorbereiten können, die in AWS Transform verfügbar sind.

AWS Transform Übergang

AWS Transform ist unsere empfohlene Lösung, die alle Funktionen des Application Discovery Service vereint und gleichzeitig leistungsstarke neue Funktionen einführt. Sie bietet umfassende Erkennungs- und Bewertungsfunktionen durch agentengestützte und agentenlose Collectoren mit verbesserter VMware Umgebungsanalyse. Der Service ermöglicht die automatische Zuordnung von Anwendungsabhängigkeiten und die Wellenplanung und bietet gleichzeitig eine verbesserte

Erkennungslogik mit Was-wäre-wenn-Analysen und Kostenschätzungen. Mit erweiterten Funktionen wie integrierter Speicher- und Datenbankerkennung, konsolidierter 3P-Toolintegration und umfassender VM-Konfigurationsanalyse AWS Transform ist er darauf ausgelegt, den Bewertungs- und Planungsprozess der Migration für Kunden effizienter und erfolgreicher zu gestalten.

Der Übergang zu AWS Transform ist unkompliziert, da keine Datenmigration erforderlich ist. Bestehende Discovery-Projekte im Application Discovery Service funktionieren bis zum Abschluss weiterhin normal. Wenn Kunden bereit sind, neue Discovery-Projekte zu starten, können sie sie AWS Transform direkt nutzen — alle Erkennungs- und Bewertungsfunktionen von Application Discovery Service sind dort mit erweiterten Funktionen verfügbar. Informationen zu den ersten Schritten AWS Transform finden Sie im [Handbuch Erste Schritte](#). AWS Das Support-Team steht Ihnen über die AWS Support-Konsole zur Verfügung, wenn Sie AWS Transform Zugriff darauf haben oder Fragen zu laufenden Discovery-Projekten haben.

Häufig gestellte Fragen

Was bedeutet das für den Dienst (werden Sie den Dienst herunterfahren)?

Der Application Discovery Service nimmt ab dem 7. November 2025 keine neuen Kunden mehr an. Der Service wird weiterhin für bestehende Kunden verfügbar sein, um ihre laufenden Migrationsprojekte abzuschließen.

Wie wird sich das auf Bestandskunden auswirken?

Bestehende Kunden werden keine Unterbrechung ihrer aktuellen Migrationsprojekte erleben. Sie können den Application Discovery Service wie gewohnt weiter verwenden, bis ihre Projekte abgeschlossen sind. Auf alle laufenden Projekte kann weiterhin zugegriffen werden, und es werden weiterhin Sicherheitsupdates bereitgestellt, um die Zuverlässigkeit des Dienstes zu gewährleisten.

Am 7. November 2025 hat der Kunde Probleme. Wie können sie eskalieren?

Kunden, die Probleme haben, können sich über ihre AWS Support-Konsole an den AWS Support wenden. Das AWS Support-Team steht Ihnen bei allen Fragen oder Bedenken rund um den Service zur Verfügung.

Welche Alternativen können Kunden prüfen?

AWS Transform ist der empfohlene alternative Service. Es wurde 2025 eingeführt und AWS Transform umfasst ähnliche Funktionen des Application Discovery Service. Bietet erweiterte

Funktionen mit verbesserter VMware Umgebungsanalyse und automatisierter Zuordnung von Abhängigkeiten. Bietet integrierte Speicher- und Datenbankerkennungsfunktionen sowie umfassende Bewertungstools. Bei der Umstellung auf sind keine speziellen Werkzeuge erforderlich. AWS Transform

Wie können Kunden den Application Discovery Service verlassen?

Es ist kein formeller Migrationsprozess erforderlich. Bestehende Projekte können bis zum Abschluss in Application Discovery Service weitergeführt werden. Bei neuen Projekten können Kunden direkt einsteigen AWS Transform, was alle bekannten Funktionen des Application Discovery Service mit erweiterten Funktionen bietet. Es ist keine Datenmigration erforderlich, und AWS Support steht zur Verfügung, um Sie bei der Umstellung zu unterstützen.

Wenn Sie weitere Fragen haben, kontaktieren Sie uns bitte über den [AWS Support](#) oder lesen Sie unsere FAQs.

Application Discovery Service einrichten

Führen Sie AWS Application Discovery Service vor der ersten Verwendung die folgenden Aufgaben aus:

[Erstellen von IAM-Benutzern](#)

[Melden Sie sich bei der Migration Hub Konsole an und wählen Sie eine Heimatregion](#)

Melde dich an für ein AWS-Konto

Um loszulegen AWS, benötigen Sie eine AWS-Konto. Informationen zum Erstellen eines AWS-Konto finden Sie unter [Erste Schritte mit einem AWS-Konto](#) im AWS -Kontenverwaltung Referenzhandbuch.

Erstellen von IAM-Benutzern

Themen

- [Einen Non-Administrative IAM-Benutzer erstellen](#)

Einen Non-Administrative IAM-Benutzer erstellen

Wenn Sie IAM-Benutzer ohne Administratorrechte erstellen, befolgen Sie die bewährte Sicherheitsmethode Grant Least [Privilege, d. h. gewähren](#) Sie Benutzern Mindestberechtigungen.

Verwenden Sie von IAM verwaltete Richtlinien, um die Zugriffsebene für IAM-Benutzer ohne Administratorrechte auf den Application Discovery Service zu definieren. Informationen zu den verwalteten Richtlinien von Application Discovery Service finden Sie unter [AWS verwaltete Richtlinien für AWS Application Discovery Service](#).

So erstellen Sie einen IAM-Benutzer ohne Administratorrechte

1. Navigieren Sie in AWS-Managementkonsole zur IAM-Konsole.
2. Erstellen Sie einen IAM-Benutzer ohne Administratorrechte, indem Sie den Anweisungen zum Erstellen eines Benutzers mit der Konsole folgen, wie unter [Erstellen eines IAM-Benutzers in Ihrem AWS Konto im](#) IAM-Benutzerhandbuch beschrieben.

Folgen Sie dabei den Anweisungen im IAM-Benutzerhandbuch:

- Wählen Sie auf der Seite „Berechtigungen festlegen“ die Option „Bestehende Richtlinien direkt an den Benutzer anhängen“. Wählen Sie dann eine verwaltete IAM-Richtlinie für Application Discovery Service aus der Richtlinienliste aus. Informationen zu den verwalteten Richtlinien von Application Discovery Service finden Sie unter [AWS verwaltete Richtlinien für AWS Application Discovery Service](#).
 - Wenn Sie sich die Zugriffsschlüssel des Benutzers (Zugriffsschlüssel-IDs und geheime Zugangsschlüssel) ansehen, folgen Sie den Anweisungen im Abschnitt Wichtiger Hinweis zur Aufbewahrung der neuen Zugriffsschlüssel-ID und des geheimen Zugangsschlüssels des Benutzers an einem sicheren Ort.
3. Nachdem Sie den Benutzer erstellt haben, gewähren Sie ihm programmatischen Zugriff, wie unter [Support programmatischen Benutzerzugriff](#) beschrieben.

Melden Sie sich bei der Migration Hub Hub-Konsole an und wählen Sie eine Heimatregion

Sie müssen in dem AWS Konto, das Sie für das verwenden, eine AWS Migration Hub Heimatregion auswählen AWS Application Discovery Service.

Um eine Heimatregion auszuwählen

1. Melden Sie sich mit Ihrem AWS Konto bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole Einstellungen und anschließend eine Heimatregion aus.

Ihre Migration Hub Hub-Daten werden in Ihrer Heimatregion zu Ermittlungs-, Planungs- und Migrationsverfolgungszwecken gespeichert. Weitere Informationen finden Sie unter [Die Heimatregion des Migration Hub](#).

AWS Agent zur Anwendungserkennung

Der AWS Application Discovery Agent (Discovery Agent) ist eine Software, die Sie auf lokalen Servern und VMs installieren, die für die Erkennung und Migration vorgesehen sind. Agenten sammeln Daten zu Systemkonfiguration, Systemleistung, laufenden Prozessen und Details der Netzwerkverbindungen zwischen Systemen. Agenten unterstützen die meisten Linux- und Windows-Betriebssysteme, und Sie können sie auf physischen lokalen Servern, Amazon EC2 EC2-Instances und virtuellen Maschinen bereitstellen.

Note

Bevor Sie den Discovery Agent bereitstellen, müssen Sie eine [Migration Hub Hub-Heimatregion](#) auswählen. Sie müssen Ihren Agenten in Ihrer Heimatregion registrieren.

Der Discovery Agent wird in Ihrer lokalen Umgebung ausgeführt und benötigt Root-Rechte. Wenn Sie den Discovery Agent starten, stellt er eine sichere Verbindung mit Ihrer Heimatregion her und registriert sich beim Application Discovery Service.

- Wenn es `eu-central-1` sich beispielsweise um Ihre Heimatregion handelt, registriert sie sich `arsenal-discovery.eu-central-1.amazonaws.com` beim Application Discovery Service.
- Oder ersetzen Sie bei Bedarf alle anderen Regionen außer US-West-2 durch Ihre Heimatregion.
- Wenn es `us-west-2` sich um Ihre Heimatregion handelt, registriert sie sich `arsenal.us-west-2.amazonaws.com` beim Application Discovery Service.

Funktionsweise

Nach der Registrierung beginnt der Agent mit der Erfassung von Daten für den Host oder die VM, auf dem er sich befindet. Der Agent sendet in Intervallen von 15 Minuten ein Ping-Signal an den Application Discovery Service, um Konfigurationsinformationen zu erhalten.

Zu den erfassten Daten gehören Systemspezifikationen, Zeitreihen mit Nutzungs- oder Leistungsdaten, Netzwerkverbindungen und Prozessdaten. Sie können anhand dieser Informationen Ihre IT-Komponenten und deren Netzwerkabhängigkeiten zuordnen. All diese Datenpunkte können Ihnen helfen, die Kosten für den Betrieb dieser Server zu ermitteln AWS und die Migration zu planen.

Daten werden von den Discovery Agents mithilfe der Transport Layer Security (TLS) - Verschlüsselung sicher an den Application Discovery Service übertragen. Agenten sind so konfiguriert, dass automatisch ein Upgrade durchgeführt wird, wenn neue Versionen verfügbar sind. Sie können diese Konfigurationseinstellung auf Wunsch ändern.

 Tip

Bevor Sie den Discovery Agent herunterladen und mit der Installation beginnen, sollten Sie alle erforderlichen Voraussetzungen unter lesen [Voraussetzungen für Discovery Agent](#)

Von Discovery Agent gesammelte Daten

AWS Application Discovery Agent (Discovery Agent) ist Software, die Sie auf lokalen Servern installieren und VMs. Discovery Agent sammelt Systemkonfigurations-, Zeitreihennutzungs- oder Leistungsdaten, Prozessdaten und TCP-Netzwerkverbindungen (Transmission Control Protocol). In diesem Abschnitt werden die gesammelten Daten beschrieben.

Tabellenlegende für die von Discovery Agent gesammelten Daten:

- Der Begriff "Host" bezieht sich auf einen physischen Server oder eine VM.
- Gesammelte Daten sind Messungen in Kilobyte (KB), sofern nicht anders angegeben.
- Entsprechende Daten in der Migration Hub Hub-Konsole werden in Megabyte (MB) gemeldet.
- Die Abfrage erfolgt in Intervallen von etwa 15 Sekunden und wird AWS alle 15 Minuten gesendet.
- Datenfelder, die mit einem Sternchen (*) gekennzeichnet sind, sind nur in den .csv Dateien verfügbar, die mit der API-Exportfunktion des Agenten erstellt wurden.

Datenfeld	Description
agentAssignedProcess ^{ID *}	Prozess-ID der vom Agenten erkannten Prozesse
agentId	Eindeutige ID des Agenten
agentProvidedTimeStempel [*]	Datum und Uhrzeit der Beobachtung des Agenten (mm/dd/yyyy hh:mm:ss am/pm)

Datenfeld	Description
cmdLine [*]	In der Befehlszeile eingegebener Prozess
cpuType	Im Host verwendeter Typ der CPU (Zentraleinheit)
destinationIp [*]	IP-Adresse des Geräts, zu dem das Paket gesendet wird
destinationPort [*]	Portnummer, an die data/request das gesendet werden soll
family [*]	Protokoll der Routing-Familie
freeRAM (MB)	Freier RAM und zwischengespeicherter RAM, der Anwendungen unmittelbar zur Verfügung gestellt werden kann, gemessen in MB
gateway [*]	Knotenadresse des Netzwerks
hostName	Name des Hosts, für den Daten gesammelt wurden
hypervisor	Typ des Hypervisors
ipAddress	IP-Adresse des Hosts
ipVersion [*]	IP-Versionsnummer
isSystem [*]	Boolesches Attribut, das angibt, ob ein Prozess zum Betriebssystem gehört
macAddress	MAC-Adresse des Hosts
name [*]	Name des Hosts, des Netzwerks, der Metrik usw., für die Daten gesammelt werden
netMask [*]	IP-Adressen-Präfix, zu der ein Netzwerk-Host gehört

Datenfeld	Description
osName	Name des Betriebssystems auf dem Host
osVersion	Version des Betriebssystems auf dem Host
Pfad	Pfad der Befehle, die ihren Ursprung in der Befehlszeile haben
sourceIp [*]	IP-Adresse des Geräts, vom dem das IP-Paket gesendet wird
sourcePort [*]	Portnummer, von der das data/request stammt
timestamp [*]	Datum und Uhrzeit des gemeldeten Attributs, die vom Agenten protokolliert wurden
totalCpuUsagePct	Prozentsatz der CPU-Nutzung auf dem Host während des Abrufzeitraums
totalDiskBytesReadPerSecond (Kbit/s)	Gesamtzahl der pro Sekunde gelesenen Kilobits auf allen Festplatten
totalDiskBytesWrittenPerSecond (Kbit/s)	Gesamtzahl der pro Sekunde geschriebenen Kilobits auf allen Festplatten
totalDiskFreeGröße (GB)	Freier Speicherplatz in GB
totalDiskReadOpsPerSecond	Gesamtzahl der I/O Lesevorgänge pro Sekunde
totalDiskSize (GB)	Gesamtkapazität der Festplatte in GB
totalDiskWriteOpsPerSecond	Gesamtzahl der I/O Schreibvorgänge pro Sekunde
totalNetworkBytesReadPerSecond (Kbit/s)	Gesamtdurchsatz der pro Sekunde gelesenen Bytes

Datenfeld	Description
totalNetworkBytesWrittenPerSecond (Kbit/s)	Gesamtdurchsatz der pro Sekunde geschriebenen Bytes
totalNumCores	Gesamtzahl der unabhängigen Verarbeitungseinheiten innerhalb der CPU
totalNumCpus	Gesamtzahl der Zentraleinheiten
totalNumDisks	Die Anzahl der physischen Festplatten auf einem Host
totalNumLogical ^{Prozessoren *}	Gesamtzahl der physischen Kerne multipliziert mit der Anzahl der Threads, die auf jedem Kern ausgeführt werden können
totalNumNetworkKarten	Gesamtzahl der Netzwerkkarten auf dem Server
totalRAM (MB)	Gesamtmenge des auf dem Host verfügbaren RAM
transportProtocol [*]	Verwendeter Typ von Transportprotokoll

Voraussetzungen für Discovery Agent

Im Folgenden sind die Voraussetzungen und Aufgaben aufgeführt, die Sie ausführen müssen, bevor Sie den AWS Application Discovery Agent (Discovery Agent) erfolgreich installieren können.

- Sie müssen eine [AWS Migration Hub Heimatregion](#) festlegen, bevor Sie mit der Installation von Discovery Agent beginnen.
- Wenn eine 1.x-Version des Agenten installiert ist, muss diese entfernt werden, bevor die neueste Version installiert wird.
- Wenn auf dem Host, auf dem der Agent installiert wird, Linux ausgeführt wird, stellen Sie sicher, dass der Host mindestens die Intel i686 CPU-Architektur (auch bekannt als P6-Mikroarchitektur) unterstützt.
- Generieren Sie die für die Installation von Discovery Agent erforderlichen [Zugriffsschlüssel](#).

- Prüfen Sie, ob Ihre Betriebssystemumgebung unterstützt wird:

Linux

Amazon Linux 2012.03, 2015.03
Amazon Linux 2 (Update vom 25. September 2018 und höher)
Ubuntu 12.04, 14.04, 16.04, 18.04, 20.04
RedHat Enterprise Linux 5.11, 6.10, 7.3, 7.7, 8.1
CentOS 5.11, 6.9, 7.3
SUSE 11 SP4, 12, 15 SP5 SP5

Windows

Windows Server 2003 R2 SP2
Windows Server 2008 R1 SP2, 2008 R2 SP1
Windows Server 2012 R1, 2012 R2
Windows Server 2016
Windows Server 2019
Windows Server 2022

- Wenn von Ihrem Netzwerk ausgehende Verbindungen eingeschränkt sind, müssen Sie Ihre Firewall-Einstellungen aktualisieren. Agenten benötigen Zugriff auf `arsenal` über den TCP-Port 443. Es ist nicht erforderlich, dass eingehende Ports geöffnet sind.

Wenn Ihre Heimatregion beispielsweise `ist-eu-central-1`, würden Sie verwenden `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

- Damit das automatische Upgrade funktioniert, ist Zugriff auf Amazon S3 in Ihrer Heimatregion erforderlich.
- Erstellen Sie einen AWS Identity and Access Management (IAM-) Benutzer in der Konsole und fügen Sie die bestehende verwaltete `AWSApplicationDiscoveryAgentAccess` IAM-Richtlinie an. Diese Richtlinie ermöglicht es dem Benutzer, die erforderlichen Agentenaktionen in Ihrem Namen auszuführen. Weitere Informationen über verwaltete Richtlinien finden Sie unter [AWS verwaltete Richtlinien für AWS Application Discovery Service](#).
- Überprüfen Sie die Zeitverzögerung von Ihren Network Time Protocol(NTP)-Servern und korrigieren Sie sie gegebenenfalls. Eine falsche Zeitsynchronisierung führt dazu, dass der Agentenregistrierungsauftrag fehlschlägt.

Note

Der Discovery Agent verfügt über eine ausführbare 32-Bit-Agent-Datei, die auf 32-Bit- und 64-Bit-Betriebssystemen funktioniert. Durch eine einzige ausführbare Datei wird die Anzahl der erforderlichen Installationspakete für die Bereitstellung reduziert. Dieser ausführbare Agent funktioniert für Linux und Windows OS. Dies wird in den jeweiligen Installationsabschnitten angesprochen, die folgen.

Discovery Agent wird installiert

Auf dieser Seite wird beschrieben, wie Sie den Discovery Agent unter Linux und Microsoft Windows installieren.

Installieren Sie Discovery Agent unter Linux

Führen Sie das folgende Verfahren unter Linux aus. Stellen Sie sicher, dass Ihre [Heimatregion für Migration Hub](#) festgelegt wurde, bevor Sie mit diesem Verfahren beginnen.

Note

Wenn Sie eine nicht aktuelle Linux-Version verwenden, lesen Sie unter [Überlegungen zu älteren Linux-Plattformen](#) nach.

Um den AWS Application Discovery Agent in Ihrem Rechenzentrum zu installieren

1. Melden Sie sich bei Ihrem Linux-basierten Server oder Ihrer VM an und erstellen Sie ein neues Verzeichnis, das Ihre Agentenkomponenten enthält.
2. Wechseln Sie zu dem neuen Verzeichnis und laden Sie das Installationsskript über die Befehlszeile oder über die Konsole herunter.
 - a. Führen Sie zum Herunterladen über die Befehlszeile den folgenden Befehl aus.

```
curl -o ./aws-discovery-agent.tar.gz https://s3.region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz
```

- b. Gehen Sie wie folgt vor, um von der Migration Hub Hub-Konsole herunterzuladen:

- i. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
 - ii. Wählen Sie auf der linken Navigationsseite unter Discover die Option Tools aus.
 - iii. Wählen Sie im Feld AWS Discovery Agent die Option Agenten herunterladen und dann Download für Linux aus. Ihr Download beginnt sofort.
3. Überprüfen Sie die kryptografische Signatur des Installationspakets mit den drei folgenden Befehlen:

```
curl -o ./agent.sig https://s3.region.amazonaws.com/aws-discovery-agent.region/linux/latest/aws-discovery-agent.tar.gz.sig
```

```
curl -o ./discovery.gpg https://s3.region.amazonaws.com/aws-discovery-agent.region/linux/latest/discovery.gpg
```

```
gpg --no-default-keyring --keyring ./discovery.gpg --verify agent.sig aws-discovery-agent.tar.gz
```

Der Fingerabdruck des öffentlichen Schlüssel des Agenten (discovery.gpg) ist 7638 F24C 6717 F97C 4F1B 3BC0 5133 255E 4DF4 2DA2.

4. Extrahieren Sie den Tarball wie im Folgenden dargestellt.

```
tar -xzf aws-discovery-agent.tar.gz
```

5. Wählen Sie eine der folgenden Installationsmethoden, um den Agenten zu installieren.

Zu ...	Vorgehensweise
Installieren Sie Discovery Agent	Um den Agenten zu installieren, führen Sie den Befehl <code>agent install</code> aus, wie im folgenden Beispiel gezeigt. Ersetzen Sie es im Beispiel <i>your-home-region</i> durch den Namen Ihrer Heimatregion, <i>aws-access-key-id</i> durch Ihre Zugriffsschlüssel-ID und <i>aws-secret-access-key</i> durch Ihren geheimen Zugriffsschlüssel.

Zu ...	Vorgehensweise
	<pre>sudo bash install -r <i>your-home-region</i> -k <i>aws-access-key-id</i> -s <i>aws-secret-access-key</i></pre> Standardmäßig laden Agenten Updates automatisch herunter und installieren sie, sobald sie verfügbar sind. Wir empfehlen die Verwendung dieser Standard-Konfiguration. Wenn Sie jedoch nicht möchten, dass Agenten Updates automatisch heruntergeladen und angewendet werden, geben Sie den <code>-u false</code> Parameter bei der Ausführung des Agent-Installationsbefehls an.

Zu ...	Vorgehensweise
(Optional) Installieren Sie Discovery Agent und konfigurieren Sie einen nicht transparenten Proxy	Um einen nicht transparenten Proxy zu konfigurieren, fügen Sie dem Installationsbefehl des Agenten die folgenden Parameter hinzu: • -e Das Proxy-Passwort. • -f Die Proxy-Portnummer. • -g Das Proxyschema. • -i Der Proxy-Benutzername. Im Folgenden finden Sie ein Beispiel für den Agenteninstallationsbefehl, der die nicht transparenten Proxyparameter verwendet. <pre>sudo bash install -r <i>your-home-region</i> -k <i>aws-access-key-id</i> -s <i>aws-secret-access-key</i> -d <i>myproxy.mycompany.com</i> -e <i>mypassword</i> -f <i>proxy-port-number</i> -g https -i <i>myusername</i></pre> Wenn Ihr Proxy keine Authentifizierung erfordert, lassen Sie die -i Parameter -e und weg. Der Beispielbefehl install verwendet https, wenn Ihr Proxy HTTP verwendet, http für den -g Parameterwert „specify“.

6. Wenn von Ihrem Netzwerk ausgehende Verbindungen eingeschränkt sind, müssen Sie Ihre Firewall-Einstellungen aktualisieren. Agenten benötigen Zugriff auf `arsenal` über den TCP-Port 443. Es ist nicht erforderlich, dass eingehende Ports geöffnet sind.

Wenn Ihre Heimatregion beispielsweise `eu-central-1`, würden Sie verwenden `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Überlegungen zu älteren Linux-Plattformen

Einige ältere Linux-Plattformen, wie SUSE 10, CentOS 5 und RHEL 5, sind entweder am Ende ihrer Betriebslebensdauer angelangt oder werden nur noch minimal unterstützt. Auf diesen Plattformen kann es zu out-of-date Verschlüsselungssammlungen kommen, die verhindern, dass das Agent-Aktualisierungsskript Installationspakete herunterlädt.

Curl

Der Application Discovery Agent benötigt eine `curl` sichere Kommunikation mit dem AWS Server. Einige alte Versionen von `curl` sind nicht in der Lage, eine sichere Kommunikation mit einem modernen Web-Service durchzuführen.

Um die im Application Discovery-Agenten enthaltene Version von `curl` zu verwenden, führen Sie das Installationsskript mit dem Parameter `-c true` aus.

Zertifizierungsstellen-Bundle

Ältere Linux-Systeme verfügen möglicherweise über ein out-of-date Certificate Authority (CA) - Paket, das für eine sichere Internetkommunikation von entscheidender Bedeutung ist.

Um das im Application Discovery-Agenten enthaltene CA-Bundle zu verwenden, führen Sie das Installationsskript mit dem Parameter `-b true` aus.

Diese Installationsskriptoptionen können zusammen verwendet werden. Im folgenden Beispielbefehl werden beide Skriptparameter an das Installationsskript übergeben:

```
sudo bash install -r your-home_region -k aws-access-key-id -s aws-secret-access-key -c true -b true
```

Installieren Sie Discovery Agent unter Microsoft Windows

Gehen Sie wie folgt vor, um einen Agenten unter Microsoft Windows zu installieren. Stellen Sie sicher, dass Ihre [Heimatregion für Migration Hub](#) festgelegt wurde, bevor Sie mit diesem Verfahren beginnen.

Um den AWS Application Discovery Agent in Ihrem Rechenzentrum zu installieren

1. Laden Sie das [Windows Agent-Installationsprogramm](#) herunter, doppelklicken Sie jedoch nicht, um das Installationsprogramm in Windows auszuführen.

Important

Doppelklicken Sie nicht, um das Installationsprogramm in Windows auszuführen, da es sonst nicht installiert werden kann. Die Installation von Agenten ist nur über die Eingabeaufforderung möglich. (Wenn Sie bereits auf das Installationsprogramm doppelt geklickt haben, müssen Sie zu Software navigieren und den Agenten deinstallieren, bevor Sie mit den verbleibenden Installationsschritten fortfahren.)

Wenn das Windows Agent-Installationsprogramm keine Version der Visual C++ x86-Laufzeit auf dem Host erkennt, installiert es automatisch die Visual C++ x86 2015–2019-Runtime vor der Installation der Agentsoftware.

2. Öffnen Sie als Administrator eine Eingabeaufforderung und navigieren Sie zum Speicherort des Installationspakets.
3. Wählen Sie eine der folgenden Installationsmethoden, um den Agenten zu installieren.

Zu ...	Vorgehensweise
Installieren Sie Discovery Agent	Um den Agenten zu installieren, führen Sie den Befehl <code>agent install</code> aus, wie im folgenden Beispiel gezeigt. Ersetzen Sie es im Beispiel <i>your-home-region</i> durch den Namen Ihrer Heimatregion, <i>aws-access-key-id</i> durch Ihre Zugriffsschlüssel-ID und <i>aws-secret-access-key</i> durch Ihren geheimen Zugriffsschlüssel. Optional können Sie den Installationsort für den Agenten festlegen, indem Sie den Ordnerpfad <i>C:\install-location</i> für den Parameter <code>INSTALLLOCATION</code> angeben. Beispiel, <code>INSTALLLOCATION=" C:\install-location "</code>.

Zu ...	Vorgehensweise
	Die daraus resultierende Ordnerhierarchie lautet [INSTALLLOCATION-Pfad]\AWS Discovery. Standardmäßig ist das Installationsverzeichnis der Program Files Ordner. Optional können LOGANDCONFIGLOCATION Sie das Standardverzeichnis (ProgramData) für den Protokollordner und die Konfigurationsdatei des Agenten überschreiben. Die resultierende Ordnerhierarchie ist [<i>LOGANDCONFIGLOCATION path</i>]\AWS Discovery . <pre data-bbox="862 840 1510 1081">.\AWSDiscoveryAgentInstall.exe REGION=" <i>your-home-region</i> " KEY_ID=" <i>aws-access-key-id</i> " KEY_SECRET=" <i>aws-secret-access-key</i> " /quiet</pre> Standardmäßig laden Agenten Updates automatisch herunter und installieren sie, sobald sie verfügbar sind. Wir empfehlen die Verwendung dieser Standard-Konfiguration. Wenn Sie jedoch nicht möchten, dass Agenten Updates automatisch herunterladen und anwenden, geben Sie bei der Ausführung des Agent-Installationsbefehls den folgenden Parameter an: AUTO_UPDATE=false

Zu ...	Vorgehensweise
	Warning Durch Deaktivieren von automatischen Upgrades wird verhindert, dass die neuesten Sicherheits-Patches installiert werden.

Zu ...	Vorgehensweise
(Optional) Installieren Sie Discovery Agent und konfigurieren Sie einen nicht transparenten Proxy	Um einen intransparenten Proxy zu konfigurieren, fügen Sie dem Installationsbefehl des Agenten die folgenden öffentlichen Eigenschaften hinzu: • <code>PROXY_HOST</code> — Der Name des Proxy-Hosts • <code>PROXY_SCHEME</code> — Das Proxyschema • <code>PROXY_PORT</code> — Die Proxy-Portnummer • <code>PROXY_USER</code> — Der Proxy-Benutzername • <code>PROXY_PASSWORD</code> — Das Proxy-Benutzerkennwort Im Folgenden finden Sie ein Beispiel für den Agent-Installationsbefehl, der die nicht transparenten Proxyeigenschaften verwendet <pre>.\AWSDiscoveryAgentInstaller.exe REGION=" your-home-region " KEY_ID="aws-access-key-id " KEY_SECRET=" aws-secret-access-key " PROXY_HOST=" myproxy.mycompany.com " PROXY_SCHEME="https" PROXY_PORT=" proxy-port-number " PROXY_USER=" myusername " PROXY_PASSWORD=" mypassword " /quiet</pre> Wenn Ihr Proxy keine Authentifizierung erfordert, lassen Sie die Eigenschaften <code>PROXY_USER</code> und <code>PROXY_PASSWORD</code> weg. Der Beispielbefehl <code>install</code> verwendet <code>https</code>. Wenn Ihr Proxy HTTP verwendet,

Zu ...	Vorgehensweise
	geben Sie <code>http</code> als <code>PROXY_SCHEME</code> Wert an.

- Wenn ausgehende Verbindungen aus Ihrem Netzwerk eingeschränkt sind, müssen Sie Ihre Firewall-Einstellungen aktualisieren. Agenten benötigen Zugriff auf `arsenal` über den TCP-Port 443. Es ist nicht erforderlich, dass eingehende Ports geöffnet sind.

Wenn Ihre Heimatregion beispielsweise `eu-central-1`, würden Sie Folgendes verwenden: `https://arsenal-discovery.eu-central-1.amazonaws.com:443`

Paketsignierung und automatische Upgrades

Für Windows Server 2008 und höher signiert Amazon das Installationspaket für den Application Discovery Service Agent kryptografisch mit einem SHA256 Zertifikat. Stellen Sie bei SHA2 -signierten automatischen Updates unter Windows Server 2008 sicher SP2, dass auf den Hosts ein Hotfix zur Unterstützung der Signaturauthentifizierung installiert ist. SHA2 Der neueste [Support-Hotfix](#) von Microsoft unterstützt die Authentifizierung unter Windows Server 2008. SHA2 SP2

Note

Die Hotfixes für den SHA256 Support für Windows 2003 sind bei Microsoft nicht mehr öffentlich erhältlich. Wenn diese Fixes nicht bereits auf Ihrem Windows 2003-Host installiert sind, sind manuelle Upgrades erforderlich.

Um Upgrades manuell durchzuführen

- Laden Sie den [Windows Agent Updater](#) herunter.
- Öffnen Sie die Eingabeaufforderung als Administrator.
- Navigieren Sie zu dem Speicherort, an dem der Updater gespeichert wurde.
- Führen Sie den folgenden Befehl aus.

```
AWSDiscoveryAgentUpdater.exe /Q
```

Den Discovery Agent-Prozess verwalten

Auf dieser Seite wird beschrieben, wie Sie den Discovery Agent unter Linux und Microsoft Windows verwalten.

Den Discovery Agent-Prozess unter Linux verwalten

Sie können das Verhalten des Discovery Agents auf Systemebene mithilfe der System `V init` Tools `systemd` `Upstart`, oder verwalten. Die folgenden Registerkarten beschreiben die Befehle für die unterstützten Aufgaben in den jeweiligen Tools.

systemd

Management-Befehle für den Application Discovery Agent

Aufgabe	Befehl
Überprüfen Sie, ob ein Agent ausgeführt wird	<code>sudo systemctl status aws-discovery-daemon.service</code>
Starten Sie einen Agenten	<code>sudo systemctl start aws-discovery-daemon.service</code>
Beenden Sie einen Agenten	<code>sudo systemctl stop aws-discovery-daemon.service</code>
Starten Sie einen Agenten neu	<code>sudo systemctl restart aws-discovery-daemon.service</code>

Upstart

Verwaltungsbefehle für den Application Discovery Agent

Aufgabe	Befehl
Überprüfen Sie, ob ein Agent ausgeführt wird	<code>sudo initctl status aws-discovery-daemon</code>
Starten Sie einen Agenten	<code>sudo initctl start aws-discovery-daemon</code>

Aufgabe	Befehl
Beenden Sie einen Agenten	<code>sudo initctl stop aws-discovery-daemon</code>
Starten Sie einen Agenten neu	<code>sudo initctl restart aws-discovery-daemon</code>

System V init

Verwaltungsbefehle für den Application Discovery Agent

Aufgabe	Befehl
Überprüfen Sie, ob ein Agent ausgeführt wird	<code>sudo /etc/init.d/aws-discovery-daemon status</code>
Starten Sie einen Agenten	<code>sudo /etc/init.d/aws-discovery-daemon start</code>
Beenden Sie einen Agenten	<code>sudo /etc/init.d/aws-discovery-daemon stop</code>
Starten Sie einen Agenten neu	<code>sudo /etc/init.d/aws-discovery-daemon restart</code>

Den Discovery Agent-Prozess unter Microsoft Windows verwalten

Sie können das Verhalten des Discovery Agents auf Systemebene über die Windows Server Manager Services-Konsole verwalten. In der folgende Tabelle wird beschrieben, wie dies möglich ist.

Aufgabe	Service-Name	Service-Status/Aktion
Überprüfen Sie, ob ein Agent ausgeführt wird	AWS Discovery Agent	Gestartet
	AWS Discovery Updater	
Starten Sie einen Agenten	AWS Discovery-Agent	Wählen Sie Starten

Aufgabe	Service-Name	Service-Status/Aktion
	AWS Discovery Updater	
Beenden Sie einen Agenten	AWS Discovery-Agent AWS Discovery Updater	Wählen Sie Stop (Anhalten) aus
Starten Sie einen Agenten neu	AWS Discovery-Agent AWS Discovery Updater	Klicken Sie auf Restart (Neu starten).

Discovery Agent wird deinstalliert

Auf dieser Seite wird beschrieben, wie Sie den Discovery Agent unter Linux und Microsoft Windows deinstallieren.

Deinstallieren Sie Discovery Agent unter Linux

In diesem Abschnitt wird beschrieben, wie Sie Discovery Agent unter Linux deinstallieren.

Um einen Agenten zu deinstallieren, wenn Sie den Yum-Paketmanager verwenden

- Verwenden Sie den folgenden Befehl, um einen Agenten zu deinstallieren, wenn Sie Yum verwenden.

```
rpm -e --nodeps aws-discovery-agent
```

Um einen Agenten zu deinstallieren, wenn Sie den Paketmanager apt-get verwenden

- Verwenden Sie den folgenden Befehl, um einen Agenten zu deinstallieren, wenn Sie apt-get verwenden.

```
apt-get remove aws-discovery-agent:i386
```

Um einen Agenten zu deinstallieren, wenn Sie den Zypper-Paketmanager verwenden

- Verwenden Sie den folgenden Befehl, um einen Agenten zu deinstallieren, wenn Sie Zypper verwenden.

```
zypper remove aws-discovery-agent
```

Deinstallieren Sie Discovery Agent unter Microsoft Windows

In diesem Abschnitt wird beschrieben, wie Sie Discovery Agent unter Microsoft Windows deinstallieren.

So deinstallieren Sie einen Erkennungsagenten unter Windows

1. Öffnen Sie die Systemsteuerung in Windows.
2. Wählen Sie Programme.
3. Wählen Sie Programme und Funktionen.
4. Wählen Sie AWS Discovery Agent aus.
5. Wählen Sie Deinstallieren.

Note

Wenn Sie den Agenten nach der Deinstallation erneut installieren möchten, führen Sie den folgenden Befehl mit den `/norestart` Optionen `/repair` und aus.

```
.\AWSDiscoveryAgentInstaller.exe REGION="your-home-region" KEY_ID="aws-access-key-id" KEY_SECRET="aws-secret-access-key" /quiet /repair /norestart
```

Um einen Discovery Agent unter Windows über die Befehlszeile zu deinstallieren

1. Rechtsklicken Sie auf Start.
2. Wählen Sie Command Prompt.

3. Verwenden Sie den folgenden Befehl, um einen Discovery Agent unter Windows zu deinstallieren.

```
wmic product where name='AWS Discovery Agent' call uninstall
```

Note

Wenn die .exe Datei auf dem Server vorhanden ist, können Sie den Agent mithilfe des folgenden Befehls vollständig vom Server deinstallieren. Wenn Sie diesen Befehl zur Deinstallation verwenden, müssen Sie bei der Neuinstallation des Agenten die `/norestart` Optionen `/repair` und nicht verwenden.

```
.\AWSDiscoveryAgentInstaller.exe /quiet /uninstall
```

Die Datenerfassung durch den Discovery Agent starten und beenden

Wenn der Discovery Agent nach der Bereitstellung und Konfiguration nicht mehr erfasst wird, können Sie ihn neu starten. Sie können die Datenerfassung über die Konsole starten oder beenden [Datensammler in der AWS Migration Hub Konsole starten und stoppen](#), indem Sie die Schritte unter befolgen oder API-Aufrufe über die tätigen AWS CLI. Stellen Sie vor dem Start sicher, dass Sie die für die Verwaltung des Discovery Agents erforderlichen [Zugriffsschlüssel](#) generieren.

Um das zu installieren AWS CLI und die Datenerfassung zu starten oder zu beenden

1. Falls Sie dies noch nicht getan haben, installieren Sie das für Ihren Betriebssystemtyp (Windows oder Mac/Linux) AWS CLI geeignete. Anweisungen finden Sie im [AWS Command Line Interface Benutzerhandbuch](#).
2. Öffnen Sie die Eingabeaufforderung (Windows) oder das Terminal (MAC/Linux).
 - a. Geben Sie `aws configure` ein und drücken Sie die Eingabetaste.
 - b. Geben Sie Ihre AWS Zugangsschlüssel-ID und Ihren AWS geheimen Zugriffsschlüssel ein.
 - c. Geben Sie beispielsweise Ihre Heimatregion als Standardregionsnamen ein `us-west-2`. (In diesem Beispiel gehen wir davon aus, dass dies Ihre Heimatregion `us-west-2` ist.)

- d. Geben Sie als Standard-Ausgabeformat text ein.
3. Geben Sie den folgenden Befehl ein, um die ID des Agenten zu ermitteln, für den Sie die Datenerfassung beenden oder starten möchten:

```
aws discovery describe-agents
```

4. Geben Sie den folgenden Befehl ein, um die Datenerfassung durch den Agenten zu starten:

```
aws discovery start-data-collection-by-agent-ids --agent-ids <agent ID>
```

Geben Sie den folgenden Befehl ein, um die Datenerfassung durch den Agenten zu beenden:

```
aws discovery stop-data-collection-by-agent-ids --agent-ids <agent ID>
```

Problembehandlung bei Discovery Agent

Diese Seite behandelt die Fehlerbehebung für den Discovery Agent unter Linux und Microsoft Windows.

Fehlerbehebung bei Discovery Agent unter Linux

Wenn bei der Installation oder Verwendung des Discovery Agent unter Linux Probleme auftreten, lesen Sie die folgenden Anleitungen zur Protokollierung und Konfiguration. Bei der Behebung potenzieller Probleme mit dem Agenten oder seiner Verbindung zum Application Discovery Service fordert der AWS Support häufig diese Dateien an.

- Protokolldateien

Die Protokolldateien für Discovery Agent befinden sich im folgenden Verzeichnis.

```
/var/log/aws/discovery/
```

Protokolldateien werden so benannt, dass sie angeben, ob sie vom Haupt-Daemon, dem automatischen Upgrader oder dem Installationsprogramm generiert wurden.

- Konfigurationsdateien

Die Konfigurationsdateien für Discovery Agent Version 2.0.1617.0 oder neuer befinden sich im folgenden Verzeichnis.

```
/etc/opt/aws/discovery/
```

Konfigurationsdateien für Versionen von Discovery Agent vor 2.0.1617.0 befinden sich im folgenden Verzeichnis.

```
/var/opt/aws/discovery/
```

- Anweisungen zum Entfernen älterer Versionen des Discovery Agent finden Sie unter [Voraussetzungen für Discovery Agent](#)

Problembehandlung für Discovery Agent unter Microsoft Windows

Wenn bei der Installation oder Verwendung des AWS Application Discovery Agent unter Microsoft Windows Probleme auftreten, lesen Sie die folgenden Anleitungen zur Protokollierung und Konfiguration. AWS Support fordert diese Dateien häufig an, um mögliche Probleme mit dem Agenten oder seiner Verbindung zum Application Discovery Service zu beheben.

- Protokollierung der Installation

In einigen Fällen scheint der Installationsbefehl für den Agenten fehl zu schlagen. Beispielsweise kann ein Fehler bei dem Windows Services Manager auftreten, der besagt, dass die Erkennungsdienste nicht erstellt werden. Fügen Sie dem Befehl in diesem Fall `/log install.log` hinzu, um ein ausführliches Installationsprotokoll zu erstellen.

- Betriebsprotokollierung

Unter Windows Server 2008 und höher finden Sie Agenten-Protokolldateien in dem folgenden Verzeichnis.

```
C:\ProgramData\AWS\AWS Discovery\Logs
```

Unter Windows Server 2003 finden Sie Agenten-Protokolldateien in dem folgenden Verzeichnis.

```
C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\Logs
```

Die Namen der Protokolldateien geben an, ob sie vom Hauptdienst, von automatischen Upgrades oder vom Installationsprogramm generiert wurden.

- Konfigurationsdatei

Unter Windows Server 2008 und höher finden Sie die Agenten-Konfigurationsdatei in dem folgenden Verzeichnis.

C:\ProgramData\AWS\AWS Discovery\config

Unter Windows Server 2003 finden Sie die Agenten-Konfigurationsdatei in dem folgenden Verzeichnis.

C:\Documents and Settings\All Users\Application Data\AWS\AWS Discovery\config

- Anweisungen zum Entfernen früherer Versionen des Discovery Agents finden Sie unter [Voraussetzungen für Discovery Agent](#).

Agentloser Collector für Application Discovery Service

Application Discovery Service Agentless Collector (Agentless Collector) ist eine lokale Anwendung, die mithilfe agentenloser Methoden Informationen über Ihre lokale Umgebung sammelt, darunter Serverprofilinformationen (z. B. Betriebssystem, Anzahl, Größe des RAM) CPUs, Datenbankmetadaten, Nutzungsmetriken und Daten über den Netzwerkverkehr zwischen lokalen Servern. Sie installieren den Agentless Collector als virtuelle Maschine (VM) in Ihrer VMware vCenter Server-Umgebung mithilfe einer Open Virtualization Archive (OVA) -Datei.

Agentless Collector verfügt über eine modulare Architektur, die die Verwendung mehrerer agentenloser Erfassungsmethoden ermöglicht. Agentless Collector bietet Module für die Datenerfassung von VMware VMs und von Datenbank- und Analyseservern. Es bietet auch ein Modul zum Sammeln von Daten über den Netzwerkverkehr zwischen Ihren lokalen Servern.

Agentless Collector unterstützt die Datenerfassung für AWS Application Discovery Service (Application Discovery Service), indem Nutzungs- und Konfigurationsdaten über Ihre lokalen Server und Datenbanken sowie Daten über den Netzwerkverkehr zwischen Ihren lokalen Servern gesammelt werden.

Der Application Discovery Service ist in einen Service integriert AWS Migration Hub, der Ihre Migrationsverfolgung vereinfacht, da er Ihre Migrationsstatusinformationen in einer einzigen Konsole zusammenfasst. Sie können die erkannten Server anzeigen, Amazon EC2 EC2-Empfehlungen abrufen, Netzwerkverbindungen visualisieren, Server zu Anwendungen gruppieren und dann den Migrationsstatus jeder Anwendung von der Migration Hub Hub-Konsole in Ihrer Heimatregion aus verfolgen.

Das Agentless Collector Datenbank- und Analysedatenerfassungsmodul ist in AWS Database Migration Service (AWS DMS) integriert. Diese Integration hilft Ihnen bei der Planung Ihrer Migration zum AWS Cloud. Sie können das Modul zur Erfassung von Datenbank- und Analysedaten verwenden, um Datenbank- und Analyseserver in Ihrer Umgebung zu ermitteln und eine Bestandsaufnahme der Server zu erstellen, auf die Sie migrieren möchten AWS Cloud. Dieses Datenerfassungsmodul erfasst Datenbankmetadaten und Messdaten zur tatsächlichen Auslastung von CPU, Arbeitsspeicher und Festplattenkapazität. Nachdem Sie diese Metriken erfasst haben, können Sie die AWS DMS Konsole verwenden, um Zielempfehlungen für Ihre Quelldatenbanken zu generieren.

Voraussetzungen für Agentless Collector

Im Folgenden sind die Voraussetzungen für die Verwendung von Application Discovery Service Agentless Collector (Agentless Collector) aufgeführt:

- Ein oder mehrere AWS Konten.
- Ein AWS Konto mit AWS Migration Hub festgelegter Heimatregion, siehe [Melden Sie sich bei der Migration Hub Hub-Konsole an und wählen Sie eine Heimatregion](#). Ihre Migration Hub Hub-Daten werden in Ihrer Heimatregion zu Ermittlungs-, Planungs- und Migrationsverfolgungszwecken gespeichert.
- Ein AWS Konto-IAM-Benutzer, der für die Verwendung der AWS verwalteten Richtlinie `AWSServiceCatalogAgentlessCollectorAccess` eingerichtet ist. Um das Modul zur Erfassung von Datenbank- und Analysedaten verwenden zu können, muss dieser IAM-Benutzer außerdem zwei vom Kunden verwaltete IAM-Richtlinien verwenden: `DMSCollectorPolicy` und `FleetAdvisorS3Policy`. Weitere Informationen finden Sie unter [Bereitstellung von Application Discovery Service Agentless Collector](#). Der IAM-Benutzer muss in einem AWS Konto erstellt werden, für das die Heimatregion von Migration Hub festgelegt ist.
- VMware vCenter Server V5.5, V6, V6.5, 6.7 oder 7.0.

Note

Der Agentless Collector unterstützt alle diese Versionen von VMware, aber wir testen derzeit mit den Versionen 6.7 und 7.0.

- Stellen Sie für die Einrichtung von VMware vCenter Server sicher, dass Sie vCenter-Anmeldeinformationen mit den für die Systemgruppe festgelegten Lese- und Anzeigeberechtigungen angeben können.
- Agentless Collector benötigt ausgehenden Zugriff über TCP-Port 443 auf mehrere Domänen. AWS Eine Liste dieser Domänen finden Sie unter [Konfigurieren Sie die Firewall für den ausgehenden Zugriff auf Domänen AWS](#)
- Um das Modul zur Erfassung von Datenbank- und Analysedaten zu verwenden, erstellen Sie einen Amazon S3 S3-Bucket in der Region AWS-Region, die Sie als Ihre Migration Hub Hub-Heimatregion festgelegt haben. Die Module zur Erfassung von Datenbank- und Analysedaten speichern Inventarmetadaten in diesem Amazon S3 S3-Bucket. Weitere Informationen finden Sie unter [Erstellen eines Buckets](#) im Amazon-S3-Benutzerhandbuch.
- Agentless Collector Version 2 erfordert ESXi 6.5 oder eine neuere Version.

Datenperimeter für den Zugriff auf Ressourcen im Besitz des AWS konfigurieren

Die automatische Aktualisierungsfunktion von Agentless Collector ruft Updates in Form von Docker-Images aus einem öffentlichen ECR-Repository des Dienstes ab AWS . Wenn Sie Datenperimeter verwenden, um den Zugriff auf Amazon ECR in Ihrer Umgebung zu kontrollieren, müssen Sie möglicherweise den Zugriff auf Folgendes explizit zulassen, um die automatische Aktualisierungsfunktion nutzen zu können:

- Ressource, für die Zugriff erforderlich ARNs ist: `arn:aws:ecr-public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b`
- Erforderliche Berechtigungen: `ecr-public:DescribeImages`

Konfigurieren Sie die Firewall für den ausgehenden Zugriff auf Domänen AWS

Wenn ausgehende Verbindungen aus Ihrem Netzwerk eingeschränkt sind, müssen Sie Ihre Firewall-Einstellungen aktualisieren, um ausgehenden Zugriff auf die AWS Domänen zu ermöglichen, die Agentless Collector benötigt. Welche AWS Domains ausgehenden Zugriff erfordern, hängt davon ab, ob Ihre Heimatregion von Migration Hub die Region USA West (Oregon), US-West-2 oder eine andere Region ist.

Für die folgenden Domains ist ausgehender Zugriff erforderlich, wenn die Heimatregion Ihres AWS Kontos US-West-2 ist:

- `arsenal-discovery.us-west-2.amazonaws.com`— Der Collector verwendet diese Domain, um zu überprüfen, ob sie mit den erforderlichen IAM-Benutzeranmeldedaten konfiguriert ist. Der Collector verwendet es auch zum Senden und Speichern gesammelter Daten, da die Heimatregion us-west-2 ist.
- `migrationhub-config.us-west-2.amazonaws.com`— Der Collector verwendet diese Domain, um anhand der angegebenen IAM-Benutzeranmeldedaten zu ermitteln, in welche Heimatregion der Collector Daten sendet.
- `api.ecr-public.us-east-1.amazonaws.com`— Der Collector verwendet diese Domain, um verfügbare Updates zu ermitteln.
- `public.ecr.aws`— Der Collector verwendet diese Domain zum Herunterladen der Updates.

- `dms.your-migrationhub-home-region.amazonaws.com`— Der Collector verwendet diese Domain, um eine Verbindung zum AWS DMS Datensammelpunkt herzustellen.
- `s3.amazonaws.com`— Der Collector verwendet diese Domain, um Daten, die vom Datenbank- und Analysedatenerfassungsmodul gesammelt wurden, in Ihren Amazon S3 S3-Bucket hochzuladen.
- `sts.amazonaws.com`— Der Collector verwendet diese Domain, um zu verstehen, mit welchem Konto der Collector konfiguriert wurde.

Für die folgenden Domains ist ausgehender Zugriff erforderlich, falls dies nicht **us-west-2** in der Heimatregion Ihres AWS Kontos der Fall ist:

- `arsenal-discovery.us-west-2.amazonaws.com`— Der Collector verwendet diese Domain, um zu überprüfen, ob sie mit den erforderlichen IAM-Benutzeranmeldeinformationen konfiguriert ist.
- `arsenal-discovery.your-migrationhub-home-region.amazonaws.com`— Der Collector verwendet diese Domain zum Senden und Speichern der gesammelten Daten.
- `migrationhub-config.us-west-2.amazonaws.com`— Der Collector verwendet diese Domain, um anhand der bereitgestellten IAM-Benutzeranmeldedaten zu bestimmen, an welche Heimatregion der Collector Daten senden soll.
- `api.ecr-public.us-east-1.amazonaws.com`— Der Collector verwendet diese Domain, um verfügbare Updates zu ermitteln.
- `public.ecr.aws`— Der Collector verwendet diese Domain zum Herunterladen der Updates.
- `dms.your-migrationhub-home-region.amazonaws.com`— Der Collector verwendet diese Domain, um eine Verbindung zum AWS DMS Datensammelpunkt herzustellen.
- `s3.amazonaws.com`— Der Collector verwendet diese Domain, um Daten, die vom Datenbank- und Analysedatenerfassungsmodul gesammelt wurden, in Ihren Amazon S3 S3-Bucket hochzuladen.
- `sts.amazonaws.com`— Der Collector verwendet diese Domain, um zu verstehen, mit welchem Konto der Collector konfiguriert wurde.

Bei der Einrichtung von Agentless Collector erhalten Sie möglicherweise folgende Fehler: Setup ist fehlgeschlagen — Überprüfen Sie Ihre Anmeldeinformationen und versuchen Sie es erneut, da sonst AWS keine Verbindung hergestellt werden kann. Bitte überprüfen Sie die Netzwerkeinstellungen. Diese Fehler können durch einen fehlgeschlagenen Versuch des Agentless Collectors verursacht

werden, eine HTTPS-Verbindung zu einer der AWS Domänen herzustellen, auf die er ausgehenden Zugriff benötigt.

Wenn keine Verbindung zu hergestellt werden AWS kann, kann Agentless Collector keine Daten aus Ihrer lokalen Umgebung sammeln. Informationen darüber, wie Sie die Verbindung zu reparieren haben AWS, finden Sie unter. [Behebung des Problems, das Agentless Collector AWS während der Installation nicht erreichen kann](#)

Bereitstellung von Application Discovery Service Agentless Collector

Um Application Discovery Service Agentless Collector bereitzustellen, müssen Sie zunächst einen IAM-Benutzer erstellen und den Collector herunterladen. Auf dieser Seite werden Sie durch die Schritte zur Bereitstellung eines Collectors geführt.

Erstellen Sie einen IAM-Benutzer für Agentless Collector

Um Agentless Collector verwenden zu können, müssen Sie in dem AWS Konto, das Sie verwendet haben [Melden Sie sich bei der Migration Hub Hub-Konsole an und wählen Sie eine Heimatregion](#), einen AWS Identity and Access Management (IAM-) Benutzer erstellen. Richten Sie diesen IAM-Benutzer dann so ein, dass er die folgende AWS verwaltete Richtlinie verwendet. [AWSApplicationDiscoveryAgentlessCollectorAccess](#) Sie fügen diese IAM-Richtlinie bei der Erstellung des IAM-Benutzers hinzu.

Um das Modul zur Erfassung von Datenbank- und Analysedaten zu verwenden, erstellen Sie zwei vom Kunden verwaltete IAM-Richtlinien. Diese Richtlinien ermöglichen den Zugriff auf Ihren Amazon S3 S3-Bucket und die AWS DMS API. Weitere Informationen finden Sie unter [Erstellen einer vom Kunden verwalteten Richtlinie](#) im IAM-Benutzerhandbuch.

- Verwenden Sie den folgenden JSON-Code, um die **DMSCollectorPolicy** Richtlinie zu erstellen.
JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
```

```

        "dms:DescribeFleetAdvisorCollectors",
        "dms:ModifyFleetAdvisorCollectorStatuses",
        "dms:UploadFileMetadataList"
    ],
    "Resource": "*"
  }]
}

```

- Verwenden Sie den folgenden JSON-Code, um die **FleetAdvisorS3Policy** Richtlinie zu erstellen.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:DeleteObject*",
        "s3:PutObject*"
      ],
      "Resource": [
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
      ]
    }
  ]
}

```

Ersetzen Sie es im vorherigen Beispiel *bucket_name* durch den Namen des Amazon S3 S3-Buckets, den Sie im Schritt Voraussetzungen erstellt haben.

Wir empfehlen, dass Sie einen IAM-Benutzer ohne Administratorrechte für die Verwendung mit Agentless Collector erstellen. Wenn Sie IAM-Benutzer ohne Administratorrechte erstellen, befolgen Sie die bewährte Sicherheitsmethode Grant Least [Privilege, d. h. gewähren Sie Benutzern Mindestberechtigungen](#).

Um einen IAM-Benutzer ohne Administratorrechte zur Verwendung mit Agentless Collector zu erstellen

1. Navigieren Sie in AWS-Managementkonsole zur IAM-Konsole und verwenden Sie dabei das AWS Konto, mit dem Sie die Heimatregion eingerichtet haben. [Melden Sie sich bei der Migration Hub Hub-Konsole an und wählen Sie eine Heimatregion](#)
2. Erstellen Sie einen IAM-Benutzer ohne Administratorrechte, indem Sie den Anweisungen zum Erstellen eines Benutzers mit der Konsole folgen, wie unter [Erstellen eines IAM-Benutzers in Ihrem AWS Konto im](#) IAM-Benutzerhandbuch beschrieben.

Folgen Sie dabei den Anweisungen im IAM-Benutzerhandbuch:

- Wählen Sie im Schritt zur Auswahl des Zugriffstyps die Option Programmatischer Zugriff aus. Hinweis: Wählen Sie den Zugriff auf die AWS Managementkonsole nur aus, wenn Sie dieselben IAM-Benutzeranmeldedaten für den Zugriff auf die AWS Konsole verwenden möchten.
- Wählen Sie im nächsten Schritt auf der Seite „Berechtigungen festlegen“ die Option „Bestehende Richtlinien direkt an den Benutzer anhängen“. Wählen Sie dann die `AWSServiceCatalogAgentlessCollectorAccess` AWS verwaltete Richtlinie aus der Liste der Richtlinien aus.

Wählen Sie als Nächstes die `DMSCollectorPolicy` und vom `FleetAdvisorS3Policy` Kunden verwalteten IAM-Richtlinien aus.

- Wenn Sie sich die Zugangsschlüssel des Benutzers (Zugriffsschlüssel IDs und geheime Zugangsschlüssel) ansehen, folgen Sie den Anweisungen im Abschnitt Wichtiger Hinweis zum Speichern der neuen Zugriffsschlüssel-ID und des geheimen Zugangsschlüssels des Benutzers an einem sicheren Ort. Sie benötigen diese Zugangsschlüssel in [Agentless Collector konfigurieren](#).

Es ist eine bewährte AWS Sicherheitsmethode, die Zugangsschlüssel abwechselnd zu verwenden. Informationen zur Rotation von Schlüsseln finden Sie im IAM-Benutzerhandbuch unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#).

Laden Sie den Agentless Collector herunter

Um den Application Discovery Service Agentless Collector (Agentless Collector) einzurichten, müssen Sie die Agentless Collector Open Virtualization Archive (OVA) -Datei herunterladen und bereitstellen. Der Agentless Collector ist eine virtuelle Appliance, die Sie in Ihrer lokalen Umgebung installieren. VMware In diesem Schritt wird beschrieben, wie Sie die Collector-OVA-Datei herunterladen, und im nächsten Schritt wird beschrieben, wie Sie sie bereitstellen.

Um die Collector-OVA-Datei herunterzuladen und ihre Prüfsumme zu überprüfen

1. Melden Sie sich als VMware Administrator bei vCenter an und wechseln Sie zu dem Verzeichnis, in das Sie die Agentless Collector OVA-Datei herunterladen möchten.
2. Laden Sie die OVA-Datei von der folgenden URL herunter:

[Agentenloser Collector OVA](#)

3. Je nachdem, welchen Hash-Algorithmus Sie in Ihrer Systemumgebung verwenden, laden Sie entweder das [MD5](#) oder herunter, [SHA256](#) um die Datei mit dem Prüfsummenwert abzurufen. Verwenden Sie den heruntergeladenen Wert, um die im vorherigen ApplicationDiscoveryServiceAgentlessCollector Schritt heruntergeladene Datei zu überprüfen.
4. Führen Sie je nach Linux-Variante den entsprechenden MD5 Befehl oder SHA256 Befehl der Version aus, um zu überprüfen, ob die kryptografische Signatur der ApplicationDiscoveryServiceAgentlessCollector.oVa Datei mit dem Wert in der entsprechenden SHA256 Datei MD5/übereinstimmt, die Sie heruntergeladen haben.

```
$ md5sum ApplicationDiscoveryServiceAgentlessCollector.oVa
```

```
$ sha256sum ApplicationDiscoveryServiceAgentlessCollector.oVa
```

Stellen Sie Agentless Collector bereit

Application Discovery Service Agentless Collector (Agentless Collector) ist eine virtuelle Appliance, die Sie in Ihrer lokalen VMware Umgebung installieren. In diesem Abschnitt wird beschrieben, wie Sie die Open Virtualization Archive (OVA) -Datei, die Sie heruntergeladen haben, in Ihrer Umgebung bereitstellen. VMware

Technische Daten der virtuellen Maschine mit Agentless Collector

Agentless Collector version 2

- Betriebssystem — Amazon Linux 2023
- Arbeitsspeicher — 16 GB
- CPU — 4 Kerne
- VMware Anforderungen — Weitere Informationen finden Sie unter [VMware Hostanforderungen für die Ausführung AL2023 auf VMware](#)

Agentless Collector version 1

- Betriebssystem — Amazon Linux 2
- Arbeitsspeicher — 16 GB
- CPU — 4 Kerne

Das folgende Verfahren führt Sie durch die Bereitstellung der Agentless Collector OVA-Datei in Ihrer VMware Umgebung.

So stellen Sie Agentless Collector bereit

1. Melden Sie sich als VMware Administrator bei vCenter an.
2. Verwenden Sie eine der folgenden Methoden, um die OVA-Datei zu installieren:
 - Verwenden Sie die Benutzeroberfläche: Wählen Sie „Datei“, wählen Sie „OVF-Vorlage bereitstellen“, wählen Sie die Collector-OVA-Datei aus, die Sie im vorherigen Abschnitt heruntergeladen haben, und schließen Sie dann den Assistenten ab. Stellen Sie sicher, dass die Proxyeinstellungen im Servermanagement-Dashboard korrekt konfiguriert sind.
 - Verwenden Sie die Befehlszeile: Um die Collector-OVA-Datei von der Befehlszeile aus zu installieren, laden Sie das VMware Open Virtualization Format Tool (ovftool) herunter und verwenden Sie es. Um ovftool herunterzuladen, wählen Sie auf der Dokumentationsseite des [OVF-Tools](#) eine Version aus.

Im Folgenden finden Sie ein Beispiel für die Verwendung des Befehlszeilentools ovftool zur Installation der Collector-OVA-Datei.

```
ovftool --acceptAllEulas --name=AgentlessCollector --datastore=datastore1
--dm=thin ApplicationDiscoveryServiceAgentlessCollector.ova
'vi://username:password@vcenterurl/Datacenter/host/esxi/'
```

Im Folgenden werden die *replaceable* Werte im Beispiel beschrieben

- Der Name ist der Name, den Sie für Ihre Agentless Collector-VM verwenden möchten.
 - Der Datenspeicher ist der Name des Datenspeichers in Ihrem vCenter.
 - Der OVA-Dateiname ist der Name der heruntergeladenen Collector-OVA-Datei.
 - Das username/password sind Ihre vCenter-Anmeldeinformationen.
 - Die vcenterurl ist die URL Ihres vCenter.
 - Der VI-Pfad ist der Pfad zu Ihrem Host. VMware ESXi
3. Suchen Sie den bereitgestellten Agentless Collector in Ihrem vCenter. Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie dann Power, Power On.
 4. Nach einigen Minuten wird die IP-Adresse des Collectors in vCenter angezeigt. Sie verwenden diese IP-Adresse, um eine Verbindung zum Collector herzustellen.

Zugriff auf die Agentless Collector-Konsole

Das folgende Verfahren beschreibt, wie Sie auf die Application Discovery Service Agentless Collector (Agentless Collector) -Konsole zugreifen.

So greifen Sie auf die Agentless Collector-Konsole zu

1. Öffnen Sie einen Webbrowser und geben Sie dann die folgende URL in die Adressleiste ein: **https:// <ip_address>/**, woher *<ip_address>* die IP-Adresse des Collectors stammt [Stellen Sie Agentless Collector bereit](#).
2. Wählen Sie Erste Schritte, wenn Sie zum ersten Mal auf Agentless Collector zugreifen. Danach werden Sie aufgefordert, sich anzumelden.

Wenn Sie zum ersten Mal auf die Agentless Collector-Konsole zugreifen, tun Sie dies als Nächstes. [Agentless Collector konfigurieren](#) Andernfalls werden Sie als Nächstes sehen [Das Agentless Collector-Dashboard](#).

Agentless Collector konfigurieren

Application Discovery Service Agentless Collector (Agentless Collector) ist eine auf Amazon Linux 2 basierende virtuelle Maschine (VM). Im folgenden Abschnitt wird beschrieben, wie Sie eine Collector-VM auf der Seite „Agentless Collector konfigurieren“ der Agentless Collector-Konsole konfigurieren.

So konfigurieren Sie eine Collector-VM auf der Seite „Agentless Collector konfigurieren“

1. Geben Sie unter Collector-Name einen Namen für den Collector ein, um ihn zu identifizieren. Der Name kann Leerzeichen, aber keine Sonderzeichen enthalten.
2. Geben Sie unter Datensynchronisierung den AWS Zugriffsschlüssel und den geheimen Schlüssel für den AWS Konto-IAM-Benutzer ein, der als Zielkonto für den Empfang der vom Collector erkannten Daten angegeben werden soll. Informationen zu den Anforderungen für den IAM-Benutzer finden Sie unter. [Bereitstellung von Application Discovery Service Agentless Collector](#)
 - a. Geben Sie für den AWS Zugriffsschlüssel den Zugriffsschlüssel des AWS Konto-IAM-Benutzers ein, den Sie als Zielkonto angeben.
 - b. Geben Sie unter AWS Secret-Key den geheimen Schlüssel des IAM-Benutzers des AWS Kontos ein, den Sie als Zielkonto angeben.
 - c. (Optional) Wenn Ihr Netzwerk die Verwendung eines Proxys für den Zugriff erfordert AWS, geben Sie den Proxyhost, den Proxy-Port und optional die Anmeldeinformationen ein, die für die Authentifizierung bei Ihrem vorhandenen Proxy-Server erforderlich sind.
3. Richten Sie unter Agentless Collector-Passwort ein Passwort ein, mit dem der Zugriff auf Agentless Collector authentifiziert werden soll.
 - Passwörter unterscheiden Groß- und Kleinschreibung
 - Passwörter müssen zwischen 8 und 64 Zeichen lang sein
 - Passwörter müssen mindestens ein Zeichen aus jeder der folgenden vier Kategorien enthalten:
 - Kleinbuchstaben (a – z)
 - Großbuchstaben (A – Z)
 - Zahlen (0 – 9)
 - Nicht-alphanumerische Zeichen (@\$! #%*? &)
 - Passwörter dürfen keine anderen Sonderzeichen als die folgenden enthalten: @\$! #%*? &
 - a. Geben Sie für das Agentless Collector-Passwort ein Passwort ein, mit dem der Zugriff auf den Collector authentifiziert werden soll.
 - b. Wenn Sie das Agentless Collector-Passwort erneut eingeben möchten, geben Sie das Passwort zur Bestätigung erneut ein.

4. Lesen Sie unter Andere Einstellungen die Lizenzvereinbarung. Wenn Sie damit einverstanden sind, sie zu akzeptieren, aktivieren Sie das Kontrollkästchen.
5. Um automatische Updates für Agentless Collector zu aktivieren, wählen Sie unter Andere Einstellungen die Option Agentless Collector automatisch aktualisieren aus. Wenn Sie dieses Kontrollkästchen nicht aktivieren, müssen Sie Agentless Collector manuell aktualisieren, wie unter beschrieben. [Manuelles Aktualisieren von Application Discovery Service Agentless Collector](#)
6. Wählen Sie Konfigurationen speichern.

In den folgenden Themen werden optionale Collector-Konfigurationsaufgaben beschrieben.

Optionale Konfigurationsaufgaben

- [\(Optional\) Konfigurieren Sie eine statische IP-Adresse für die Agentless Collector-VM](#)
- [\(Optional\) Setzen Sie die Agentless Collector-VM wieder auf DHCP zurück](#)
- [\(Optional\) Konfigurieren Sie das Kerberos-Authentifizierungsprotokoll](#)

(Optional) Konfigurieren Sie eine statische IP-Adresse für die Agentless Collector-VM

In den folgenden Schritten wird beschrieben, wie Sie eine statische IP-Adresse für die VM Application Discovery Service Agentless Collector (Agentless Collector) konfigurieren. Bei der ersten Installation ist die Collector-VM für die Verwendung des Dynamic Host Configuration Protocol (DHCP) konfiguriert.

Note

Der Agentless Collector unterstützt IPv4. Er unterstützt IPv6 nicht.

Agentless Collector version 2

Um eine statische IP-Adresse für die Collector-VM zu konfigurieren

1. Sammeln Sie die folgenden Netzwerkinformationen von VMware vCenter:
 - Statische IP-Adresse — Eine unsignierte IP-Adresse im Subnetz. Zum Beispiel 192.168.1.138.

- CIDR-Netzmaske — Um die CIDR-Netzmaske abzurufen, überprüfen Sie die IP-Adresseinstellung des VMware vCenter-Hosts, der die Collector-VM hostet. Zum Beispiel /24.
 - Standard-Gateway — Um das Standard-Gateway zu erhalten, überprüfen Sie die IP-Adresseinstellung des VMware vCenter-Hosts, der die Collector-VM hostet. Zum Beispiel 192.168.1.1.
 - Primärer DNS — Um den primären DNS abzurufen, überprüfen Sie die IP-Adresseinstellung des VMware vCenter-Hosts, der die Collector-VM hostet. Zum Beispiel 192.168.1.1.
 - (Optional) Sekundäres DNS
 - (Optional) Lokaler Domänenname — Dadurch kann der Collector die vCenter-Host-URL ohne den Domännennamen erreichen.
2. Öffnen Sie die VM-Konsole des Collectors und melden Sie sich **ec2-user** mit dem Passwort an, **collector** wie im folgenden Beispiel gezeigt.

```
username: ec2-user
password: collector
```

3. Deaktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl in das Remote-Terminal eingeben.

```
sudo ip link set ens192 down
```

4. Aktualisieren Sie die Schnittstellenkonfiguration mithilfe der folgenden Schritte.

- a. Öffnen Sie cloud-init-ens 10-192.network im vi-Editor mit dem folgenden Befehl.

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

- b. Aktualisieren Sie die Werte, wie im folgenden Beispiel gezeigt, mit den Informationen, die Sie im Schritt Netzwerkinformationen sammeln gesammelt haben.

```
[Match]
Name=ens192

[Network]
DHCP=no
Address=static-ip-value/CIDR-netmask
```

```
Gateway=gateway-value  
DNS=dnserver-value
```

5. Aktualisieren Sie das Domain Name System (DNS) mithilfe der folgenden Schritte.

a. Öffnen Sie die `resolv.conf` Datei in vi mit dem folgenden Befehl.

```
sudo vi /etc/resolv.conf
```

b. Aktualisieren Sie die `resolv.conf` Datei in vi mit dem folgenden Befehl.

```
search localdomain-name  
options timeout:2 attempts:5  
nameserver dnserver-value
```

Das folgende Beispiel zeigt eine bearbeitete `resolv.conf` Datei.

```
search vsphere.local  
options timeout:2 attempts:5  
nameserver 192.168.1.1
```

6. Aktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl eingeben.

```
sudo ip link set ens192 up
```

7. Starten Sie die VM neu, wie im folgenden Beispiel gezeigt.

```
sudo reboot
```

8. Überprüfen Sie Ihre Netzwerkeinstellungen mithilfe der folgenden Schritte.

a. Überprüfen Sie, ob die IP-Adresse korrekt konfiguriert ist, indem Sie die folgenden Befehle eingeben.

```
ifconfig  
ip addr show
```

b. Überprüfen Sie, ob das Gateway korrekt hinzugefügt wurde, indem Sie den folgenden Befehl eingeben.

```
route -n
```

Die Ausgabe sollte dem folgenden Beispiel ähneln.

```
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use
Iface
0.0.0.0          192.168.1.1    0.0.0.0         UG    0      0      0 eth0
172.17.0.0       0.0.0.0        255.255.0.0     U    0      0      0
docker0
192.168.1.0      0.0.0.0        255.255.255.0   U    0      0      0
```

- c. Stellen Sie sicher, dass Sie eine öffentliche URL pingen können, indem Sie den folgenden Befehl eingeben.

```
ping www.google.com
```

- d. Stellen Sie sicher, dass Sie die vCenter-IP-Adresse oder den Hostnamen wie im folgenden Beispiel gezeigt pingen können.

```
ping vcenter-host-url
```

Agentless Collector version 1

Um eine statische IP-Adresse für die Collector-VM zu konfigurieren

1. Sammeln Sie die folgenden Netzwerkinformationen von VMware vCenter:
 - Statische IP-Adresse — Eine unsignierte IP-Adresse im Subnetz. Zum Beispiel 192.168.1.138.
 - Netzwerkmaske — Um die Netzwerkmaske abzurufen, überprüfen Sie die IP-Adresseinstellung des VMware vCenter-Hosts, der die Collector-VM hostet. Zum Beispiel 255.255.255.0.
 - Standard-Gateway — Um das Standard-Gateway zu erhalten, überprüfen Sie die IP-Adresseinstellung des VMware vCenter-Hosts, der die Collector-VM hostet. Zum Beispiel 192.168.1.1.
 - Primärer DNS — Um den primären DNS abzurufen, überprüfen Sie die IP-Adresseinstellung des VMware vCenter-Hosts, der die Collector-VM hostet. Zum Beispiel 192.168.1.1.

- (Optional) Sekundäres DNS
 - (Optional) Lokaler Domänenname — Dadurch kann der Collector die vCenter-Host-URL ohne den Domännennamen erreichen.
2. Öffnen Sie die VM-Konsole des Collectors und melden Sie sich **ec2-user** mit dem Passwort an, **collector** wie im folgenden Beispiel gezeigt.

```
username: ec2-user
password: collector
```

3. Deaktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl in das Remote-Terminal eingeben.

```
sudo /sbin/ifdown eth0
```

4. Aktualisieren Sie die Konfiguration der Schnittstelle eth0 mithilfe der folgenden Schritte.

- a. Öffnen Sie ifcfg-eth0 im vi-Editor mit dem folgenden Befehl.

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

- b. Aktualisieren Sie die Schnittstellenwerte, wie im folgenden Beispiel gezeigt, mit den Informationen, die Sie im Schritt Netzwerkinformationen sammeln gesammelt haben.

```
DEVICE=eth0
BOOTPROTO=static
ONBOOT=yes
IPADDR=static-ip-value
NETMASK=netmask-value
GATEWAY=gateway-value
TYPE=Ethernet
USERCTL=yes
PEERDNS=no
RES_OPTIONS="timeout:2 attempts:5"
```

5. Aktualisieren Sie das Domain Name System (DNS) mithilfe der folgenden Schritte.
- a. Öffnen Sie die `resolv.conf` Datei in vi mit dem folgenden Befehl.

```
sudo vi /etc/resolv.conf
```

- b. Aktualisieren Sie die `resolv.conf` Datei in vi mit dem folgenden Befehl.

```
search localdomain-name
options timeout:2 attempts:5
nameserver dnsserver-value
```

Das folgende Beispiel zeigt eine bearbeitete `resolv.conf` Datei.

```
search vsphere.local
options timeout:2 attempts:5
nameserver 192.168.1.1
```

6. Aktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl eingeben.

```
sudo /sbin/ifup eth0
```

7. Starten Sie die VM neu, wie im folgenden Beispiel gezeigt.

```
sudo reboot
```

8. Überprüfen Sie Ihre Netzwerkeinstellungen mithilfe der folgenden Schritte.

- a. Überprüfen Sie, ob die IP-Adresse korrekt konfiguriert ist, indem Sie die folgenden Befehle eingeben.

```
ifconfig
ip addr show
```

- b. Überprüfen Sie, ob das Gateway korrekt hinzugefügt wurde, indem Sie den folgenden Befehl eingeben.

```
route -n
```

Die Ausgabe sollte dem folgenden Beispiel ähneln.

```
Kernel IP routing table
Destination      Gateway          Genmask         Flags Metric Ref    Use
Iface
0.0.0.0          192.168.1.1     0.0.0.0         UG    0      0      0 eth0
```

172.17.0.0	0.0.0.0	255.255.0.0	U	0	0	0
docker0						
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	

- c. Stellen Sie sicher, dass Sie eine öffentliche URL pingen können, indem Sie den folgenden Befehl eingeben.

```
ping www.google.com
```

- d. Stellen Sie sicher, dass Sie die vCenter-IP-Adresse oder den Hostnamen wie im folgenden Beispiel gezeigt pingen können.

```
ping vcenter-host-url
```

(Optional) Setzen Sie die Agentless Collector-VM wieder auf DHCP zurück

In den folgenden Schritten wird beschrieben, wie Sie die Agentless Collector-VM für die Verwendung von DHCP neu konfigurieren.

Agentless Collector version 2

So konfigurieren Sie die Collector-VM für die Verwendung von DHCP

1. Deaktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl im Remote-Terminal ausführen.

```
sudo ip link set ens192 down
```

2. Aktualisieren Sie die Schnittstellenkonfiguration mithilfe der folgenden Schritte.
 - a. Öffnen Sie die `10-cloud-init-ens192.network` Datei mit dem folgenden Befehl im vi-Editor.

```
sudo vi /etc/systemd/network/10-cloud-init-ens192.network
```

- b. Aktualisieren Sie die Werte wie im folgenden Beispiel gezeigt.

```
[Match]
Name=ens192
```

```
[Network]
DHCP=yes

[DHCP]
ClientIdentifier=mac
```

3. Setzen Sie die DNS-Einstellung zurück, indem Sie den folgenden Befehl eingeben.

```
echo "" | sudo tee /etc/resolv.conf
```

4. Aktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl eingeben.

```
sudo ip link set ens192 up
```

5. Starten Sie die Collector-VM neu, wie im folgenden Beispiel gezeigt.

```
sudo reboot
```

Agentless Collector version 1

Um die Collector-VM für die Verwendung von DHCP zu konfigurieren

1. Deaktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl im Remote-Terminal ausführen.

```
sudo /sbin/ifdown eth0
```

2. Aktualisieren Sie die Netzwerkkonfiguration mithilfe der folgenden Schritte.

- a. Öffnen Sie die `ifcfg-eth0` Datei mit dem folgenden Befehl im vi-Editor.

```
sudo /sbin/ifdown eth0
```

- b. Aktualisieren Sie die Werte in der `ifcfg-eth0` Datei wie im folgenden Beispiel gezeigt.

```
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
TYPE=Ethernet
USERCTL=yes
```

```
PEERDNS=yes
DHCPV6C=yes
DHCPV6C_OPTIONS=-nw
PERSISTENT_DHCLIENT=yes
RES_OPTIONS="timeout:2 attempts:5"
```

3. Setzen Sie die DNS-Einstellung zurück, indem Sie den folgenden Befehl eingeben.

```
echo "" | sudo tee /etc/resolv.conf
```

4. Aktivieren Sie die Netzwerkschnittstelle, indem Sie den folgenden Befehl eingeben.

```
sudo /sbin/ifup eth0
```

5. Starten Sie die Collector-VM neu, wie im folgenden Beispiel gezeigt.

```
sudo reboot
```

(Optional) Konfigurieren Sie das Kerberos-Authentifizierungsprotokoll

Wenn Ihr Betriebssystemserver das Kerberos-Authentifizierungsprotokoll unterstützt, können Sie dieses Protokoll verwenden, um eine Verbindung zu Ihrem Server herzustellen. Dazu müssen Sie die Application Discovery Service Agentless Collector VM konfigurieren.

In den folgenden Schritten wird beschrieben, wie Sie das Kerberos-Authentifizierungsprotokoll auf Ihrer Application Discovery Service Agentless Collector-VM konfigurieren.

So konfigurieren Sie das Kerberos-Authentifizierungsprotokoll auf Ihrer Collector-VM

1. Öffnen Sie die VM-Konsole des Collectors und melden Sie sich **ec2-user** mit dem Passwort an, **collector** wie im folgenden Beispiel gezeigt.

```
username: ec2-user
password: collector
```

2. Öffnen Sie die `krb5.conf` Konfigurationsdatei im `/etc` Ordner. Dazu können Sie das folgende Codebeispiel verwenden.

```
cd /etc
sudo nano krb5.conf
```


3. Aktualisieren Sie die `krb5.conf` Konfigurationsdatei mit den folgenden Informationen.

```
[libdefaults]
    forwardable = true
    dns_lookup_realm = true
    dns_lookup_kdc = true
    ticket_lifetime = 24h
    renew_lifetime = 7d
    default_realm = default_Kerberos_realm

[realms]
default_Kerberos_realm = {
    kdc = KDC_hostname
    server_name = server_hostname
    default_domain = domain_to_expand_hostnames
}

[domain_realm]
.domain_name = default_Kerberos_realm
domain_name = default_Kerberos_realm
```

Speichern Sie die Datei und schließen Sie den Texteditor.

4. Starten Sie die Collector-VM neu, wie im folgenden Beispiel gezeigt.

```
sudo reboot
```

Verwenden des Netzwerkdaterfassungsmoduls Agentless Collector

Das Modul Network Data Collection ermöglicht es Ihnen, Abhängigkeiten zwischen Servern in Ihrem lokalen Rechenzentrum zu ermitteln. Diese Netzwerkdaten beschleunigen Ihre Migrationsplanung, indem sie einen Überblick darüber bieten, wie Anwendungen zwischen Servern kommunizieren.

Das Network Data Collection-Modul stellt eine Verbindung zu den Servern her, die das VMware vCenter-Modul identifiziert, und analysiert den IP/port Quell-IP-Ziel-Verkehr für diese Server.

Themen

- [Einrichtung des Moduls zur Erfassung von Netzwerkdaten](#)

- [Versuche, Netzwerkdaten zu sammeln](#)
- [Serverstatus im Modul Netzwerkdaterfassung](#)

Einrichtung des Moduls zur Erfassung von Netzwerkdaten

Das Modul Network Data Collection sammelt Netzwerkdaten für das Serverinventar, das vom VMware vCenter-Modul stammt. Um das Network Data Collection-Modul zu verwenden, müssen Sie daher zunächst das VMware vCenter-Modul einrichten. Folgen Sie den Anleitungen in den folgenden Themen, um Anweisungen zu erhalten:

1. [the section called "Bereitstellen eines Collectors"](#)
2. [the section called "Zugriff auf die Collector-Konsole"](#)
3. [the section called "Den Collector konfigurieren"](#)
4. [the section called "Verwenden des VMware Datenerfassungsmoduls"](#)

So richten Sie das Modul Netzwerkdaterfassung ein

1. Wählen Sie im Agentless Collector-Dashboard im Bereich Netzwerkdaterfassung die Option Netzwerkverbindungen anzeigen aus.
2. Wählen Sie auf der Seite Netzwerkverbindungen die Option Collector bearbeiten aus.
3. Geben Sie im Abschnitt Anmeldeinformationen mindestens einen Satz von Anmeldeinformationen ein. Sie können bis zu 10 Sätze von Anmeldeinformationen eingeben. Wenn das Modul zum ersten Mal versucht, Daten für einen Server zu sammeln, versucht es alle Anmeldeinformationen, bis es einen Satz von Anmeldeinformationen findet, der funktioniert. Dann speichert es diesen Satz und verwendet ihn bei nachfolgenden Versuchen erneut. Hinweise zum Einrichten von Anmeldeinformationen finden Sie unter [the section called "Anmeldeinformationen einrichten"](#).
4. Wählen Sie im Abschnitt Einstellungen für die Datenerfassung die Option Datenerfassung automatisch starten aus, um bei einem Serverneustart automatisch mit der Datenerfassung zu beginnen.
5. Wenn Sie keine WinRM-Zertifikate eingerichtet haben, wählen Sie WinRM-Zertifikatsprüfungen deaktivieren aus.
6. Wählen Sie Speichern.

7. Die Erfassung erfolgt alle 15 Sekunden auf den Servern. Um die Details der Sammelversuche für einen bestimmten Server anzuzeigen, aktivieren Sie das Kontrollkästchen links neben dem Server in der Tabelle Server.

Anmeldeinformationen einrichten

Das Modul Network Data Collection verwendet WinRM, um Daten von Windows-Servern zu sammeln. Es verwendet SNMPv2 und SNMPv3 sammelt Daten von Linux-Servern.

WinRM-Anmeldeinformationen:

- Geben Sie den Benutzernamen und das Passwort eines Windows-Kontos an, das Folgendes hat:
 - Lesezugriff auf den `\root\standardcimv2` Namespace
 - Leseberechtigungen für die Klasse `MSFT_NetTCPConnection`
 - WMI-Fernzugriff
- Wir empfehlen Ihnen, ein spezielles Dienstkonto mit den erforderlichen Mindestberechtigungen zu erstellen.
- Vermeiden Sie die Verwendung von Domänenadministrator- oder lokalen Administratorkonten.
- Port 5986 (HTTPS) muss zwischen Collector- und Zielservers geöffnet sein.
- Vermeiden Sie es, die WinRM-Zertifikatsprüfung zu deaktivieren. Hinweise zum Einrichten von WinRM-Zertifikaten finden Sie unter [the section called “Behebung von Problemen mit selbstsignierten Zertifizierungen bei der Konfiguration von WinRM-Zertifikaten”](#).

SNMPv2 Anmeldeinformationen:

- Geben Sie eine schreibgeschützte Community-Zeichenfolge an, die auf 1.3.6.1.2.1.6.13.* OID zugreifen kann
- SNMPv3 ist SNMPv2 vorzuziehen wegen der verbesserten Sicherheit in SNMPv3
- Port 161/UDP muss zwischen Collector- und Zielservers geöffnet sein
- Verwenden Sie komplexe, nicht standardmäßige Community-Zeichenketten
- Vermeiden Sie häufig verwendete Zeichenketten wie „öffentlich“ oder „privat“
- Behandeln Sie Community-Zeichenketten wie Passwörter

SNMPv3 Anmeldedaten

- Geben Sie eine username/password und auth/privacy -Details mit Lesezugriff an, die auf die OID 1.3.6.1.2.1.6.13.* zugreifen können.
- Port 161/UDP muss zwischen Collector- und Zielservern geöffnet sein
- Aktivieren Sie sowohl Authentifizierung als auch Datenschutz
- Verwenden Sie starke Authentifizierungsprotokolle (SHA wird bevorzugt MD5)
- Verwenden Sie starke Verschlüsselungsprotokolle (AES wird dem vorgezogen)
- Verwenden Sie komplexe Passwörter sowohl für die Authentifizierung als auch für den Datenschutz
- Verwenden Sie eindeutige Benutzernamen (vermeiden Sie gebräuchliche Namen)

Allgemeine bewährte Methoden für die Verwaltung von Anmeldeinformationen

- Speichern Sie Anmeldeinformationen sicher
- Wechseln Sie regelmäßig alle Anmeldeinformationen
- Verwenden Sie Passwort-Manager oder sichere Tresore
- Überwachen Sie die Verwendung von Anmeldeinformationen
- Folgen Sie dem Prinzip der geringsten Rechte und gewähren Sie nur die erforderlichen Mindestberechtigungen

Versuche, Netzwerkdaten zu sammeln

Wenn ein neuer Server erkannt wird, versucht der Collector, alle konfigurierten Anmeldeinformationen für jede IP-Adresse zu verwenden. Nachdem der Collector gültige Anmeldeinformationen gefunden hat, verwendet er nur diese Anmeldeinformationen. Nach zwei aufeinanderfolgenden Fehlern versucht der Collector nach 30 Minuten, 2 Stunden, 8 Stunden und dann 24 Stunden, Netzwerkdaten für einen Server zu sammeln. Nach sechs fehlgeschlagenen Versuchen versucht der Collector weiterhin einmal täglich, alle konfigurierten Anmeldeinformationen zu überprüfen. Um das Problem zu beheben, bearbeiten Sie entweder die aktuellen Anmeldeinformationen oder fügen Sie zusätzliche hinzu, indem Sie Collector bearbeiten wählen, oder nehmen Sie Änderungen am überwachten Zielserver vor.

Serverstatus im Modul Netzwerkdatenerfassung

In der folgenden Tabelle werden die Werte für den Erfassungsstatus erläutert.

Status	Bedeutung
Wird gesammelt oder gesammelt	Der letzte Versuch, Netzwerkverbindungen zu sammeln, war erfolgreich.
Fehler oder Fehler	Der letzte Versuch, Netzwerkverbindungen zu sammeln, schlug aufgrund eines Netzwerk- oder Berechtigungsproblems fehl. Weitere Informationen erhalten Sie, wenn Sie das Kontrollkästchen links neben dem Server aktivieren, auf dem der Fehler aufgetreten ist.
Übersprungen	Server, für die keine gültigen Anmeldeinformationen angegeben wurden. Aktualisieren oder konfigurieren Sie zusätzliche Serveranmeldeinformationen.
Keine Daten	Die Datenerfassung für den Server wurde nicht gestartet. Um mit der Datenerfassung zu beginnen, wählen Sie Sammler starten.
Ausstehend	Die Erfassung wurde gestartet, aber es wurden keine Sammlungsversuche unternommen. Warten Sie ein paar Minuten und aktualisieren Sie dann die Liste.

Verwenden des VMware vCenter Agentless Collector-Datenerfassungsmoduls

In diesem Abschnitt wird das VMware vCenter-Datenerfassungsmodul Application Discovery Service Agentless Collector (Agentless Collector) beschrieben, mit dem Serverinventar-, Profil- und Nutzungsdaten von Ihrem erfasst werden. VMware VMs

Topics

- [Einrichten des Agentless Collector-Datenerfassungsmoduls für vCenter VMware](#)
- [Details VMware zur Datenerfassung anzeigen](#)

- [Steuerung des Umfangs der vCenter-Datenerfassung](#)
- [Vom VMware vCenter-Datenerfassungsmodul Agentless Collector gesammelte Daten](#)

Einrichten des Agentless Collector-Datenerfassungsmoduls für vCenter VMware

In diesem Abschnitt wird beschrieben, wie Sie das VMware vCenter-Datenerfassungsmodul Agentless Collector einrichten, um Serverinventar-, Profil- und Nutzungsdaten von Ihrem zu sammeln. VMware VMs

Note

Bevor Sie mit dem vCenter-Setup beginnen, stellen Sie sicher, dass Sie vCenter-Anmeldeinformationen mit den für die Systemgruppe festgelegten Lese- und Anzeigeberechtigungen angeben können.

So richten Sie das VMware vCenter-Datenerfassungsmodul ein

1. Wählen Sie auf der Agentless Collector-Dashboard-Seite unter Datenerfassung im Abschnitt VMware vCenter die Option Einrichten aus.
2. Gehen Sie auf der Seite VMware vCenter-Datenerfassung einrichten wie folgt vor:
 - a. Unter den vCenter-Anmeldeinformationen:
 - i. Geben Sie für vCenter URL/IP die IP-Adresse Ihres VMware vCenter Server-Hosts ein.
 - ii. Geben Sie unter vCenter-Benutzername den Namen eines lokalen Benutzers oder eines Domänenbenutzers ein, den der Collector für die Kommunikation mit vCenter verwendet. Für Domänenbenutzer: Verwenden Sie die Form Domäne\Benutzername oder Benutzername@Domäne.
 - iii. Geben Sie für vCenter Password (vCenter-Passwort) das lokale oder Domänenbenutzerpasswort ein.
 - b. Gehen Sie unter Einstellungen zur Datenerfassung wie folgt vor:
 - Um sofort nach einer erfolgreichen Einrichtung automatisch mit der Datenerfassung zu beginnen, wählen Sie Datenerfassung automatisch starten aus.
 - c. Wählen Sie Einrichten aus.

Als Nächstes wird die Seite mit den Details zur VMware Datenerfassung angezeigt, die im nächsten Thema beschrieben wird.

Details VMware zur Datenerfassung anzeigen

Auf der Seite mit den Details zur VMware Datenerfassung werden Details zu dem vCenter angezeigt, in [Einrichten des Agentless Collector-Datenerfassungsmoduls für vCenter VMware](#) dem Sie es eingerichtet haben.

Unter Entdeckte vCenter-Server wird das von Ihnen eingerichtete vCenter mit den folgenden Informationen zum vCenter aufgeführt:

- Die IP-Adresse des vCenter Servers.
- Die Anzahl der Server im vCenter.
- Der Status der Datenerfassung.
- Wie viel Zeit ist seit dem letzten Update vergangen?

Wählen Sie „vCenter Server entfernen“, um den angezeigten vCenter Server zu entfernen und zur Seite „VMware vCenter-Datenerfassung einrichten“ zurückzukehren.

Wenn Sie sich nicht dafür entschieden haben, die Datenerfassung automatisch zu starten, können Sie die Datenerfassung starten, indem Sie auf dieser Seite auf die Schaltfläche Datenerfassung starten klicken. Nach dem Start der Datenerfassung ändert sich die Startschaltfläche in Datenerfassung beenden.

Wenn in der Spalte Sammlungsstatus Erfassung angezeigt wird, wurde die Datenerfassung gestartet.

Sie sehen sich die gesammelten Daten in der AWS Migration Hub Konsole an. Wenn Sie Daten für ein VMware vCenter Server-Inventar sammeln, können Sie auf Daten zugreifen, die etwa 15 Minuten nach dem Einschalten der Datenerfassung in der Konsole angezeigt werden.

Sie können auf dieser Seite Server in Migration Hub anzeigen auswählen, um die Migration Hub Hub-Konsole zu öffnen, sofern Ihr Internetzugang nicht blockiert ist. Unabhängig davon, ob Sie diese Schaltfläche wählen oder nicht, finden Sie Informationen zum Zugriff auf die Migration Hub Hub-Konsole unter [Ihre gesammelten Daten anzeigen](#).

Im Folgenden finden Sie die Richtlinien für die empfohlene Dauer der Datenerfassung gemäß den Aktivitäten zur Migrationsplanung:

- Gesamtbetriebskosten (TCO): 2 bis 4 Wochen

- Migrationsplanung — 2 bis 6 Wochen

Steuerung des Umfangs der vCenter-Datenerfassung

Der vCenter-Benutzer benötigt für jeden ESX-Host oder jede virtuelle Maschine nur Leseberechtigungen für die Inventarisierung mithilfe des Application Discovery Service. Mithilfe der Berechtigungseinstellungen können Sie steuern, welche Hosts und welche in der VMs Datenerfassung enthalten sind. Sie können entweder zulassen, dass alle Hosts und die VMs unter dem aktuellen vCenter befindlichen Hosts inventarisiert werden, oder Berechtigungen auf Basis erteilen. case-by-case

Note

Aus Sicherheitsgründen empfehlen wir, dem vCenter-Benutzer des Application Discovery Service keine zusätzlichen, nicht benötigten Berechtigungen zu gewähren.

In den folgenden Verfahren werden Konfigurationsszenarien in aufsteigender Reihenfolge von der geringsten zur höchsten Feinabstimmung beschrieben. Diese Verfahren gelten für vSphere Client v6.7.0.2. Die Verfahren für andere Versionen des Clients können unterschiedlich sein, je nachdem, welche Version des vSphere-Clients Sie verwenden.

Um Daten über alle ESX-Hosts und VMs unter dem aktuellen vCenter zu ermitteln

1. Wählen Sie in Ihrem VMware vSphere-Client vCenter und dann entweder Hosts and Clusters oder VMs Templates aus.
2. Wählen Sie eine Rechenzentrumsressource und dann Berechtigungen aus.
3. Wählen Sie den vCenter-Benutzer und dann das Symbol aus, um eine Benutzerrolle hinzuzufügen, zu bearbeiten oder zu entfernen.
4. Wählen Sie im Menü Rolle die Option Schreibgeschützt aus.
5. Wählen Sie „An Kinder weitergeben“ und anschließend „OK“.

Entdecken von Informationen über einen bestimmten ESX-Host und alle seine untergeordneten Objekte

1. Wählen Sie in Ihrem VMware vSphere-Client vCenter und dann entweder Hosts and Clusters oder VMs Templates aus.

2. Wählen Sie nacheinander Related Objects und Hosts aus.
3. Öffnen Sie das Kontextmenü (rechte Maustaste) für den Host-Namen und wählen Sie nacheinander All vCenter Actions und Add Permission aus.
4. Fügen Sie den Benutzer von vCenter unter Add Permission dem Host hinzu. Wählen Sie für Assigned Role die Option Read-only aus.
5. Wählen Sie Propagate to children und dann OK aus.

Um Daten zu einem bestimmten ESX-Host oder einer untergeordneten VM zu ermitteln

1. Wählen Sie in Ihrem VMware vSphere-Client vCenter und dann entweder Hosts and Clusters oder VMs Templates aus.
2. Wählen Sie Related Objects aus.
3. Wählen Sie Hosts (zeigt eine Liste der ESX-Hosts an, die vCenter bekannt sind) oder Virtuelle Maschinen (zeigt eine Liste aller VMs ESX-Hosts an).
4. Öffnen Sie das Kontextmenü (rechte Maustaste) für den Host- oder VM-Namen und wählen Sie nacheinander All vCenter Actions und Add Permission aus.
5. Fügen Sie den Benutzer von vCenter unter Add Permission dem Host oder der VM hinzu. Wählen Sie für Assigned Role die Option Read-only aus.
6. Wählen Sie OK aus.

Note

Wenn Sie „An Kinder weitergeben“ ausgewählt haben, können Sie ESX-Hosts weiterhin die Nur-Lese-Berechtigung entziehen, und zwar auf einer bestimmten Basis. VMs case-by-case. Diese Option hat keine Auswirkung auf vererbte Berechtigungen, die für andere ESX-Hosts gelten und. VMs

Vom VMware vCenter-Datenerfassungsmodul Agentless Collector gesammelte Daten

Die folgenden Informationen beschreiben die Daten, die vom VMware vCenter-Datenerfassungsmodul Application Discovery Service Agentless Collector (Agentless Collector)

gesammelt werden. Informationen zum Einrichten der Datenerfassung finden Sie unter. [Einrichten des Agentless Collector-Datenerfassungsmoduls für vCenter VMware](#)

Tabellenlegende für die gesammelten Daten von Agentless Collector VMware vCenter:

- Gesammelte Daten sind Messungen in Kilobyte (KB), sofern nicht anders angegeben.
- Entsprechende Daten in der Migration Hub Hub-Konsole werden in Megabyte (MB) gemeldet.
- Datenfelder, die mit einem Sternchen (*) gekennzeichnet sind, sind nur in den CSV-Dateien verfügbar, die mit der API-Exportfunktion des Application Discovery Service erstellt wurden.

Der Agentless Collector unterstützt den Datenexport über die AWS CLI. Um gesammelte Daten mit der AWS CLI zu exportieren, folgen Sie den Anweisungen, die unter Exportieren von Systemleistungsdaten für alle Server auf der Seite [Gesammelte Daten exportieren](#) im Application Discovery Service Service-Benutzerhandbuch beschrieben sind.

- Der Abrufzeitraum ist in Intervallen von ca. 60 Minuten.
- Datenfelder mit einem doppelten Sternchen (**) geben derzeit den Wert Null zurück.

Datenfeld	Description
applicationConfigurationId*	ID der Migrationsanwendung, unter der die VM gruppiert ist.
avgCpuUsagePct	Durchschnittlicher Prozentsatz der CPU-Auslastung während des Abfragezeitraums.
avgDiskBytesReadPerSecond	Durchschnittliche Anzahl von Byte, die während des Abfragezeitraums von der Festplatte gelesen wurden.
avgDiskBytesWrittenPerSecond	Durchschnittliche Anzahl von Byte, die während des Abfragezeitraums auf die Festplatte geschrieben wurden.
avgDiskReadOpsPerSecond**	Durchschnittliche Anzahl von I/O Lesevorgängen pro Sekunde Null.

Datenfeld	Description
avgDiskWriteOpsPerSecond**	Durchschnittliche Anzahl von I/O Schreibvorgängen pro Sekunde.
avgFreeRAM	Durchschnittlicher freier Arbeitsspeicher, ausgedrückt in MB.
avgNetworkBytesReadPerSecond	Durchschnittlicher Durchsatz der pro Sekunde gelesenen Byte.
avgNetworkBytesWrittenPerSecond	Durchschnittlicher Durchsatz an geschriebenen Byte pro Sekunde.
Computer-Hersteller	Vom ESXi Host gemeldeter Anbieter.
Computermodell	Vom ESXi Host gemeldetes Computermodell.
configId	ID, die der erkannten VM vom Application Discovery Service zugewiesen wurde.
configType	Art der erkannten Ressource.
connectorId	ID der virtuellen Appliance.
cpuType	vCPU für eine VM, aktuelles Modell für einen Host.
datacenterId	ID des vCenter.
hostId*	ID des VM-Hosts.
hostName	Name des Hosts, auf dem die Virtualisierungssoftware ausgeführt wird.
hypervisor	Typ des Hypervisors.
id	ID des Servers.
lastModifiedTimeStempel*	Spätestes Datum und Uhrzeit der Datenerfassung vor dem Datenexport.

Datenfeld	Description
macAddress	MAC-Adresse der VM.
manufacturer	Hersteller der Virtualisierungssoftware.
maxCpuUsagePct	Maximaler Prozentsatz der CPU-Auslastung während des Abfragezeitraums.
maxDiskBytesReadPerSecond	Max. Anzahl der während des Abfragezeitraums von der Festplatte gelesenen Byte.
maxDiskBytesWrittenPerSecond	Max. Anzahl von Byte, die während des Abfragezeitraums auf die Festplatte geschrieben wurden.
maxDiskReadOpsPerSecond ^{**}	Max. Anzahl von I/O Lesevorgängen pro Sekunde.
maxDiskWriteOpsPerSecond ^{**}	Max. Anzahl von I/O Schreibvorgängen pro Sekunde.
maxNetworkBytesReadPerSecond	Max. Durchsatzmenge der pro Sekunde gelesenen Byte.
maxNetworkBytesWrittenPerSecond	Max. Durchsatzmenge der pro Sekunde geschriebenen Byte.
memoryReservation [*]	Grenzwert, um eine Überbelegung des Arbeitsspeichers auf der VM zu vermeiden.
moRefId	Eindeutige Referenz-ID für verwaltete vCenter-Objekte.
name [*]	Name der VM oder des Netzwerks (vom Benutzer angegeben).
numCores	Anzahl der CPU-Kerne, die der VM zugewiesen sind.

Datenfeld	Description
numCpus	Anzahl der CPU-Sockel auf dem ESXi Host.
numDisks ^{**}	Anzahl der Festplatten auf der VM.
numNetworkCards ^{**}	Anzahl der Netzwerkkarten auf der VM.
osName	Name des Betriebssystems auf der VM.
osVersion	Betriebssystemversion auf der VM.
portGroupId [*]	ID der Gruppe von Mitgliedsports des VLAN.
portGroupName [*]	Name der Gruppe von Mitgliedsports des VLAN.
powerState [*]	Status der Stromversorgung.
serverId	Der Application Discovery Service hat der erkannten VM eine ID zugewiesen.
smBiosId [*]	ID/Version des Systemmanagement-BIOS.
state [*]	Status der virtuellen Appliance.
toolsStatus	Betriebszustand der VMware Tools
totalDiskFreeGröße	Freier Festplattenspeicher, ausgedrückt in MB. Verfügbar für vCenter Server 7.0 und spätere Versionen.
totalDiskSize	Gesamtkapazität der Festplatte, ausgedrückt in MB.
totalRAM	Gesamtmenge des auf der virtuellen Maschine verfügbaren Arbeitsspeichers in MB.
type	Art des Hosts.
vCenterId	Eindeutige ID-Nummer einer VM.

Datenfeld	Description
vCenterName *	Name des vCenter-Hosts.
virtualSwitchName *	Name des virtuellen Switches.
vmFolderPath	Verzeichnispfad der VM-Dateien.
vmName	Name der virtuellen Maschine.

Verwenden des Datenbank- und Analysedatenerfassungsmoduls

In diesem Abschnitt wird beschrieben, wie Sie ein Modul zur Erfassung von Datenbank- und Analysedaten einrichten, konfigurieren und verwenden. Sie können dieses Datenerfassungsmodul verwenden, um eine Verbindung zu Ihrer Datenumgebung herzustellen und Metadaten und Leistungskennzahlen von Ihren lokalen Datenbanken und Analyseservern zu sammeln. Informationen zu den Messwerten, die Sie mit diesem Modul sammeln können, finden Sie unter [Vom Agentless Collector-Datenbank- und Analysedatenerfassungsmodul gesammelte Daten](#).

Important

Hinweis zum Ende des Supports: Am 20. Mai 2026 AWS wird der Support für AWS Database Migration Service Fleet Advisor eingestellt. Nach dem 20. Mai 2026 können Sie nicht mehr auf die AWS DMS Fleet Advisor-Konsole oder AWS DMS die Fleet Advisor-Ressourcen zugreifen. Weitere Informationen finden Sie unter [Ende des Supports für AWS DMS Fleet Advisor](#).

Wenn Sie das Modul zur Erfassung von Datenbank- und Analysedaten verwenden, müssen Sie generell die folgenden Schritte ausführen.

1. Führen Sie die erforderlichen Schritte aus, konfigurieren Sie Ihren IAM-Benutzer und erstellen Sie den AWS DMS Datensammelpunkt.
2. Konfigurieren Sie die Datenweiterleitung, um sicherzustellen, dass Ihr Datenerfassungsmodul die gesammelten Metadaten und Leistungskennzahlen an diese AWS senden kann.

3. Fügen Sie Ihre LDAP-Server hinzu und verwenden Sie sie, um Betriebssystemserver in Ihrer Datenumgebung zu ermitteln. Fügen Sie Ihre Betriebssystemserver alternativ manuell hinzu oder verwenden Sie den [Verwenden des VMware Datenerfassungsmoduls](#).
4. Konfigurieren Sie die Verbindungsanmeldeinformationen zu Ihren Betriebssystemservern und verwenden Sie sie dann, um Datenbankserver zu erkennen.
5. Konfigurieren Sie die Verbindungsanmeldeinformationen für Ihre Datenbank- und Analyseserver und führen Sie dann die Datenerfassung aus. Weitere Informationen finden Sie unter [Erfassung von Datenbank- und Analysedaten](#).
6. Zeigen Sie die gesammelten Daten in der AWS DMS Konsole an und verwenden Sie sie, um Zielempfehlungen für eine Migration zum zu generieren AWS Cloud. Weitere Informationen finden Sie unter [Erfassung von Datenbank- und Analysedaten](#).

Topics

- [Unterstützte Betriebssystem-, Datenbank- und Analyseserver](#)
- [Den AWS DMS Datensammelpunkt erstellen](#)
- [Konfiguration der Datenweiterleitung](#)
- [Fügen Sie Ihre LDAP- und OS-Server hinzu](#)
- [Ermitteln Sie Ihre Datenbankserver](#)
- [Vom Agentless Collector-Datenbank- und Analysedatenerfassungsmodul gesammelte Daten](#)

Unterstützte Betriebssystem-, Datenbank- und Analyseserver

Das Modul zur Erfassung von Datenbank- und Analysedaten im Agentless Collector unterstützt Microsoft Active Directory-LDAP-Server.

Dieses Datenerfassungsmodul unterstützt die folgenden Betriebssystemserver.

- Amazon Linux 2
- CentOS Linux Version 6 und höher
- Debian Version 10 und höher
- Red Hat Enterprise Linux Version 7 und höher
- SUSE Linux Enterprise Server Version 12 und höher
- Ubuntu Version 16.01 und höher
- Windows Server 2012 und höher

- Windows XP und höher

Das Modul zur Erfassung von Datenbank- und Analysedaten unterstützt außerdem die folgenden Datenbankserver.

- Microsoft SQL Server Version 2012 und bis 2019
- MySQL Version 5.6 und bis 8
- Oracle Version 11g, Release 2 und bis 12c, 19c und 21c
- PostgreSQL Version 9.6 und bis 13

Den AWS DMS Datensammelpunkt erstellen

Ihr Modul zur Erfassung von Datenbank- und Analysedaten verwendet einen AWS DMS Datensammelpunkt, um mit der AWS DMS Konsole zu interagieren. Sie können die gesammelten Daten in der AWS DMS Konsole anzeigen oder sie verwenden, um die richtige Größe der AWS Ziel-Engine zu ermitteln. Weitere Informationen finden Sie unter [Verwenden der AWS DMS Fleet Advisor-Funktion für Zielempfehlungen](#).

Bevor Sie einen AWS DMS Datensammler erstellen, erstellen Sie eine IAM-Rolle, die Ihr AWS DMS Datensammelpunkt für den Zugriff auf Ihren Amazon S3 S3-Bucket verwendet. Sie haben diesen Amazon S3 S3-Bucket erstellt, als Sie die Voraussetzungen in erfüllt haben [Voraussetzungen für Agentless Collector](#).

Um eine IAM-Rolle für Ihren AWS DMS Datensammler für den Zugriff auf Amazon S3 zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter. <https://console.aws.amazon.com/iam/>
2. Wählen Sie im Navigationsbereich Rollen und anschließend Rolle erstellen aus.
3. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen unter Typ der vertrauenswürdigen Entität die Option AWS -Service aus. Wählen Sie für Anwendungsfälle für andere AWS Dienste DMS aus.
4. Markieren Sie das Kontrollkästchen DMS und wählen Sie Weiter.
5. Wählen Sie auf der Seite „Berechtigungen hinzufügen“ die Option FleetAdvisorS3Policy aus, die Sie zuvor erstellt haben. Wählen Sie Weiter aus.
6. Geben Sie auf der Seite Benennen, Prüfen und Erstellen **FleetAdvisorS3Role** für Rollename ein und wählen Sie dann Rolle erstellen.

7. Öffnen Sie die Rolle, die Sie erstellt haben, und wählen Sie die Registerkarte Vertrauensbeziehungen aus. Wählen Sie Vertrauensrichtlinie bearbeiten aus.
8. Fügen Sie auf der Seite Vertrauensrichtlinie bearbeiten den folgenden JSON-Code in den Editor ein und ersetzen Sie damit den vorhandenen Code.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "dms.amazonaws.com",
        "dms-fleet-advisor.amazonaws.com"
      ]
    },
    "Action": "sts:AssumeRole"
  }]
}
```

9. Wählen Sie Richtlinie aktualisieren.

Erstellen Sie jetzt einen Datensammelpunkt in der AWS DMS Konsole.

Um einen AWS DMS Datensammler zu erstellen

1. Melden Sie sich bei <https://console.aws.amazon.com/dms/v2/> an AWS-Managementkonsole und öffnen Sie die AWS DMS Konsole.
2. Wählen Sie AWS-Region die Region aus, die Sie als Ihre Migration Hub Hub-Heimatregion festgelegt haben. Weitere Informationen finden Sie unter [Melden Sie sich bei Migration Hub an und wählen Sie eine Heimatregion](#).
3. Wählen Sie im Navigationsbereich Datensammler unter Entdecken aus. Die Seite Datenkollektoren wird geöffnet.
4. Wählen Sie Datenkollektor erstellen aus. Die Seite Datenkollektor erstellen wird geöffnet.
5. Geben Sie im Abschnitt Allgemeine Konfiguration unter Name den Namen Ihres Datenkollektors ein.

6. Wählen Sie im Abschnitt Konnektivität die Option S3 durchsuchen aus. Wählen Sie den Amazon S3 S3-Bucket, den Sie zuvor erstellt haben, aus der Liste aus.
7. Wählen Sie für die IAM-Rolle die Rolle aus, `FleetAdvisorS3Role` die Sie zuvor erstellt haben.
8. Wählen Sie Datenkollektor erstellen aus.

Konfiguration der Datenweiterleitung

Nachdem Sie die erforderlichen AWS Ressourcen erstellt haben, konfigurieren Sie die Datenweiterleitung vom Modul zur Erfassung von Datenbank- und Analysedaten an Ihren AWS DMS Collector.

Um die Datenweiterleitung zu konfigurieren

1. Öffnen Sie die Agentless Collector-Konsole. Weitere Informationen finden Sie unter [Zugriff auf die Collector-Konsole](#).
2. Wählen Sie Datenbank und Analytics-Kollektor anzeigen aus.
3. Wählen Sie auf der Dashboard-Seite im Abschnitt Datenweiterleitung die Option Datenweiterleitung konfigurieren aus.
4. Für die AWS-Region IAM-Zugriffsschlüssel-ID und den geheimen IAM-Zugriffsschlüssel verwendet Ihr Agentless Collector die Werte, die Sie zuvor konfiguriert haben. Weitere Informationen erhalten Sie unter [Melden Sie sich bei Migration Hub an und wählen Sie eine Heimatregion](#) und [Bereitstellen eines Collectors](#).
5. Wählen Sie unter Connected DMS data Collector Ihren Datensammelpunkt aus, den Sie in der Konsole erstellt haben. AWS DMS
6. Wählen Sie Speichern.

Nachdem Sie die Datenweiterleitung konfiguriert haben, überprüfen Sie den Abschnitt Datenweiterleitung auf der Dashboard-Seite. Vergewissern Sie sich, dass in Ihrem Modul zur Erfassung von Datenbank- und Analysedaten Connected for Access to DMS und Access to S3 angezeigt wird.

Fügen Sie Ihre LDAP- und OS-Server hinzu

Das Modul zur Erfassung von Datenbank- und Analysedaten verwendet LDAP in Microsoft Active Directory, um Informationen über das Betriebssystem, die Datenbank und die Analyseserver in

Ihrem Netzwerk zu sammeln. Das Lightweight Directory Access Protocol (LDAP) ist ein offenes Standardanwendungsprotokoll. Sie können dieses Protokoll verwenden, um über Ihr IP-Netzwerk auf verteilte Verzeichnisdienstleistungen zuzugreifen und diese zu verwalten.

Sie können Ihrem Datenbank- und Analysedatenerfassungsmodul einen vorhandenen LDAP-Server hinzufügen, um Betriebssystemserver in Ihrem Netzwerk automatisch zu erkennen. Wenn Sie LDAP nicht verwenden, können Sie Betriebssystemserver manuell hinzufügen.

Um Ihrem Modul zur Erfassung von Datenbank- und Analysedaten einen LDAP-Server hinzuzufügen

1. Öffnen Sie die Agentless Collector-Konsole. Weitere Informationen finden Sie unter [Zugriff auf die Collector-Konsole](#).
2. Wählen Sie View Database and Analytics Collector und anschließend im Navigationsbereich unter Discovery die Option LDAP-Server aus.
3. Wählen Sie LDAP-Server hinzufügen. Die Seite LDAP-Server hinzufügen wird geöffnet.
4. Geben Sie als Hostname den Hostnamen Ihres LDAP-Servers ein.
5. Geben Sie für Port die Portnummer ein, die für LDAP-Anfragen verwendet wird.
6. Geben Sie unter Benutzername den Benutzernamen ein, den Sie für die Verbindung mit Ihrem LDAP-Server verwenden.
7. Geben Sie unter Passwort das Passwort ein, mit dem Sie eine Verbindung zu Ihrem LDAP-Server herstellen.
8. (Optional) Wählen Sie Verbindung überprüfen, um sicherzustellen, dass Sie Ihre LDAP-Serveranmeldeinformationen korrekt hinzugefügt haben. Alternativ können Sie Ihre Anmeldeinformationen für die LDAP-Serververbindung später anhand der Liste auf der LDAP-Serverseite überprüfen.
9. Wählen Sie LDAP-Server hinzufügen.
10. Wählen Sie auf der Seite LDAP-Server Ihren LDAP-Server aus der Liste aus und wählen Sie Discover OS servers aus.

 Important

Für die Betriebssystemerkennung benötigt das Datenerfassungsmodul Anmeldeinformationen für den Domänenserver, um Anfragen mithilfe des LDAP-Protokolls ausführen zu können.

Das Modul zur Erfassung von Datenbank- und Analysedaten stellt eine Verbindung zu Ihrem LDAP-Server her und erkennt Ihre Betriebssystemserver. Nachdem das Datenerfassungsmodul die Erkennung der OS-Server abgeschlossen hat, können Sie die Liste der erkannten OS-Server anzeigen, indem Sie OS-Server anzeigen wählen.

Alternativ können Sie Ihre Betriebssystemserver manuell hinzufügen oder die Serverliste aus einer Datei mit kommagetrennten Werten (CSV) importieren. Sie können auch das VMware vCenter Agentless Collector-Datenerfassungsmodul verwenden, um Ihre Betriebssystemserver zu ermitteln. Weitere Informationen finden Sie unter [Verwenden des VMware Datenerfassungsmoduls](#).

So fügen Sie Ihrem Datenbank- und Analysedatenerfassungsmodul einen Betriebssystemserver hinzu

1. Wählen Sie auf der Collector-Seite für Datenbanken und Analysen im Navigationsbereich unter Discovery die Option OS-Server aus.
2. Wählen Sie OS-Server hinzufügen aus. Die Seite „OS-Server hinzufügen“ wird geöffnet.
3. Geben Sie Ihre Anmeldeinformationen für den OS-Server ein.
 - a. Wählen Sie als Betriebssystemtyp das Betriebssystem Ihres Servers aus.
 - b. Geben Sie für Hostname/IP den Hostnamen oder die IP-Adresse Ihres OS-Servers ein.
 - c. Geben Sie für Port die Portnummer ein, die für Remote-Abfragen verwendet wird.
 - d. Wählen Sie unter Authentifizierungstyp den Authentifizierungstyp aus, den Ihr Betriebssystemserver verwendet.
 - e. Geben Sie unter Benutzername den Benutzernamen ein, den Sie für die Verbindung mit Ihrem OS-Server verwenden.
 - f. Geben Sie unter Passwort das Passwort ein, mit dem Sie eine Verbindung zu Ihrem OS-Server herstellen.
 - g. Wählen Sie Überprüfen, um sicherzustellen, dass Sie Ihre Betriebssystemserver-Anmeldeinformationen korrekt hinzugefügt haben.
4. (Optional) Fügen Sie mehrere Betriebssystemserver aus einer CSV-Datei hinzu.
 - a. Wählen Sie OS-Server in großen Mengen aus CSV importieren.
 - b. Wählen Sie Vorlage herunterladen, um eine CSV-Datei zu speichern, die eine Vorlage enthält, die Sie anpassen können.

- c. Geben Sie die Verbindungsanmeldedaten für Ihre Betriebssystemserver entsprechend der Vorlage in die Datei ein. Das folgende Beispiel zeigt, wie Sie die Anmeldeinformationen für die Verbindung zum OS-Server in einer CSV-Datei angeben können.

```
OS type,Hostname/IP,Port,Authentication type,Username>Password
Linux,192.0.2.0,22,Key-based authentication,USER-EXAMPLE,ANPAJ2UCCR6DPCEXAMPLE
Windows,203.0.113.0,,NTLM,USER2-EXAMPLE,AKIAIOSFODNN7EXAMPLE
```

Speichern Sie Ihre CSV-Datei, nachdem Sie Anmeldeinformationen für alle Ihre Betriebssystemserver hinzugefügt haben.

- d. Wählen Sie Durchsuchen und dann Ihre CSV-Datei aus.
5. Wählen Sie „OS-Server hinzufügen“.
 6. Nachdem Sie Anmeldeinformationen für alle Betriebssystemserver hinzugefügt haben, wählen Sie Ihre Betriebssystemserver aus und klicken Sie auf Datenbankserver ermitteln.

Ermitteln Sie Ihre Datenbankserver

Dieser Abschnitt führt Sie durch die Schritte, die Sie zur Konfiguration Ihres Betriebssystems und Ihrer Datenbankserver ausführen müssen. Anschließend ermitteln Sie Ihre Server und haben die Möglichkeit, manuell einen Datenbank- oder Analyseserver hinzuzufügen.

Für die Datenbankerkennung müssen Sie Benutzer für Ihre Quelldatenbanken mit den für das Datenerfassungsmodul erforderlichen Mindestberechtigungen erstellen. Weitere Informationen finden Sie im Benutzerhandbuch unter [Datenbankbenutzer für AWS DMS Fleet Advisor erstellen](#).AWS DMS

Konfiguration, Einrichtung

Um die Datenbanken zu ermitteln, die auf den zuvor hinzugefügten OS-Servern laufen, benötigt das Datenerfassungsmodul Zugriff auf das Betriebssystem und die Datenbankserver. Auf dieser Seite werden die Schritte beschrieben, die Sie ergreifen müssen, um sicherzustellen, dass auf Ihre Datenbank über den Port zugegriffen werden kann, den Sie in den Verbindungseinstellungen angegeben haben. Außerdem aktivieren Sie die Remoteauthentifizierung auf Ihrem Datenbankserver und erteilen Ihrem Datenerfassungsmodul Berechtigungen.

Konfiguration unter Linux

Gehen Sie wie folgt vor, um das Setup für die Erkennung von Datenbankservern unter Linux zu konfigurieren.

So konfigurieren Sie Linux für die Erkennung von Datenbankservern

1. Gewähren Sie sudo-Zugriff auf die netstat Befehle ss und.

Das folgende Codebeispiel gewährt sudo-Zugriff auf die Befehle ss und netstat.

```
sudo bash -c "cat << EOF >> /etc/sudoers.d/username
username ALL=(ALL) NOPASSWD: /usr/bin/ss
username ALL=(ALL) NOPASSWD: /usr/bin/netstat
EOF"
```

Ersetzen Sie es im vorherigen Beispiel *username* durch den Namen des Linux-Benutzers, den Sie in den Anmeldeinformationen für die Verbindung zum Betriebssystemserver angegeben haben.

Im vorherigen Beispiel wird der /usr/bin/ Pfad zu den netstat Befehlen ss und verwendet. Dieser Pfad kann in Ihrer Umgebung anders sein. Um den Pfad zu den netstat Befehlen ss und zu ermitteln, führen Sie die which netstat Befehle which ss and aus.

2. Konfigurieren Sie Ihre Linux-Server so, dass sie die Ausführung von SSH-Skripts und den ICMP-Verkehr (Internet Control Message Protocol) zulassen.

Konfiguration unter Microsoft Windows

Gehen Sie wie folgt vor, um das Setup für die Erkennung von Datenbankservern unter Microsoft Windows zu konfigurieren.

So konfigurieren Sie Microsoft Windows für die Erkennung von Datenbankservern

1. Geben Sie Anmeldeinformationen ein, um Abfragen mit Windows Management Instrumentation (WMI) und WMI Query Language (WQL) auszuführen und die Registrierung zu lesen.
2. Fügen Sie den Windows-Benutzer, den Sie in den Anmeldeinformationen für die Verbindung mit dem Betriebssystemserver angegeben haben, den folgenden Gruppen hinzu: Distributed COM Users, Performance Log-Benutzer, Performance Monitor-Benutzer und Event Log Readers. Verwenden Sie dazu das folgende Codebeispiel.

```
net localgroup "Distributed COM Users" username /ADD
net localgroup "Performance Log Users" username /ADD
net localgroup "Performance Monitor Users" username /ADD
net localgroup "Event Log Readers" username /ADD
```

Ersetzen Sie es im vorherigen Beispiel durch den Namen des Windows-Benutzers, den Sie in den Anmeldeinformationen für die Verbindung *username* mit dem Betriebssystemserver angegeben haben.

3. Erteilen Sie dem Windows-Benutzer, den Sie in den Anmeldeinformationen für die Verbindung mit dem Betriebssystemserver angegeben haben, die erforderlichen Berechtigungen.
 - Wählen Sie unter Eigenschaften für Windows-Verwaltung und Instrumentierung die Option Lokaler Start und Remoteaktivierung aus.
 - Wählen Sie für die WMI-Steuerung die Berechtigungen Methoden ausführen, Konto aktivieren, Fernaktivierung und Lesesicherheit für die WMI Namespaces CIMV2DEFAULT,StandartCimv2, und aus.
 - Führen Sie das WMI-Plug-In aus und wählen Sie dann **winrm configsddl default** Lesen und Ausführen.
4. Konfigurieren Sie Ihren Windows-Host mithilfe des folgenden Codebeispiels.

```
netsh advfirewall firewall add rule name="Open Ports for WinRM incoming traffic"
  dir=in action=allow protocol=TCP localport=5985, 5986 # Opens ports for WinRM
netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any
  dir=in action=allow # Allows ICMP traffic

Enable-PSRemoting -Force # Enables WinRM
Set-Service WinRM -StartMode Automatic # Allows WinRM service to run on host
startup
Set-Item WSMan:\localhost\Client\TrustedHosts -Value {IP} -Force # Sets the
specific IP from which the access to WinRM is allowed

winrm set winrm/config/service '@{Negotiation="true"}' # Allow Negotiate auth usage
winrm set winrm/config/service '@{AllowUnencrypted="true"}' # Allow unencrypted
connection
```

Ermitteln Sie einen Datenbankserver

Führen Sie die folgenden Aufgaben aus, um Datenbankserver auf der Konsole zu finden und hinzuzufügen.

Um mit der Erkennung Ihrer Datenbankserver zu beginnen

1. Wählen Sie auf der Collector-Seite für Datenbanken und Analysen im Navigationsbereich unter Discovery die Option OS-Server aus.
2. Wählen Sie die Betriebssystemserver aus, zu denen Ihre Datenbank- und Analyseserver gehören, und wählen Sie dann im Menü Aktionen die Option Verbindung überprüfen aus.
3. Bearbeiten Sie bei Servern mit dem Konnektivitätsstatus Fehlgeschlagen die Verbindungsanmeldedaten.
 - a. Wählen Sie einen einzelnen Server oder mehrere Server aus, wenn sie identische Anmeldeinformationen haben, und wählen Sie dann im Menü Aktionen die Option Bearbeiten aus. Die Seite „Betriebssystemserver bearbeiten“ wird geöffnet.
 - b. Geben Sie für Port die Portnummer ein, die für Remote-Abfragen verwendet wird.
 - c. Wählen Sie unter Authentifizierungstyp den Authentifizierungstyp aus, den Ihr Betriebssystemserver verwendet.
 - d. Geben Sie unter Benutzername den Benutzernamen ein, den Sie für die Verbindung mit Ihrem OS-Server verwenden.
 - e. Geben Sie unter Passwort das Passwort ein, mit dem Sie eine Verbindung zu Ihrem OS-Server herstellen.
 - f. Wählen Sie Verbindung überprüfen, um sicherzustellen, dass Sie Ihre Betriebssystemserver-Anmeldeinformationen korrekt aktualisiert haben. Wählen Sie als Nächstes Speichern.
4. Nachdem Sie die Anmeldeinformationen für alle Betriebssystemserver aktualisiert haben, wählen Sie Ihre Betriebssystemserver aus und wählen Sie Discover database servers.

Das Modul zur Erfassung von Datenbank- und Analysedaten stellt eine Verbindung zu Ihren Betriebssystemservern her und erkennt die unterstützten Datenbank- und Analyseserver. Nachdem das Datenerfassungsmodul die Erkennung abgeschlossen hat, können Sie die Liste der erkannten Datenbank- und Analyseserver anzeigen, indem Sie Datenbankserver anzeigen wählen.

Alternativ können Sie Ihre Datenbank- und Analyseserver manuell zum Inventar hinzufügen. Sie können die Serverliste auch aus einer CSV-Datei importieren. Sie können diesen Schritt überspringen, wenn Sie bereits alle Datenbank- und Analyseserver zum Inventar hinzugefügt haben.

Um einen Datenbank- oder Analyseserver manuell hinzuzufügen

1. Wählen Sie auf der Seite Datenbank- und Analyse-Collector im Navigationsbereich die Option Datenerfassung aus.
2. Wählen Sie Datenbankserver hinzufügen aus. Die Seite Datenbankserver hinzufügen wird geöffnet.
3. Geben Sie Ihre Anmeldeinformationen für den Datenbankserver ein.
 - a. Wählen Sie für Datenbank-Engine die Datenbank-Engine Ihres Servers aus. Weitere Informationen finden Sie unter [Unterstützte Betriebssystem-, Datenbank- und Analyseserver](#).
 - b. Geben Sie für Hostname/IP den Hostnamen oder die IP-Adresse Ihres Datenbank- oder Analyseservers ein.
 - c. Geben Sie für Port den Port ein, auf dem Ihr Server läuft.
 - d. Wählen Sie unter Authentifizierungstyp den Authentifizierungstyp aus, den Ihr Datenbank- oder Analyseserver verwendet.
 - e. Geben Sie unter Benutzername den Benutzernamen ein, den Sie für die Verbindung mit Ihrem Server verwenden.
 - f. Geben Sie unter Passwort das Passwort ein, mit dem Sie eine Verbindung zu Ihrem Server herstellen.
 - g. Wählen Sie Überprüfen, um sicherzustellen, dass Sie Ihre Datenbank- oder Analytics-Server-Anmeldeinformationen korrekt hinzugefügt haben.
4. (Optional) Fügen Sie mehrere Server aus einer CSV-Datei hinzu.
 - a. Wählen Sie Datenbankserver in großen Mengen aus CSV importieren.
 - b. Wählen Sie Vorlage herunterladen, um eine CSV-Datei zu speichern, die eine Vorlage enthält, die Sie anpassen können.
 - c. Geben Sie die Verbindungsanmeldedaten für Ihre Datenbank- und Analyseserver entsprechend der Vorlage in die Datei ein. Das folgende Beispiel zeigt, wie Sie die Anmeldeinformationen für die Datenbank- oder Analyseserver-Verbindung in einer CSV-Datei angeben können.

```
Database engine,Hostname/IP,Port,Authentication type,Username,Password,Oracle  
service name,Database,Allow public key retrieval,Use SSL,Trust server  
certificate  
Oracle,192.0.2.1,1521,Login/Password authentication,USER-  
EXAMPLE,AKIAI44QH8DHBEXAMPLE,orcl,,,,
```

```
PostgreSQL,198.51.100.1,1533,Login/Password authentication,USER2-EXAMPLE,bPxRfiCYEXAMPLE,,postgre,,TRUE,
MSSQL,203.0.113.1,1433,Login/Password authentication,USER3-EXAMPLE,h3yCo8nvbEXAMPLE,,,,TRUE
MySQL,2001:db8:4006:812:ffff:200e,8080,Login/Password authentication,USER4-EXAMPLE,APKAEIVFHP46CEXAMPLE,,mysql,TRUE,TRUE,
```

Speichern Sie Ihre CSV-Datei, nachdem Sie Anmeldeinformationen für alle Ihre Datenbank- und Analyseserver hinzugefügt haben.

- d. Wählen Sie Durchsuchen und dann Ihre CSV-Datei aus.
5. Wählen Sie Datenbankserver hinzufügen.
6. Nachdem Sie Anmeldeinformationen für alle Betriebssystemserver hinzugefügt haben, wählen Sie Ihre Betriebssystemserver aus und klicken Sie auf Datenbankserver ermitteln.

Nachdem Sie alle Ihre Datenbank- und Analyseserver zum Datenerfassungsmodul hinzugefügt haben, fügen Sie sie dem Inventar hinzu. Das Modul zur Erfassung von Datenbank- und Analysedaten kann vom Inventar aus eine Verbindung zu den Servern herstellen und sammelt Metadaten und Leistungsmetriken.

Um Ihre Datenbank- und Analyseserver zum Inventar hinzuzufügen

1. Wählen Sie auf der Collector-Seite für Datenbanken und Analysen im Navigationsbereich unter Discovery die Option Datenbankserver aus.
2. Wählen Sie die Datenbank- und Analyseserver aus, für die Sie Metadaten und Leistungsmetriken sammeln möchten.
3. Wählen Sie Zum Inventar hinzufügen aus.

Nachdem Sie alle Datenbank- und Analyseserver zu Ihrem Inventar hinzugefügt haben, können Sie mit der Erfassung von Metadaten und Leistungsmetriken beginnen. Weitere Informationen finden Sie unter [Erfassung von Datenbank- und Analysedaten](#).

Vom Agentless Collector-Datenbank- und Analysedatenerfassungsmodul gesammelte Daten

Das Datenbank- und Analysedatenerfassungsmodul Application Discovery Service Agentless Collector (Agentless Collector) erfasst die folgenden Metriken aus Ihrer Datenumgebung.

Informationen zum Einrichten der Datenerfassung finden Sie unter. [Verwenden des Datenbank- und Analysedatenerfassungsmoduls](#)

Wenn Sie das Modul zur Erfassung von Datenbank- und Analysedaten verwenden, um Metadaten und Datenbankkapazität zu erfassen, werden die folgenden Messwerte erfasst.

- Verfügbarer Arbeitsspeicher auf Ihren Betriebssystemservern
- Verfügbarer Speicherplatz auf Ihren Betriebssystemservern
- Datenbankversion und Edition
- Anzahl der Server CPUs auf Ihrem Betriebssystem
- Anzahl der Schemata
- Anzahl gespeicherter Prozeduren
- Anzahl der Tabellen
- Anzahl der Auslöser
- Anzahl der Ansichten
- Schema-Struktur

Nachdem Sie die Schemaanalyse in der AWS DMS Konsole gestartet haben, analysiert Ihr Datenerfassungsmodul die folgenden Messwerte und zeigt sie an.

- Daten für die Datenbankunterstützung
- Anzahl der Codezeilen
- Schema-Komplexität
- Ähnlichkeit der Schemata

Wenn Sie das Modul zur Erfassung von Datenbank- und Analysedaten verwenden, um Metadaten, Datenbankkapazität und Ressourcenauslastung zu erfassen, erfasst es die folgenden Kennzahlen.

- E/A-Durchsatz auf Ihren Datenbankservern
- Eingabe-/Ausgabevorgänge pro Sekunde (IOPS) auf Ihren Datenbankservern
- Anzahl davon CPUs , die Ihre Betriebssystemserver verwenden
- Arbeitsspeichernutzung auf Ihren Betriebssystemservern
- Speichernutzung auf Ihren Betriebssystemservern

Sie können das Modul zur Erfassung von Datenbank- und Analysedaten verwenden, um Metadaten, Kapazität und Nutzungsmetriken aus Ihren Oracle- und SQL Server-Datenbanken zu sammeln. Gleichzeitig kann das Datenerfassungsmodul für PostgreSQL- und MySQL-Datenbanken nur Metadaten sammeln.

Ihre gesammelten Daten anzeigen

Important

Hinweis zum Ende des Supports: Am 20. Mai 2026 AWS wird der Support für AWS Database Migration Service Fleet Advisor eingestellt. Nach dem 20. Mai 2026 können Sie nicht mehr auf die AWS DMS Fleet Advisor-Konsole oder AWS DMS die Fleet Advisor-Ressourcen zugreifen. Weitere Informationen finden Sie unter [Ende des Supports für AWS DMS Fleet Advisor](#).

Sie können die Daten, die Ihr Application Discovery Service Agentless Collector (Agentless Collector) gesammelt hat, in der Migration Hub Hub-Konsole anzeigen, indem Sie die Schritte unter befolgen. [Server in der Konsole anzeigen AWS Migration Hub](#)

Sie können die gesammelten Messwerte für Datenbank- und Analyseserver auch in der AWS DMS Konsole anzeigen, indem Sie die folgenden Schritte ausführen.

So zeigen Sie die vom Modul zur Erfassung von Datenbank- und Analysedaten erkannten Daten in der AWS DMS Konsole an

1. Melden Sie sich bei <https://console.aws.amazon.com/dms/v2/> an AWS-Managementkonsole und öffnen Sie die AWS DMS Konsole.
2. Wählen Sie unter Discover die Option Inventar aus. Die Seite Inventar wird geöffnet.
3. Wählen Sie Inventare analysieren aus, um Eigenschaften des Datenbankschemas wie Ähnlichkeit und Komplexität zu ermitteln.
4. Wählen Sie die Registerkarte Schemas, um die Ergebnisse der Analyse zu sehen.

Sie können die AWS DMS Konsole verwenden, um doppelte Schemas zu identifizieren, die Komplexität der Migration zu bestimmen und die Inventarinformationen für die future Analyse zu exportieren. Weitere Informationen finden Sie unter [Verwenden von Inventaren für Analysen in AWS DMS Fleet Advisor](#).

Zugriff auf den Agentless Collector

In diesem Abschnitt wird beschrieben, wie Sie den Application Discovery Service Agentless Collector (Agentless Collector) verwenden.

Topics

- [Das Agentless Collector-Dashboard](#)
- [Bearbeiten der Agentless Collector-Einstellungen](#)
- [Bearbeiten von VMware vCenter-Anmeldeinformationen](#)

Das Agentless Collector-Dashboard

Auf der Dashboardseite Application Discovery Service Agentless Collector (Agentless Collector) können Sie den Status des Collectors sehen und eine Methode zur Datenerfassung auswählen, wie in den folgenden Themen beschrieben.

Topics

- [Collector-Status](#)
- [Datenerfassung](#)

Collector-Status

Der Collector-Status gibt Ihnen Statusinformationen über den Collector. Der Name des Collectors, der Status der Verbindung des Collectors zu AWS, die Heimatregion des Migration Hub und die Version.

Wenn Sie AWS Verbindungsprobleme haben, müssen Sie möglicherweise die Agentless Collector-Konfigurationseinstellungen bearbeiten.

Um die Collector-Konfigurationseinstellungen zu bearbeiten, wählen Sie Collector-Einstellungen bearbeiten und folgen Sie den Anweisungen unter [Bearbeiten der Agentless Collector-Einstellungen](#).

Datenerfassung

Unter Datenerfassung können Sie eine Datenerfassungsmethode auswählen. Application Discovery Service Agentless Collector (Agentless Collector) unterstützt derzeit die Datenerfassung von VMware VMs und von Datenbank- und Analyseservern. Zukünftige Module werden die Erfassung von zusätzlichen Virtualisierungsplattformen sowie die Erfassung auf Betriebssystemebene unterstützen.

Topics

- [VMware vCenter-Datenerfassung](#)
- [Erfassung von Datenbank- und Analysedaten](#)

VMware vCenter-Datenerfassung

Richten Sie Verbindungen zu Ihren vCenter-Servern ein, um Serverinventar- VMware VMs, Profil- und Nutzungsdaten von Ihnen zu sammeln. Um die Verbindungen einzurichten, wählen Sie im Abschnitt VMware vCenter die Option Einrichten aus und folgen Sie den Anweisungen unter [Verwenden des VMware vCenter Agentless Collector-Datenerfassungsmoduls](#).

Nachdem Sie die vCenter-Datenerfassung eingerichtet haben, können Sie vom Dashboard aus Folgendes ausführen:

- Status der Datenerfassung anzeigen
- Starten der Datenerfassung
- Beenden der Datensammlung

Note

Nachdem Sie die vCenter-Datenerfassung eingerichtet haben, wird auf der Dashboard-Seite die Schaltfläche Einrichten im Abschnitt VMwarevCenter durch Statusinformationen zur Datenerfassung, die Schaltflächen Datenerfassung beenden und Anzeigen und Bearbeiten ersetzt.

Erfassung von Datenbank- und Analysedaten

Sie können Ihr Modul zur Erfassung von Datenbank- und Analysedaten in den folgenden beiden Modi ausführen.

Metadaten und Datenbankkapazität

Das Datenerfassungsmodul sammelt Informationen wie Schemas, Versionen, Editionen, CPU, Arbeitsspeicher und Festplattenkapazität von Ihren Datenbank- und Analyseservern. Sie können diese gesammelten Informationen verwenden, um Zielempfehlungen in der AWS DMS Konsole zu berechnen. Wenn Ihre Quelldatenbank über- oder unterprovisioniert ist, werden auch die Zielempfehlungen über- oder unterprovisioniert.

Das ist der Standardmodus.

Metadaten, Datenbankkapazität und Ressourcennutzung

Zusätzlich zu den Metadaten und Informationen zur Datenbankkapazität erfasst das Datenerfassungsmodul die tatsächlichen Nutzungskennzahlen für CPU, Arbeitsspeicher und Festplattenkapazität für die Datenbanken und Analyseserver. Dieser Modus bietet genauere Zielempfehlungen als der Standardmodus, da die Empfehlungen auf den tatsächlichen Datenbank-Workloads basieren. In diesem Modus erfasst das Datenerfassungsmodul jede Minute Leistungskennzahlen.

Um mit der Erfassung von Metadaten und Leistungsmetriken von Ihren Datenbank- und Analyseservern zu beginnen

1. Wählen Sie auf der Seite Datenbank- und Analyse-Collector im Navigationsbereich die Option Datenerfassung aus.
2. Wählen Sie in der Liste Datenbankinventar die Datenbank- und Analyseserver aus, für die Sie Metadaten und Leistungsmetriken sammeln möchten.
3. Wählen Sie Datenerfassung ausführen aus. Das Dialogfeld Datenerfassungstyp wird geöffnet.
4. Wählen Sie aus, wie Daten für die Analyse gesammelt werden sollen.

Wenn Sie die Option Metadaten, Datenbankkapazität und Ressourcennutzung wählen, legen Sie den Zeitraum für die Datenerfassung fest. Sie können Daten in den nächsten 7 Tagen erfassen oder den benutzerdefinierten Zeitraum von 1–60 Tagen festlegen.

5. Wählen Sie Datenerfassung ausführen aus. Die Seite Datenerfassung wird geöffnet.
6. Wählen Sie die Registerkarte „Integrität der Erfassung“, um den Status der Datenerfassung zu sehen.

Nach Abschluss der Datenerfassung lädt Ihr Datenerfassungsmodul die gesammelten Daten in Ihren Amazon S3 S3-Bucket hoch. Anschließend können Sie sich diese gesammelten Daten wie unter beschrieben ansehen. [Ihre gesammelten Daten anzeigen](#)

Bearbeiten der Agentless Collector-Einstellungen

Sie haben den Collector konfiguriert, als Sie Application Discovery Service Agentless Collector (Agentless Collector) zum ersten Mal eingerichtet haben, wie unter beschrieben. [Agentless](#)

[Collector konfigurieren](#) Im folgenden Verfahren wird beschrieben, wie Sie die Agentless Collector-Konfigurationseinstellungen bearbeiten.

Um die Collector-Konfigurationseinstellungen zu bearbeiten

- Wählen Sie im Agentless Collector-Dashboard die Schaltfläche Collector-Einstellungen bearbeiten.

Gehen Sie auf der Seite Collector-Einstellungen bearbeiten wie folgt vor:

- a. Geben Sie unter Collector-Name einen Namen ein, um den Collector zu identifizieren. Der Name kann Leerzeichen, aber keine Sonderzeichen enthalten.
- b. Geben Sie unter AWS Zielkonto für Ermittlungsdaten den AWS Zugriffsschlüssel und den geheimen Schlüssel für das AWS Konto ein, das als Zielkonto für den Empfang der vom Collector erkannten Daten angegeben werden soll. Informationen zu den Anforderungen für den IAM-Benutzer finden Sie unter [Bereitstellung von Application Discovery Service Agentless Collector](#).
 - i. Geben Sie für den AWS Zugriffsschlüssel den Zugriffsschlüssel des AWS Konto-IAM-Benutzers ein, den Sie als Zielkonto angeben.
 - ii. Geben Sie für AWS Secret-Key den geheimen Schlüssel des AWS Konto-IAM-Benutzers ein, den Sie als Zielkonto angeben.
- c. Ändern Sie unter Agentless Collector-Passwort das Passwort, das zur Authentifizierung des Zugriffs auf den Agentless Collector verwendet werden soll.
 - i. Geben Sie für das Agentless Collector-Passwort ein Passwort ein, mit dem Sie den Zugriff auf den Agentless Collector authentifizieren können.
 - ii. Um das Agentless Collector-Passwort erneut einzugeben, geben Sie das Passwort zur Bestätigung erneut ein.
- d. Wählen Sie Konfigurationen speichern.

Als Nächstes werden Sie sehen [Das Agentless Collector-Dashboard](#).

Bearbeiten von VMware vCenter-Anmeldeinformationen

Richten Sie Verbindungen zu Ihren vCenter-Servern ein, um Serverinventar- VMware VMs, Profil- und Nutzungsdaten von Ihnen zu sammeln. Informationen zum Einrichten von VMware

vCenter-Verbindungen finden Sie unter [Verwenden des VMware vCenter Agentless Collector-Datenerfassungsmoduls](#).

In diesem Abschnitt wird beschrieben, wie Sie die vCenter-Anmeldeinformationen bearbeiten.

 Note

Stellen Sie vor dem Bearbeiten der vCenter-Anmeldeinformationen sicher, dass Sie vCenter-Anmeldeinformationen mit den für die Systemgruppe festgelegten Lese- und Anzeigeberechtigungen angeben können.

So bearbeiten Sie die VMware vCenter-Anmeldeinformationen

Wählen Sie auf der [Details VMware zur Datenerfassung anzeigen](#) Seite die Option vCenter-Server bearbeiten aus.

- Gehen Sie auf der Seite „vCenter bearbeiten“ wie folgt vor:
 - a. Unter den vCenter-Anmeldeinformationen:
 - i. Geben Sie für vCenter URL/IP die IP-Adresse Ihres VMware vCenter Server-Hosts ein.
 - ii. Geben Sie bei vCenter Username (vCenter-Benutzername) den Namen eines lokalen oder Domänenbenutzers ein, den der Konnektor zur Kommunikation mit vCenter verwendet. Für Domänenbenutzer: Verwenden Sie die Form Domäne\Benutzername oder Benutzername@Domäne.
 - iii. Geben Sie für vCenter Password (vCenter-Passwort) das lokale oder Domänenbenutzerpasswort ein.
 - b. Wählen Sie Speichern.

Manuelles Aktualisieren von Application Discovery Service Agentless Collector

Wenn Sie Application Discovery Service Agentless Collector (Agentless Collector) konfigurieren, können Sie wählen, ob automatische Updates aktiviert werden sollen, wie unter beschrieben.

[Agentless Collector konfigurieren](#) Wenn Sie automatische Updates nicht aktivieren, müssen Sie Agentless Collector manuell aktualisieren.

Im folgenden Verfahren wird beschrieben, wie Agentless Collector manuell aktualisiert wird.

Um Agentless Collector manuell zu aktualisieren

1. Besorgen Sie sich die neueste Agentless Collector Open Virtualization Archive (OVA) -Datei.
2. (Optional) Wir empfehlen, dass Sie die vorherige Agentless Collector OVA-Datei löschen, bevor Sie die neueste bereitstellen.
3. Folgen Sie den Anweisungen unter [Stellen Sie Agentless Collector bereit](#).

Das vorherige Verfahren aktualisiert nur den Agentless Collector. Es liegt in Ihrer Verantwortung, das Betriebssystem auf dem neuesten Stand zu halten.

So aktualisieren Sie Ihre Amazon EC2 EC2-Instance

1. Rufen Sie die IP-Adresse des Agentless Collectors von VMware vCenter ab.
2. Öffnen Sie die VM-Konsole des Collectors und melden Sie sich **ec2-user** mit dem Passwort an, **collector** wie im folgenden Beispiel gezeigt.

```
username: ec2-user
password: collector
```

3. Folgen Sie den Anweisungen unter [Instance-Software auf Ihrer AL2 Instance aktualisieren](#) im Amazon Linux 2-Benutzerhandbuch.

Kernel Live-Patching

Agentless Collector version 2

Die virtuelle Maschine Agentless Collector Version 2 verwendet Amazon Linux 2023, wie unter beschrieben [Stellen Sie Agentless Collector bereit](#).

Informationen zur Aktivierung und Verwendung von Live Patching für Amazon Linux 2023 finden Sie unter [Kernel Live Patching on AL2023](#) im Amazon EC2 EC2-Benutzerhandbuch.

Agentless Collector version 1

Die virtuelle Maschine Agentless Collector Version 1 verwendet Amazon Linux 2, wie unter beschrieben [Stellen Sie Agentless Collector bereit](#).

Informationen zur Aktivierung und Verwendung von Live Patching für Amazon Linux 2 finden Sie unter [Kernel Live Patching on AL2](#) im Amazon EC2 EC2-Benutzerhandbuch.

Um ein Upgrade von Agentless Collector Version 1 auf Version 2 durchzuführen

1. Installieren Sie eine neue Agentless Collector OVA mithilfe des neuesten Images.
2. Richten Sie die Anmeldeinformationen ein.
3. Löschen Sie die alte virtuelle Appliance.

Fehlerbehebung bei Agentless Collector

Dieser Abschnitt enthält Themen, die Ihnen bei der Behebung bekannter Probleme mit Application Discovery Service Agentless Collector (Agentless Collector) helfen können.

Themen

- [Reparieren Unable to retrieve manifest or certificate file error](#)
- [Behebung von Problemen mit selbstsignierten Zertifizierungen bei der Konfiguration von WinRM-Zertifikaten](#)
- [Behebung des Problems, das Agentless Collector AWS während der Installation nicht erreichen kann](#)
- [Behebung von Problemen mit selbstsignierten Zertifizierungen beim Herstellen einer Verbindung zum Proxyhost](#)
- [Suche nach fehlerhaften Collectors](#)
- [Behebung von Problemen mit IP-Adressen](#)
- [Behebung von Problemen mit vCenter-Anmeldeinformationen](#)
- [Behebung von Problemen bei der Datenweiterleitung im Modul zur Erfassung von Datenbank- und Analysedaten](#)
- [Behebung von Verbindungsproblemen im Modul zur Erfassung von Datenbank- und Analysedaten](#)
- [Unterstützung eigenständiger ESX-Hosts](#)
- [Kontaktaufnahme mit dem AWS Support bei Problemen mit Agentless Collector](#)

Reparieren **Unable to retrieve manifest or certificate file error**

Wenn Sie diesen Fehler erhalten, wenn Sie versuchen, die OVA über die Amazon S3 S3-URL in der VMware vCenter-Benutzeroberfläche bereitzustellen, stellen Sie sicher, dass Ihr vCenter Server die folgenden Anforderungen erfüllt:

- VMware vCenter Server Version 8.0 Update 1 oder höher
- VMware vCenter Server 7.0 Update 3q (ISO Build 23788036) oder höher

Behebung von Problemen mit selbstsignierten Zertifizierungen bei der Konfiguration von WinRM-Zertifikaten

Wenn Sie WinRM-Zertifikatsprüfungen aktivieren, müssen Sie möglicherweise eine selbstsignierte Zertifizierungsstelle in den Agentless Collector importieren.

Um eine selbstsignierte Zertifizierungsstelle zu importieren

1. Öffnen Sie die VM-Webkonsole des Collectors in VMware vCenter und melden Sie sich `ec2-user` mit dem Passwort an, `collector` wie im folgenden Beispiel gezeigt.

```
username: ec2-user
password: collector
```

2. Stellen Sie sicher, dass sich jedes selbstsignierte CA-Zertifikat, das zum Signieren von WinRM-Zertifikaten verwendet wird, im Verzeichnis befindet. `/etc/pki/ca-trust/source/anchors`
Beispiel:

```
/etc/pki/ca-trust/source/anchors/https-winrm-ca-1.pem
```

3. Führen Sie den folgenden Befehl aus, um die neuen Zertifikate zu installieren.

```
sudo update-ca-trust
```

4. Starten Sie den Agentless Collector neu, indem Sie den folgenden Befehl ausführen

```
sudo shutdown -r now
```

5. (Optional) Um zu überprüfen, ob Zertifikate erfolgreich importiert wurden, können Sie den folgenden Befehl ausführen.

```
sudo trust list --filter=ca-anchors | less
```

Behebung des Problems, das Agentless Collector AWS während der Installation nicht erreichen kann

Agentless Collector benötigt ausgehenden Zugriff über TCP-Port 443 auf mehrere Domänen. AWS Bei der Konfiguration von Agentless Collector in der Konsole kann die folgende Fehlermeldung angezeigt werden.

Konnte nicht erreicht werden AWS

AWS kann nicht erreicht werden. Bitte überprüfen Sie die Netzwerkeinstellungen.

Dieser Fehler tritt aufgrund eines fehlgeschlagenen Versuchs von Agentless Collector auf, eine HTTPS-Verbindung zu einer AWS Domain herzustellen, mit der der Collector während des Einrichtungsvorgangs kommunizieren muss. Die Agentless Collector-Konfiguration schlägt fehl, wenn keine Verbindung hergestellt werden kann.

Um die Verbindung zu reparieren AWS

1. Erkundigen Sie sich bei Ihrem IT-Administrator, ob die Firewall Ihres Unternehmens ausgehenden Datenverkehr auf Port 443 zu AWS Domänen blockiert, für die ausgehenden Zugriff erforderlich ist. Für welche AWS Domains ein ausgehender Zugriff erforderlich ist, hängt davon ab, ob Ihre Heimatregion die Region USA West (Oregon), US-West-2 oder eine andere Region ist.

Für die folgenden Domains ist ausgehender Zugriff erforderlich, wenn die Heimatregion Ihres AWS Kontos US-West-2 ist:

- `arsenal-discovery.us-west-2.amazonaws.com`
- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

Für die folgenden Domains ist ausgehender Zugriff erforderlich, wenn die Heimatregion Ihres AWS Kontos nicht der Fall ist: **us-west-2**

- `arsenal-discovery.us-west-2.amazonaws.com`
- `arsenal-discovery.your-home-region.amazonaws.com`
- `migrationhub-config.us-west-2.amazonaws.com`
- `api.ecr-public.us-east-1.amazonaws.com`
- `public.ecr.aws`

Wenn Ihre Firewall den ausgehenden Zugriff auf die AWS Domains blockiert, mit denen Agentless Collector kommunizieren muss, konfigurieren Sie im Abschnitt Datensynchronisierung unter Collector-Konfiguration einen Proxyhost.

2. Wenn das Verbindungsproblem durch die Aktualisierung der Firewall nicht behoben wird, gehen Sie wie folgt vor, um sicherzustellen, dass die virtuelle Collector-Maschine über eine ausgehende Netzwerkverbindung zu den im vorherigen Schritt aufgeführten Domänen verfügt.
 - a. Rufen Sie die IP-Adresse des Agentless Collectors von VMware vCenter ab.
 - b. Öffnen Sie die VM-Webkonsole des Collectors und melden Sie sich **ec2-user** mit dem Passwort an, **collector** wie im folgenden Beispiel gezeigt.

```
username: ec2-user
password: collector
```

- c. Testen Sie die Verbindung zu den aufgelisteten Domänen, indem Sie Telnet auf den Ports 443 ausführen, wie im folgenden Beispiel gezeigt.

```
telnet migrationhub-config.us-west-2.amazonaws.com 443
```

3. Wenn Telnet die Domain nicht auflösen kann, versuchen Sie, einen statischen DNS-Server anhand der [Anweisungen für Amazon Linux 2](#) zu konfigurieren.
4. Falls der Fehler weiterhin besteht, finden Sie weitere Unterstützung unter [Kontaktaufnahme mit dem AWS Support bei Problemen mit Agentless Collector](#).

Behebung von Problemen mit selbstsignierten Zertifizierungen beim Herstellen einer Verbindung zum Proxyhost

Wenn die Kommunikation mit dem optional bereitgestellten Proxy über HTTPS erfolgt und der Proxy über ein selbstsigniertes Zertifikat verfügt, müssen Sie möglicherweise ein Zertifikat bereitstellen.

1. Rufen Sie die IP-Adresse des Agentless Collectors von VMware vCenter ab.
2. Öffnen Sie die VM-Webkonsole des Collectors und melden Sie sich `ec2-user` mit dem Passwort an, `collector` wie im folgenden Beispiel gezeigt.

```
username: ec2-user
password: collector
```

3. Fügen Sie den Hauptteil des Zertifikats, das dem sicheren Proxy zugeordnet ist, einschließlich `-----BEGIN CERTIFICATE-----` sowohl als auch `-----END CERTIFICATE-----`, in die folgende Datei ein:

```
/etc/pki/ca-trust/source/anchors/https-proxy-ca.pem
```

4. Führen Sie die folgenden Befehle aus, um das neue Zertifikat zu installieren:

```
sudo update-ca-trust
```

5. Starten Sie den Agentless Collector neu, indem Sie den folgenden Befehl ausführen:

```
sudo shutdown -r now
```

Suche nach fehlerhaften Collectors

Statusinformationen für jeden Collector finden Sie auf der Seite [Datensammler](#) der AWS Migration Hub (Migration Hub) -Konsole. Sie können Collectors mit Problemen identifizieren, indem Sie alle Collectors mit dem Status `Erfordert Aufmerksamkeit` suchen.

Im folgenden Verfahren wird beschrieben, wie Sie auf die Agentless Collector-Konsole zugreifen können, um Gesundheitsprobleme zu identifizieren.

So greifen Sie auf die Agentless Collector-Konsole zu

1. Melden Sie sich mit Ihrem AWS Konto bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole unter Discover die Option Datensammler aus.
3. Notieren Sie sich auf der Registerkarte Agentless Collectors die IP-Adresse für jeden Connector, der den Status Erfordert Aufmerksamkeit.
4. Öffnen Sie einen Webbrowser, um die Agentless Collector-Konsole zu öffnen. Geben Sie dann die folgende URL in die Adressleiste ein: **https:// <ip_address>/**, wobei ip_address die IP-Adresse eines fehlerhaften Collectors ist.
5. Wählen Sie Anmelden und geben Sie dann das Agentless Collector-Passwort ein, das bei der Konfiguration des Collectors eingerichtet wurde. [Agentless Collector konfigurieren](#)
6. Wählen Sie auf der Agentless Collector-Dashboard-Seite unter Datenerfassung im Abschnitt VMware vCenter die Option Anzeigen und bearbeiten aus.
7. Folgen Sie den Anweisungen unter [Bearbeiten von VMware vCenter-Anmeldeinformationen](#), um die URL und die Anmeldeinformationen zu korrigieren.

Nach der Behebung der Integritätsprobleme stellt der Collector die Konnektivität mit dem vCenter Server wieder her, und der Status des Collectors ändert sich in den Status Sammeln. Falls die Probleme weiterhin bestehen, finden Sie weitere Informationen unter. [Kontaktaufnahme mit dem AWS Support bei Problemen mit Agentless Collector](#)

Die häufigsten Ursachen für fehlerhafte Collectors sind Probleme mit IP-Adressen und Anmeldeinformationen. [Behebung von Problemen mit IP-Adressen](#) und [Behebung von Problemen mit vCenter-Anmeldeinformationen](#) kann Ihnen helfen, diese Probleme zu lösen und einen Collector wieder in einen fehlerfreien Zustand zu versetzen.

Behebung von Problemen mit IP-Adressen

Ein Collector kann in einen fehlerhaften Zustand übergehen, wenn der beim Collector-Setup angegebene vCenter-Endpoint fehlerhaft oder ungültig ist oder wenn der vCenter Server derzeit ausgefallen und nicht erreichbar ist. In diesem Fall erhalten Sie eine Verbindungsfehlermeldung.

Das folgende Verfahren kann bei der Behebung von IP-Adressproblemen helfen.

Um Probleme mit der Collector-IP-Adresse zu beheben

1. Rufen Sie die IP-Adresse des Agentless Collectors von VMware vCenter ab.
2. Öffnen Sie die Agentless Collector-Konsole, indem Sie einen Webbrowser öffnen, und geben Sie dann die folgende URL in die Adressleiste ein: **https:// <ip_address>/**, wobei ip_address die IP-Adresse des Collectors ist. [Stellen Sie Agentless Collector bereit](#)
3. Wählen Sie Anmelden und geben Sie dann das Agentless Collector-Passwort ein, das bei der Konfiguration des Collectors eingerichtet wurde. [Agentless Collector konfigurieren](#)
4. Wählen Sie auf der Agentless Collector-Dashboard-Seite unter Datenerfassung im Abschnitt VMware vCenter die Option Anzeigen und bearbeiten aus.
5. Notieren Sie sich auf der Seite mit den Details zur VMware Datenerfassung unter Entdeckte vCenter-Server die IP-Adresse in der Spalte vCenter.
6. Überprüfen Sie mit einem separaten Befehlszeilentool wie ping oder traceroute, ob der zugehörige vCenter Server aktiv ist und die IP von der Collector-VM aus erreichbar ist.
 - Wenn die IP-Adresse falsch ist und der vCenter-Dienst aktiv ist, aktualisieren Sie die IP-Adresse in der Collector-Konsole und wählen Sie Weiter.
 - Wenn die IP-Adresse richtig, der vCenter-Server aber inaktiv ist, aktivieren Sie den Server.
 - Wenn die IP-Adresse richtig und der vCenter-Server aktiv ist, prüfen Sie, ob er aufgrund der Firewall-Einstellungen eingehende Netzwerkverbindungen blockiert. Falls ja, aktualisieren Sie Ihre Firewall-Einstellungen, um eingehende Verbindungen von der Collector-VM zuzulassen.

Behebung von Problemen mit vCenter-Anmeldeinformationen

Collectors können in einen fehlerhaften Zustand übergehen, wenn die bei der Konfiguration eines Collectors angegebenen vCenter-Benutzeranmeldedaten ungültig sind oder keine vCenter Read- und View-Kontoberechtigungen haben.

Wenn Sie Probleme mit den vCenter-Anmeldeinformationen haben, stellen Sie sicher, dass Sie die vCenter-Lese- und View-Berechtigungen für die Systemgruppe festgelegt haben.

Informationen zum Bearbeiten von vCenter-Anmeldeinformationen finden Sie unter [Bearbeiten von VMware vCenter-Anmeldeinformationen](#).

Behebung von Problemen bei der Datenweiterleitung im Modul zur Erfassung von Datenbank- und Analysedaten

Auf der Startseite des Moduls zur Erfassung von Datenbank- und Analysedaten in Agentless Collector wird der Verbindungsstatus für Access to DMS und Access to S3 angezeigt. Wenn für Access to DMS und Access to S3 die Option Kein Zugriff angezeigt wird, konfigurieren Sie die Datenweiterleitung. Weitere Informationen finden Sie unter [Konfiguration der Datenweiterleitung](#).

Wenn dieses Problem nach der Konfiguration der Datenweiterleitung auftritt, überprüfen Sie, ob Ihr Datenerfassungsmodul auf das Internet zugreifen kann. Stellen Sie anschließend sicher, dass Sie Ihrem DMSCollectorIAM-Benutzer die Richtlinien Policy und FleetAdvisorS3Policy hinzugefügt haben. Weitere Informationen finden Sie unter [Bereitstellung von Application Discovery Service Agentless Collector](#).

Wenn Ihr Datenerfassungsmodul keine Verbindung zu den folgenden Domänen herstellen kann AWS, gewähren Sie ausgehenden Zugriff auf die folgenden Domänen.

- `dms.your-home-region.amazonaws.com`
- `s3.amazonaws.com`

Behebung von Verbindungsproblemen im Modul zur Erfassung von Datenbank- und Analysedaten

Das Modul zur Erfassung von Datenbank- und Analysedaten in Agentless Collector stellt eine Verbindung zu Ihren LDAP-Servern her, um Betriebssystemserver in Ihrer Datenumgebung zu erkennen. Anschließend stellt das Datenerfassungsmodul eine Verbindung zu Ihren Betriebssystemservern her, um Datenbank- und Analyseserver zu ermitteln. Von diesen Datenbankservern sammelt das Datenerfassungsmodul Kapazitäts- und Leistungskennzahlen. Wenn Ihr Datenerfassungsmodul keine Verbindung zu diesen Servern herstellen kann, stellen Sie sicher, dass Sie eine Verbindung zu Ihren Servern herstellen können.

Ersetzen Sie in den folgenden Beispielen *replaceable* Werte durch Ihre Werte.

- Um zu überprüfen, ob Sie eine Verbindung zu Ihrem LDAP-Server herstellen können, installieren Sie das `ldap-util` Paket. Führen Sie dazu den folgenden Befehl aus.

```
sudo apt-get install ldap-util
```

Führen Sie anschließend den folgenden Befehl aus.

```
ldapsearch -x -D "CN=user,CN=Users,DC=example,DC=com" -w "password" -b  
"dc=example,dc=com" -h
```

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einem Linux-Betriebssystemserver herstellen können.

```
ssh -i C:\Users\user\private_key.pem -p 22 username@my-linux-host.domain.com
```

Führen Sie das vorherige Beispiel als Administrator in Windows aus.

```
ssh username@my-linux-host.domain.com
```

Führen Sie das vorherige Beispiel unter Linux aus.

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einem Windows-Betriebssystemserver herstellen können.

```
winrs -r:[hostname or ip] -u:username -p:password cmd
```

Führen Sie das vorherige Beispiel als Administrator in Windows aus.

```
sudo apt install -y winrm  
winrm --user=username --password=password [http or https]://[hostname or ip]:[port]  
"[cmd.exe or any other CLI command]"
```

Führen Sie das vorherige Beispiel unter Linux aus.

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einer SQL Server-Datenbank herstellen können.

```
sqlcmd -S [hostname or IP] -U username -P 'password'  
SELECT GETDATE() AS sysdate
```

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einer MySQL-Datenbank herstellen können.

```
mysql -u username -p 'password' -h [hostname or IP] -P [port]
```

```
SELECT NOW() FROM DUAL
```

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einer Oracle-Datenbank herstellen können.

```
sqlplus username/password@[hostname or IP]:port/servicename  
SELECT SYSDATE FROM DUAL
```

- Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Sie eine Verbindung zu einer PostgreSQL-Datenbank herstellen können.

```
psql -U username -h [hostname or IP] -p port -d database  
SELECT CURRENT_TIMESTAMP AS sysdate
```

Wenn Sie keine Verbindung zu Ihren Datenbank- und Analyseservern herstellen können, stellen Sie sicher, dass Sie die erforderlichen Berechtigungen bereitstellen. Weitere Informationen finden Sie unter [Ermitteln Sie Ihre Datenbankserver](#).

Unterstützung eigenständiger ESX-Hosts

Der Agentless Collector unterstützt keinen eigenständigen ESX-Host. Der ESX-Host muss Teil der vCenter Server-Instance sein.

Kontaktaufnahme mit dem AWS Support bei Problemen mit Agentless Collector

Wenn Sie Probleme mit Application Discovery Service Agentless Collector (Agentless Collector) haben und Hilfe benötigen, wenden Sie sich an den [AWS Support](#). Sie werden kontaktiert und möglicherweise aufgefordert, die Collector-Protokolle zu senden.

Um Agentless Collector-Protokolle zu erhalten

1. Rufen Sie die IP-Adresse des Agentless Collectors von VMware vCenter ab.
2. Öffnen Sie die VM-Webkonsole des Collectors und melden Sie sich **ec2-user** mit dem Passwort an, **collector** wie im folgenden Beispiel gezeigt.

```
username: ec2-user  
password: collector
```

3. Verwenden Sie den folgenden Befehl, um zum Protokollordner zu navigieren.

```
cd /var/log/aws/collector
```

4. Komprimieren Sie die Protokolldateien mithilfe der folgenden Befehle.

```
sudo cp /local/agentless_collector/compose.log .  
docker inspect $(docker ps --format {{.Names}}) | sudo tee docker_inspect.log >/dev/null  
sudo tar czf logs_$(date '+%d-%m-%Y_%H.%M.%S').tar.gz --exclude='db.mv*' *
```

5. Kopieren Sie die Protokolldatei von der Agentless Collector-VM.

```
scp logs*.tar.gz targetuser@targetaddress
```

6. Geben Sie die tar.gz Datei an AWS Enterprise Support weiter.

Daten in Migration Hub importieren

AWS Migration Hub Mit dem Import von (Migration Hub) können Sie Details Ihrer lokalen Umgebung direkt in Migration Hub importieren, ohne den Application Discovery Service Agentless Collector (Agentless Collector) oder den AWS Application Discovery Agent (Discovery Agent) zu verwenden, sodass Sie die Migrationsbewertung und -planung direkt anhand Ihrer importierten Daten durchführen können. Sie können auch Ihre Geräte als Anwendungen gruppieren und deren Migrationsstatus nachverfolgen.

Auf dieser Seite werden die Schritte zum Ausfüllen einer Importanfrage beschrieben. Zunächst verwenden Sie eine der folgenden beiden Optionen, um Ihre lokalen Serverdaten vorzubereiten.

- Verwenden Sie gängige Tools von Drittanbietern, um eine Datei zu generieren, die Ihre lokalen Serverdaten enthält.
- Laden Sie unsere Importvorlage für kommagetrennte Werte (CSV) herunter und füllen Sie sie mit Ihren lokalen Serverdaten auf.

Nachdem Sie eine der beiden zuvor beschriebenen Methoden verwendet haben, um Ihre lokale Datendatei zu erstellen, laden Sie die Datei auf Migration Hub hoch, indem Sie die Migration Hub Hub-Konsole verwenden AWS CLI, oder eine der AWS SDKs. Weitere Informationen zu den beiden Optionen finden Sie unter [the section called “Unterstützte Importformate”](#).

Sie können mehrere Importanforderungen übermitteln. Jede Anforderung wird sequentiell verarbeitet. Sie können den Status Ihrer Importanfragen jederzeit über die Konsole oder den Import überprüfen APIs.

Nachdem eine Importanfrage abgeschlossen ist, können Sie die Details der einzelnen importierten Datensätze anzeigen. Zeigen Sie Nutzungsdaten, Tags und Anwendungszuordnungen direkt in der Migration Hub Hub-Konsole an. Wenn während des Importvorgangs Fehler aufgetreten sind, können Sie die Anzahl der erfolgreichen und fehlgeschlagenen Datensätze sowie die Fehlerdetails für jeden fehlgeschlagenen Datensatz prüfen.

Fehlerbehandlung: Ein Link wird bereitgestellt, um das Fehlerprotokoll und fehlgeschlagene Datensatzdateien im CSV-Format als komprimiertes Archiv herunterzuladen. Verwenden Sie diese Dateien, um Ihre Importanfrage erneut zu senden, nachdem Sie die Fehler korrigiert haben.

Es gibt Beschränkungen in Bezug auf die Anzahl der importierten Datensätze, der importierten Server und der gelöschten Datensätze, die Sie behalten können. Weitere Informationen finden Sie unter [AWS Application Discovery Service Kontingente](#).

Unterstützte Importformate

Migration Hub unterstützt die folgenden Importformate.

- [RVTools](#)
- [Migration Hub Hub-Importvorlage](#)

RVTools

Migration Hub unterstützt den Import von Exporten von VMware vSphere über RVTools. Wählen Sie beim Speichern von RVTools Daten zuerst die Option Alles nach CSV exportieren oder Alle nach Excel exportieren, komprimieren Sie dann den Ordner und importieren Sie die ZIP-Datei in Migration Hub. Die folgenden Dateien sind in der ZIP-Datei erforderlich: vInfo, vNetwork, vCPU, vMemory, vDisk, vPartition, vSource, vTools, vHost, vNIC, vSC_VMK.

Migration Hub Hub-Importvorlage

Mit dem Migration Hub Hub-Import können Sie Daten aus einer beliebigen Quelle importieren. Die bereitgestellten Daten müssen im unterstützten Format für eine CSV-Datei vorliegen, und die Daten dürfen nur die unterstützten Felder mit den unterstützten Bereichen für diese Felder enthalten.

Ein Sternchen (*) neben einem Importfeldnamen in der folgenden Tabelle weist darauf hin, dass es sich um ein erforderliches Feld handelt. Für jeden Datensatz Ihrer Importdatei müssen mindestens eines oder mehrere dieser Pflichtfelder ausgefüllt sein, damit die eindeutige Identifizierung eines Servers oder einer Anwendung möglich ist. Ein Datensatz ohne Angaben in einem der erforderlichen Felder wird nicht importiert.

Ein Einfügezeichen (^) neben dem Namen einer Importdatei in der folgenden Tabelle bedeutet, dass sie schreibgeschützt ist, wenn eine serverId angegeben wird.

Note

Wenn Sie eines der beiden verwenden. VMware MoRefId oder VMWare. VCenterID, um einen Datensatz zu identifizieren, müssen Sie beide Felder in demselben Datensatz haben.

Importfeldname	Description	Beispiele
ExternalId [^]	Eine benutzerdefinierte Kennung, die es Ihnen ermöglicht, die Datensätze als eindeutig zu kennzeichnen. Dies ExternalId kann beispielsweise die Inventarnummer für den Server in Ihrem Rechenzentrum sein.	Inventory Id 1 Server 2 CMBD Id 3
SMBiosID [^]	Systemmanagement-BIOS-(SMBIOS) ID.	
IPAddress [^]	Eine durch Kommata getrennte Liste von IP-Adressen des Servers, in Anführungszeichen.	192.0.0.2 „10.12.31.233, 10.12.32.11“
MACAddress [^]	Eine durch Kommata getrennte Liste von MAC-Adressen des Servers, in Anführungszeichen.	00:1B:44:11:3A:B7 „00-15-E9-2B-99-3C, 00-14-22-01-23-45“
HostName [^]	Der Hostname des Servers. Wir empfehlen die Verwendung des vollständig qualifizierten Domännennamens (FQDN, Fully Qualified Domain Name) für diesen Wert.	ip-1-2-3-4 localhost.domain
VMware.MoRefId [^]	Die verwaltete Objektreferenz-ID Muss mit einem VMware versehen sein. VCenterAusweis.	
VMware.VCenterID [^]	Eindeutige Kennung einer virtuellen Maschine. Muss mit	

Importfeldname	Description	Beispiele
	einem versehen sein. VMware MoRefld.	
CPU. NumberOfProcessors^	Die Anzahl von CPUs.	4
CPU. NumberOfCores^	Die Gesamtzahl der physischen Kerne.	8
ZENTRALPROZESSOR. NumberOfLogicalCores^	Die Gesamtzahl der Threads, die gleichzeitig auf allen CPUs Threads auf einem Server ausgeführt werden können. Einige CPUs unterstützen die gleichzeitige Ausführung mehrerer Threads auf einem einzelnen CPU-Kern. In diesen Fällen ist diese Zahl größer als die Anzahl der physischen (oder virtuellen) Kerne.	16
Betriebssystemname^	Der Name des Betriebssystems.	Linux Windows.Hat
Betriebssystemversion ^	Die Version des Betriebssystems.	16.04.3 NT 6.2.8
VMware.VMName^	Der Name der virtuellen Maschine.	Corp1
RAM. TotalSizeInMB ^	Der gesamte auf dem Server verfügbare RAM in MB.	64 128

Importfeldname	Description	Beispiele
RAM. UsedSizeInMB. AVG ^	Die durchschnittliche Menge an verwendetem RAM auf dem Server in MB.	64 128
RAM. UsedSizeInMB.max^	Die maximale Menge von auf dem Server verfügbaren verwendeten RAM in MB.	64 128
ZENTRALPROZESSOR. UsagePct.Avg^	Die durchschnittliche CPU-Auslastung während der Datenerfassung durch das Discovery-Tool.	45 23.9
ZENTRALPROZESSOR. UsagePct.Max^	Die maximale CPU-Auslastung während der Datenerfassung durch das Discovery-Tool.	55.34 24
DiskReadsPerSecond InkB.AVG^	Die durchschnittliche Anzahl der Festplattenlesevorgänge pro Sekunde, in KB.	1159 84506
DiskWritesPerSecond InkB.AVG^	Die durchschnittliche Anzahl der Festplattenschreibvorgänge pro Sekunde, in KB.	199 6197
DiskReadsPerSecond InKB.max^	Die maximale Anzahl der Festplattenlesevorgänge pro Sekunde, in KB.	37892 869962
DiskWritesPerSecond InkB.max^	Die maximale Anzahl der Festplattenschreibvorgänge pro Sekunde, in KB.	18436 1808
DiskReadsOpsPerSecond.Avg^	Durchschnittliche Anzahl der Lesevorgänge pro Sekunde.	45 28

Importfeldname	Description	Beispiele
DiskWritesOpsPerSecond.Avg^	Durchschnittliche Anzahl der Festplattenschreibvorgänge pro Sekunde.	8 3
DiskReadsOpsPerSecond.Max^	Die maximale Anzahl der Festplattenlesevorgänge pro Sekunde.	1083 176
DiskWritesOpsPerSecond.Max^	Die maximale Anzahl der Festplattenschreibvorgänge pro Sekunde.	535 71
NetworkReadsPerSecondInkB.AVG^	Die durchschnittliche Anzahl der Netzwerklesevorgänge pro Sekunde, in KB.	45 28
NetworkWritesPerSecondInkB.AVG^	Die durchschnittliche Anzahl der Netzwerkschreibvorgänge pro Sekunde, in KB.	8 3
NetworkReadsPerSecondInkB.max^	Die maximale Anzahl der Netzwerklesevorgänge pro Sekunde, in KB.	1083 176
NetworkWritesPerSecondInkB.max^	Die maximale Anzahl der Netzwerkschreibvorgänge pro Sekunde, in KB.	535 71

Importfeldname	Description	Beispiele
Anwendungen	Eine durch Kommata getrennte Liste der Anwendungen, die diesen Server enthalten, in Anführungszeichen. Dieser Wert kann bestehende Anwendungen und and/or neue Anwendungen einschließen, die beim Import erstellt werden.	Application1 „Application2, Application3“
ApplicationWave	Die Migrationswelle für diesen Server.	
Stichworte [^]	Eine durch Kommata getrennte Liste der als Name:Wert formatierten Tags.	„zone:1, critical:yes“ „zone:3, critical:no, zone:1“
	 Important Speichern Sie keine sensiblen Informationen (wie persönliche Daten) in Tags.	
ServerId	Die Server-ID, wie sie in der Migration Hub-Serverliste zu sehen ist.	d-server-01kk9i6yw waxmp

Sie können Daten importieren, auch wenn Sie nicht für alle in der Importvorlage definierten Felder Daten eingegeben haben, sofern jeder Datensatz mindestens eines der Pflichtfelder enthält. Duplikate werden über mehrere Importanfragen hinweg über einen externen oder internen Abgleichsschlüssel verwaltet. Wenn Sie Ihren eigenen Abgleichsschlüssel eingeben, External ID, wird dieses Feld zur eindeutigen Identifizierung und zum Import der Datensätze verwendet. Wenn kein Abgleichsschlüssel angegeben wird, verwendet der Import einen intern generierten

Abgleichsschlüssel, der aus einigen der Spalten in der Importvorlage abgeleitet wird. Weitere Informationen zu diesem Abgleich finden Sie unter [Abgleichslogik für entdeckte Server und Anwendungen](#).

 Note

Der Migration Hub Hub-Import unterstützt keine Felder außerhalb der Felder, die in der Importvorlage definiert sind. Jegliche benutzerdefinierte Felder werden ignoriert und nicht importiert.

Importberechtigungen einrichten

Bevor Sie Ihre Daten importieren können, stellen Sie sicher, dass Ihr IAM-Benutzer über die erforderlichen Amazon S3-Berechtigungen verfügt, um Ihre Importdatei auf Amazon S3 hochzuladen (`s3:PutObject`) und das Objekt (`s3:GetObject`) zu lesen. Sie müssen auch den programmatischen Zugriff (für den AWS CLI) oder den Konsolenzugriff einrichten, indem Sie eine IAM-Richtlinie erstellen und sie dem IAM-Benutzer zuordnen, der Importe in Ihrem Konto durchführt.

AWS

Console Permissions

Gehen Sie wie folgt vor, um die Berechtigungsrichtlinie für den IAM-Benutzer zu bearbeiten, der über die Konsole Importanfragen in Ihrem AWS Konto stellt.

Die einem Benutzer hinzugefügten verwalteten Richtlinien bearbeiten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>
2. Klicken Sie im Navigationsbereich auf Users (Benutzer).
3. Wählen Sie den Namen des Benutzers aus, dessen Berechtigungsrichtlinie Sie ändern möchten.
4. Wählen Sie die Registerkarte Permissions (Berechtigungen) und anschließend die Option Add Permissions (Berechtigungen hinzufügen) aus.
5. Wählen Sie Attach existing policies directly (Vorhandene Richtlinien direkt zuweisen) und dann Create policy (Richtlinie erstellen).

- a. Wählen Sie auf der dann angezeigten Seite Create policy (Richtlinie erstellen) die Option JSON, und fügen Sie die folgende Richtlinie ein. Denken Sie daran, den Namen Ihres Buckets durch den tatsächlichen Namen des Buckets zu ersetzen, in den der IAM-Benutzer die importierten Dateien hochladen wird.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::importBucket/*"]
    }
  ]
}
```

- b. Wählen Sie Richtlinie prüfen.
- c. Geben Sie Ihrer Richtlinie unter Name einen neuen Namen, und fügen Sie optional eine Beschreibung hinzu, bevor Sie die Zusammenfassung der Richtlinie anzeigen.
- d. Wählen Sie Richtlinie erstellen aus.

6. Kehren Sie zur Seite „Berechtigungen gewähren“ in der IAM-Konsole für den Benutzer zurück, der Importanfragen in Ihrem AWS Konto stellen wird.
7. Aktualisieren Sie die Richtlinientabelle, und suchen Sie nach dem Namen der soeben erstellten Richtlinie.
8. Wählen Sie Weiter: Prüfen aus.
9. Wählen Sie Add permissions.

Nachdem Sie die Richtlinie Ihrem IAM-Benutzer hinzugefügt haben, können Sie den Importvorgang starten.

AWS CLI Permissions

Verwenden Sie das folgende Verfahren, um die verwalteten Richtlinien zu erstellen, die erforderlich sind, um einem IAM-Benutzer die Berechtigungen zu erteilen, Importdatenanfragen mithilfe von zu stellen. AWS CLI

Um die verwalteten Richtlinien zu erstellen und anzuhängen

1. Verwenden Sie den `aws iam create-policy` AWS CLI Befehl, um eine IAM-Richtlinie mit den folgenden Berechtigungen zu erstellen. Denken Sie daran, den Namen Ihres Buckets durch den tatsächlichen Namen des Buckets zu ersetzen, in den der IAM-Benutzer die importierten Dateien hochladen wird.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::importBucket"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ]
    }
  ],
}
```

```

    "Resource": ["arn:aws:s3:::importBucket/*"]
  }
]
}

```

Weitere Informationen zur Verwendung dieses Befehls finden Sie unter [create-policy](#) in der AWS CLI Befehlsreferenz.

2. Verwenden Sie den `aws iam create-policy` AWS CLI Befehl, um eine zusätzliche IAM-Richtlinie mit den folgenden Berechtigungen zu erstellen.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "discovery:ListConfigurations",
        "discovery:CreateApplication",
        "discovery:UpdateApplication",
        "discovery:AssociateConfigurationItemsToApplication",
        "discovery:DisassociateConfigurationItemsFromApplication",
        "discovery:GetDiscoverySummary",
        "discovery:StartImportTask",
        "discovery:DescribeImportTasks",
        "discovery:BatchDeleteImportData"
      ],
      "Resource": "*"
    }
  ]
}

```

3. Verwenden Sie den `aws iam attach-user-policy` AWS CLI Befehl, um die Richtlinien, die Sie in den beiden vorherigen Schritten erstellt haben, an den IAM-Benutzer anzuhängen, der Importanfragen in Ihrem AWS Konto mithilfe von durchführt. AWS CLI Weitere Informationen zur Verwendung dieses Befehls finden Sie [attach-user-policy](#) in der AWS CLI Befehlsreferenz.

Nachdem Sie Ihrem IAM-Benutzer die Richtlinien hinzugefügt haben, können Sie den Importvorgang starten.

Denken Sie daran, dass der IAM-Benutzer, wenn er Objekte in den von Ihnen angegebenen Amazon S3 S3-Bucket hochlädt, die Standardberechtigungen für die Objekte beibehalten muss, damit der Benutzer das Objekt lesen kann.

Ihre Importdatei auf Amazon S3 hochladen

Als Nächstes müssen Sie Ihre CSV-formatierte Importdatei in Amazon S3 hochladen, damit sie importiert werden kann. Bevor Sie beginnen, sollten Sie über einen Amazon S3 S3-Bucket verfügen, in dem Ihre zuvor and/or erstellte Importdatei gespeichert wird.

Console S3 Upload

So laden Sie Ihre Importdatei auf Amazon S3 hoch

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon S3 S3-Konsole unter <https://console.aws.amazon.com/s3/>.
2. Wählen Sie in der Liste Bucket name (Bucket-Name) den Namen des Buckets aus, zu dem Sie Ihr Objekt hochladen möchten.
3. Klicken Sie auf Upload.
4. Wählen Sie im Dialogfeld Upload (Hochladen) die Option Add Files (Dateien hinzufügen) aus, um die hochzuladende Datei auszuwählen.
5. Wählen Sie eine hochzuladende Datei und dann Öffnen aus.
6. Klicken Sie auf Upload.
7. Nachdem Sie die Datei hochgeladen haben, wählen Sie den Namen Ihres Datendatei-Objekts aus Ihrem Bucket-Dashboard.
8. Kopieren Sie von der Registerkarte Overview (Übersicht) der Objektdetails-Seite die Object URL (Objekt-URL). Sie benötigen diese beim Erstellen Ihrer Importanforderung.
9. Rufen Sie die Importseite in der Migration Hub Hub-Konsole auf, wie unter [beschrieben](#) [Importieren von Daten](#). Fügen Sie dann die Objekt-URL in das Feld Amazon S3 S3-Objekt-URL ein.

AWS CLI S3 Upload

So laden Sie Ihre Importdatei auf Amazon S3 hoch

1. Öffnen Sie ein Terminalfenster und navigieren Sie zu dem Verzeichnis, in dem Ihre Importdatei gespeichert ist.
2. Geben Sie den folgenden Befehl ein:

```
aws s3 cp ImportFile.csv s3://BucketName/ImportFile.csv
```

3. Dies gibt die folgenden Ergebnisse zurück:

```
upload: .\ImportFile.csv to s3://BucketName/ImportFile.csv
```

4. Kopieren Sie den vollständigen Amazon S3 S3-Objektpfad, der zurückgegeben wurde. Sie benötigen dies, wenn Sie Ihre Importanfrage erstellen.

Importieren von Daten

Nachdem Sie die Importvorlage von der Migration Hub-Konsole heruntergeladen und mit Ihren vorhandenen lokalen Serverdaten gefüllt haben, können Sie mit dem Import der Daten in Migration Hub beginnen. In den folgenden Anweisungen werden zwei Möglichkeiten beschrieben, dies zu tun, entweder mithilfe der Konsole oder durch API-Aufrufe über die AWS CLI

Console Import

Starten Sie den Datenimport auf der Seite Tools der Migration Hub Hub-Konsole.

So starten Sie den Datenimport:

1. Wählen Sie im Navigationsbereich unter Discover (Entdecken) Tools aus.
2. Wenn Sie nicht bereits eine Importvorlage ausgefüllt haben, können Sie die Vorlage herunterladen, indem Sie Import template (Importvorlage) im Feld Import auswählen. Öffnen Sie die heruntergeladene Vorlage, und füllen Sie sie mit Ihren vorhandenen lokalen Serverdaten aus. Sie können die Importvorlage auch aus unserem Amazon S3 S3-Bucket unter https://s3.us-west-2.amazonaws.com/templates-7cfcf56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv herunterladen
3. Um die Importseite zu öffnen, wählen Sie Import im Importfeld aus.

4. Geben Sie unter Importname einen Namen für den Import ein.
5. Füllen Sie das Feld Amazon S3 S3-Objekt-URL aus. Um diesen Schritt durchzuführen, müssen Sie Ihre Importdatei auf Amazon S3 hochladen. Weitere Informationen finden Sie unter [Ihre Importdatei auf Amazon S3 hochladen](#).
6. Wählen Sie Import im unteren rechten Bereich. Dadurch wird die Seite Imports (Importe) geöffnet, auf der Sie Ihren Import und seinen Status in der Tabelle sehen können.

Nachdem Sie die vorangegangenen Schritte zum Starten Ihres Datenimports durchgeführt haben, zeigt die Seite Imports (Importe) Details zu jeder Importanfrage einschließlich ihres Fortschritts, des Abschlusszeitpunkts und der Anzahl der erfolgreichen und fehlgeschlagenen Datensätze an; diese Datensätze können heruntergeladen werden. Von diesem Bildschirm können Sie auch zur Seite Servers (Server) unter Discover (Entdecken) navigieren, um die tatsächlichen importierten Daten anzuzeigen.

Auf der Seite Servers (Server) sehen Sie eine Liste aller erkannten Server (Geräte) zusammen mit dem jeweiligen Importnamen. Wenn Sie von der Seite Importe (Importverlauf) aus navigieren, indem Sie den Namen des Imports in der Spalte Name auswählen, werden Sie zur Seite Server weitergeleitet, auf der ein Filter angewendet wird, der auf dem Datensatz des ausgewählten Imports basiert. Dann sehen Sie nur Daten, die zu diesem bestimmten Import gehören.

Das Archiv ist im .zip-Format und enthält zwei Dateien; `errors-file` (Fehlerdatei) und `failed-entries-file` (Datei mit den fehlgeschlagenen Einträgen). Die Fehlerdatei enthält eine Liste der Fehlermeldungen zu jeder fehlgeschlagenen Zeile und dem zugehörigen Spaltennamen aus Ihrer Datendatei, deren Import fehlgeschlagen ist. Sie können diese Datei verwenden, um schnell zu identifizieren, wo Probleme aufgetreten sind. Die Datei mit den fehlgeschlagenen Einträgen enthält jede Zeile und die angegebenen fehlgeschlagenen Spalten. Sie können die in der Fehlerdatei angegebenen Korrekturen vornehmen und versuchen, die Datei erneut mit den korrigierten Informationen zu importieren.

AWS CLI Import

Um den Datenimportvorgang von aus zu starten AWS CLI, AWS CLI muss der zuerst in Ihrer Umgebung installiert werden. Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch unter [Installation der AWS Befehlszeilenschnittstelle](#).

 Note

Wenn Sie noch keine Importvorlage ausgefüllt haben, können Sie die Importvorlage hier aus unserem Amazon S3 S3-Bucket herunterladen: https://s3.us-west-2.amazonaws.com/templates-7cfff56-bd96-4b1c-b45b-a5b42f282e46/import_template.csv

So starten Sie den Datenimport:

1. Öffnen Sie ein Terminalfenster, und geben Sie den folgenden Befehl ein:

```
aws discovery start-import-task --import-url s3://BucketName/ImportFile.csv --  
name ImportName
```

2. Dadurch wird Ihre Importaufgabe erstellt und es werden die folgenden Statusinformationen zurückgegeben:

```
{  
  "task": {  
    "status": "IMPORT_IN_PROGRESS",  
    "applicationImportSuccess": 0,  
    "serverImportFailure": 0,  
    "serverImportSuccess": 0,  
    "name": "ImportName",  
    "importRequestTime": 1547682819.801,  
    "applicationImportFailure": 0,  
    "clientRequestToken": "EXAMPLE1-abcd-1234-abcd-EXAMPLE1234",  
    "importUrl": "s3://BucketName/ImportFile.csv",  
    "importTaskId": "import-task-EXAMPLE1229949eabfEXAMPLE03862c0"  
  }  
}
```

Nachverfolgung Ihrer Migration Hub Hub-Importanfragen

Sie können den Status Ihrer Migration Hub Hub-Importanfragen über die Konsole oder eine der folgenden Optionen verfolgen AWS SDKs. AWS CLI

Console Tracking

Im Import-Dashboard in der Migration Hub Hub-Konsole finden Sie die folgenden Elemente.

- Name — Der Name der Importanfrage.
- Import-ID — Die eindeutige ID der Importanfrage.
- Importzeit — Datum und Uhrzeit der Erstellung der Importanforderung.
- Importstatus — Der Status der Importanfrage. Dabei kann es sich um einen der folgenden Werte handeln:
 - Import — Diese Datendatei wird gerade importiert.
 - Importiert — Die gesamte Datendatei wurde erfolgreich importiert.
 - Fehlerhaft importiert — Ein oder mehrere Datensätze in der Datendatei konnten nicht importiert werden. Wählen Sie zum Umgang mit fehlgeschlagenen Datensätzen `Download failed records` (Fehlgeschlagene Datensätze herunterladen) für Ihre Importaufgabe, und beheben Sie die Fehler in der .csv-Datei mit fehlgeschlagenen Einträgen. Wiederholen Sie dann den Import.
 - Import fehlgeschlagen — Keiner der Datensätze in der Datendatei wurde importiert. Wählen Sie zum Umgang mit fehlgeschlagenen Datensätzen `Download failed records` (Fehlgeschlagene Datensätze herunterladen) für Ihre Importaufgabe, und beheben Sie die Fehler in der .csv-Datei mit fehlgeschlagenen Einträgen. Wiederholen Sie dann den Import.
- Importierte Datensätze — Die Anzahl der Datensätze in einer bestimmten Datendatei, die erfolgreich importiert wurden.
- Fehlgeschlagene Datensätze — Die Anzahl Datensätze in einer bestimmten Datendatei, die nicht importiert wurden.

CLI Tracking

Sie können den Status Ihrer Importaufgaben mit dem `aws discovery describe-import-tasks` AWS CLI Befehl verfolgen.

1. Öffnen Sie ein Terminalfenster, und geben Sie den folgenden Befehl ein:

```
aws discovery describe-import-tasks
```

2. Dadurch wird eine Liste aller Importaufgaben im JSON-Format zurückgegeben, vollständig mit Status- und weiteren relevanten Informationen. Optional können Sie die Ergebnisse filtern, um eine Teilmenge Ihrer Importaufgaben auszugeben.

Bei der Nachverfolgung Ihrer Importaufgaben kann es vorkommen, dass der ausgegebene `serverImportFailure`-Wert größer als Null ist. Wenn dies der Fall ist, enthielt Ihre Importdatei einen oder mehrere Einträge, die nicht importiert werden konnten. Sie können dies beheben, indem Sie Ihr Archiv fehlgeschlagener Datensätze herunterladen, die darin befindlichen Dateien überprüfen und mit der modifizierten Datei `failed-entries.csv` eine weitere Importanfrage erstellen.

Nach dem Erstellen der Importaufgabe können Sie weitere Aktionen durchführen, um Ihre Datenmigration zu unterstützen und nachzuverfolgen. Sie können beispielsweise ein Archiv fehlgeschlagener Datensätze für eine bestimmte Anfrage herunterladen. Informationen zur Verwendung des Archivs fehlgeschlagener Datensätze für die Behebung von Importproblemen, finden Sie unter [Fehlerbehebung bei fehlgeschlagenen Datensätzen](#).

Entdeckte Daten anzeigen und untersuchen

Sowohl Application Discovery Service Agentless Collector (Agentless Collector) als auch AWS Discovery Agent (Discovery Agent) liefern Systemleistungsdaten, die auf durchschnittlicher Auslastung und Spitzenauslastung basieren. Sie können die gesammelten Systemleistungsdaten verwenden, um die Gesamtbetriebskosten (TCO) auf hohem Niveau zu ermitteln. Discovery Agents sammeln detailliertere Daten, darunter Zeitreihendaten für Systemleistungsinformationen, eingehende und ausgehende Netzwerkverbindungen und Prozesse, die auf dem Server ausgeführt werden. Sie können mithilfe dieser Daten die Netzwerkabhängigkeiten zwischen Servern besser verstehen und die zugehörigen Server für die Migrationsplanung als Anwendungen gruppieren.

In diesem Abschnitt finden Sie Anweisungen zum Anzeigen und Bearbeiten von Daten, die von Agentless Collector und Discovery Agent sowohl von der Konsole als auch von der Konsole aus entdeckt wurden. AWS CLI

Themen

- [Gesammelte Daten mit der Migration Hub Hub-Konsole anzeigen](#)
- [Erkunden von Daten in Amazon Athena](#)

Gesammelte Daten mit der Migration Hub Hub-Konsole anzeigen

Sowohl für den Application Discovery Service Agentless Collector (Agentless Collector) als auch für den AWS Discovery Agent (Discovery Agent) können Sie nach dem Start des Datenerfassungsprozesses die Konsole verwenden, um deren gesammelte Daten über Ihre Server und VMs. Die Daten werden etwa 15 Minuten nach Beginn der Datenerfassung in der Konsole angezeigt. Sie können diese Daten auch im CSV-Format anzeigen, indem Sie die gesammelten Daten exportieren, indem Sie API-Aufrufe mit dem tätigen AWS CLI.

Um die gesammelten Daten zu erkannten Servern in der Konsole anzuzeigen, folgen Sie den Schritten unter [Server in der Konsole anzeigen AWS Migration Hub](#). Weitere Informationen zur Verwendung der Konsole zum Anzeigen, Sortieren und Markieren von Servern, die von Ihren Agentless Collectors oder Discovery Agents entdeckt wurden, finden Sie unter [Daten mit der AWS Migration Hub Konsole ermitteln](#).

Das Agentless Collector Datenbank- und Analysedatenerfassungsmodul lädt die gesammelten Daten in den Amazon S3 S3-Bucket hoch. Sie können die Daten aus diesem Bucket in der AWS

DMS-Konsole einsehen. Um die gesammelten Daten zu erkannten Datenbank- und Analyseservern einzusehen, folgen Sie den Schritten unter [Ihre gesammelten Daten anzeigen](#).

Abgleichslogik für entdeckte Server und Anwendungen

AWS Application Discovery Service (Application Discovery Service) verfügt über eine integrierte Abgleichslogik, die erkennt, wenn entdeckte Server mit vorhandenen Einträgen übereinstimmen. Wenn diese Logik eine Übereinstimmung findet, werden die Informationen für den bereits vorhandenen erkannten Server mit den neuen Werten aktualisiert.

Diese Abgleichslogik verarbeitet doppelte Server aus mehreren Quellen, darunter AWS Migration Hub (Migration Hub) -Import, Application Discovery Service Agentless Collector (Agentless Collector), AWS Application Discovery Agent (Discovery Agent) und andere Migrationstools. Weitere Informationen zum Migration Hub Hub-Import finden Sie unter [Migration Hub Hub-Import](#).

Wenn ein Server erkannt wird, wird jeder Eintrag anhand vorher importierter Datensätze geprüft, um sicherzustellen, dass der importierte Server nicht bereits vorhanden ist. Wenn keine Übereinstimmung gefunden wird, wird ein neuer Datensatz erstellt und eine neue eindeutige Server-ID zugewiesen. Wenn eine Übereinstimmung gefunden wird, wird ebenfalls ein neuer Eintrag erstellt, diesem wird jedoch dieselbe eindeutige Server-ID zugewiesen wie dem vorhandenen Server. Wenn Sie diesen Server in der Migration Hub Hub-Konsole anzeigen, finden Sie nur einen eindeutigen Eintrag für den Server.

Server-Attribute für diesen Eintrag werden zusammengeführt, um Attributwerte von einem vorher verfügbaren Datensatz und von dem neu importierten Datensatz anzuzeigen. Wenn mehr als ein Wert für ein Serverattribut aus mehreren Quellen vorliegt, etwa zwei unterschiedliche Werte für Total RAM zu einem Server, der mittels Import und vom Discovery Agent erkannt wurde, wird der neueste aktualisierte Wert in dem abgeglichenen Datensatz für den Server gezeigt.

Übereinstimmende Felder

Die folgenden Felder werden bei der Verwendung von Erkennungstools für den Abgleich von Servern verwendet.

- **ExternalId**— Dies ist das primäre Feld, das für die Zuordnung von Servern verwendet wird. Wenn der Wert in diesem Feld mit einem anderen Wert `ExternalId` in einem anderen Eintrag identisch ist, gleicht Application Discovery Service die beiden Einträge ab, unabhängig davon, ob die anderen Felder übereinstimmen oder nicht.
- **IPAddress**

- **HostName**
- **MacAddress**
- **VMware. MoRefId** und **VMware. vCenterId** — Beide Werte müssen mit den entsprechenden Feldern in einem anderen Eintrag identisch sein, damit Application Discovery Service eine Übereinstimmung durchführt.

Erkunden von Daten in Amazon Athena

Die Datenexploration in Amazon Athena ermöglicht es Ihnen, die Daten, die von allen erkannten lokalen Servern von Discovery Agent gesammelt wurden, an einem Ort zu analysieren. Sobald die Datenexploration in Amazon Athena über die Migration Hub Hub-Konsole (oder mithilfe der StartContinuousExport API) aktiviert und die Datenerfassung für Agenten aktiviert ist, werden die von Agenten gesammelten Daten automatisch in regelmäßigen Abständen in Ihrem S3-Bucket gespeichert. Weitere Informationen finden Sie unter [Erkunden von Daten in Amazon Athena](#).

Die Datenexploration in Amazon Athena ermöglicht es Ihnen, die Daten, die von allen erkannten lokalen Servern von Discovery Agents gesammelt wurden, an einem Ort zu analysieren. Sobald die Datenexploration in Amazon Athena über die Migration Hub Hub-Konsole (oder mithilfe der StartContinuousExport API) aktiviert und die Datenerfassung für Agenten aktiviert ist, werden die von Agenten gesammelten Daten automatisch in regelmäßigen Abständen in Ihrem S3-Bucket gespeichert.

Anschließend können Sie Amazon Athena aufrufen, um vordefinierte Abfragen auszuführen, um die Zeitreihen-Systemleistung für jeden Server, die Art der Prozesse, die auf jedem Server ausgeführt werden, und die Netzwerkabhängigkeiten zwischen verschiedenen Servern zu analysieren. Darüber hinaus können Sie mit Amazon Athena Ihre eigenen benutzerdefinierten Abfragen schreiben, zusätzliche vorhandene Datenquellen wie Configuration Management Database (CMDB) -Exporte hochladen und die erkannten Server den eigentlichen Geschäftsanwendungen zuordnen. Sie können die Athena-Datenbank auch in Amazon Quick integrieren, um die Abfrageergebnisse zu visualisieren und zusätzliche Analysen durchzuführen.

In den Themen dieses Abschnitts wird beschrieben, wie Sie mit Ihren Daten in Athena arbeiten können, um die Migration Ihrer lokalen Umgebung zu beurteilen und zu planen. AWS

Datenexploration in Amazon Athena aktivieren

Die Datenexploration in Amazon Athena wird aktiviert, indem Sie Continuous Export über die Migration Hub Hub-Konsole oder einen API-Aufruf von aktivieren. AWS CLI Sie müssen die

Datenexploration aktivieren, bevor Sie Ihre erkannten Daten in Amazon Athena sehen und mit der Erkundung beginnen können.

Wenn Sie Continuous Export aktivieren, `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` wird die mit dem Service verknüpfte Rolle automatisch von Ihrem Konto verwendet. Weitere Informationen zu dieser serviceverknüpften Rolle finden Sie unter [Dienstbezogene Rollenberechtigungen für Application Discovery Service](#).

Die folgenden Anweisungen zeigen, wie Sie die Datenexploration in Amazon Athena mithilfe der Konsole und der AWS CLI aktivieren.

Turn on with the console

Die Datenexploration in Amazon Athena wird dadurch aktiviert, dass Continuous Export implizit aktiviert wird, wenn Sie „Datenerfassung starten“ wählen oder auf der Seite „Datensammler“ der Migration Hub Hub-Konsole auf den Schalter „Datenexploration in Amazon Athena“ klicken.

So aktivieren Sie die Datenexploration in Amazon Athena von der Konsole aus

1. Klicken Sie im Navigationsbereich auf Data Collectors (Datensammler).
2. Wählen Sie die Registerkarte Agents (Agenten).
3. Wählen Sie Datenerfassung starten aus, oder wenn Sie die Datenerfassung bereits aktiviert haben, klicken Sie auf den Schalter Datenexploration in Amazon Athena.
4. Klicken Sie in dem im vorherigen Schritt erstellten Dialogfeld auf das Kontrollkästchen, um sich mit den anfallenden Gebühren einverstanden zu erklären. Klicken Sie dann auf Continue (Fortfahren) oder Enable (Aktivieren).

Note

Ihre Agenten laufen jetzt im Modus „Kontinuierlicher Export“, sodass Sie Ihre erkannten Daten in Amazon Athena sehen und damit arbeiten können. Bei der ersten Aktivierung kann es bis zu 30 Minuten dauern, bis Ihre Daten in Amazon Athena angezeigt werden.

Enable with the AWS CLI

Die Datenexploration in Amazon Athena wird ermöglicht, indem Continuous Export explizit über einen API-Aufruf von aktiviert wird. AWS CLI Dazu AWS CLI muss der zunächst in Ihrer Umgebung installiert werden.

Um die Datenexploration in Amazon Athena zu installieren AWS CLI und zu aktivieren

1. Installieren Sie das AWS CLI für Ihr Betriebssystem (Linux, macOS oder Windows). Anweisungen finden Sie im [AWS Command Line Interface Benutzerhandbuch](#).
2. Öffnen Sie die Eingabeaufforderung (Windows) oder das Terminal (Linux oder macOS).
 - a. Geben Sie `aws configure` ein und drücken Sie die Eingabetaste.
 - b. Geben Sie Ihre AWS Zugangsschlüssel-ID und Ihren AWS geheimen Zugriffsschlüssel ein.
 - c. Geben Sie als standardmäßigen Regionsnamen `us-west-2` ein.
 - d. Geben Sie als Standard-Ausgabeformat `text` ein.
3. Geben Sie den folgenden Befehl ein:

```
aws discovery start-continuous-export
```

Note

Ihre Agenten laufen jetzt im Modus „Kontinuierlicher Export“, sodass Sie Ihre erkannten Daten in Amazon Athena sehen und damit arbeiten können. Bei der ersten Aktivierung kann es bis zu 30 Minuten dauern, bis Ihre Daten in Amazon Athena angezeigt werden.

Daten direkt in Amazon Athena untersuchen

Nachdem Sie die Datenexploration in Amazon Athena aktiviert haben, können Sie mit der Erkundung und Bearbeitung detaillierter aktueller Daten beginnen, die von Ihren Agenten entdeckt wurden, indem Sie die Daten direkt in Athena abfragen. Sie können die Daten verwenden, um Tabellen zu generieren, eine Kostenanalyse auszuführen, die Abfrage zum Erstellen eines Diagramms der Netzwerkabhängigkeiten auf ein Visualisierungsprogramm portieren und vieles mehr.

In den folgenden Anweisungen wird erklärt, wie Sie Ihre Agentendaten direkt in der Athena-Konsole untersuchen können. Wenn Sie keine Daten in Athena haben oder die Datenexploration in Amazon Athena nicht aktiviert haben, werden Sie in einem Dialogfeld aufgefordert, die Datenexploration in Amazon Athena zu aktivieren, wie unter erklärt. [Datenexploration in Amazon Athena aktivieren](#)

Um von Agenten entdeckte Daten direkt in Athena zu untersuchen

1. Wählen Sie in der AWS Migration Hub Konsole im Navigationsbereich Server aus.
2. Um die Amazon Athena-Konsole zu öffnen, wählen Sie Explore data in Amazon Athena.
3. Prüfen Sie auf der Seite Query Editor (Abfrage-Editor) im Navigationsbereich unter Database (Datenbank), ob `application_discovery_service_database` ausgewählt ist.

 Note

In Tables (Tabellen) stellen die folgenden Tabellen die nach Agenten gruppierten Datensätze dar.

- `os_info_agent`
- `network_interface_agent`
- `sys_performance_agent`
- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

4. Fragen Sie die Daten in der Amazon Athena Athena-Konsole ab, indem Sie SQL-Abfragen im Athena-Abfrage-Editor schreiben und ausführen. Beispielsweise können Sie die folgende Abfrage verwenden, um alle erkannten Server-IP-Adressen anzuzeigen.

```
SELECT * FROM network_interface_agent;
```

Weitere Beispiele für Abfragen finden Sie unter [Verwenden vordefinierter Abfragen in Amazon Athena](#).

Visualisierung von Amazon Athena Athena-Daten

Um Ihre Daten zu visualisieren, kann eine Abfrage in ein Visualisierungsprogramm wie Amazon Quick oder andere Open-Source-Visualisierungstools wie Cytoscape, yEd oder Gephi portiert werden. Verwenden Sie diese Tools zum Rendern von Netzwerkdiagrammen, zusammenfassenden Diagrammen und anderen grafischen Darstellungen. Wenn diese Methode verwendet wird, stellen Sie über das Visualisierungsprogramm eine Verbindung zu Athena her, sodass es auf Ihre gesammelten Daten als Quelle für die Erstellung der Visualisierung zugreifen kann.

So visualisieren Sie Ihre Amazon Athena Athena-Daten mit Quick

1. Melden Sie sich bei [Amazon Quick](#) an.
2. Wählen Sie Connect to another data source or upload a file (Mit einer anderen Datenquelle verbinden oder eine Datei hochladen).
3. Wähle Athena. Das Dialogfeld Neue Athena-Datenquelle wird angezeigt.
4. Geben Sie einen Namen in das Feld Data source name (Datenquellennamen) ein.
5. Klicken Sie auf Create data source.
6. Wählen Sie im Dialogfeld „gents-servers-osTabelle auswählen“ die Tabelle A aus und wählen Sie „Auswählen“.
7. Wählen Sie im Dialogfeld Finish data set creation (Datensatzerstellung fertigstellen) die Option Import to SPICE for quicker analytics (Für schnellere Analysen in SPICE importieren) aus. Wählen Sie anschließend Visualize (Visualisieren) aus.

Ihre Visualisierung wird gerendert.

Verwenden vordefinierter Abfragen in Amazon Athena

Dieser Abschnitt enthält eine Reihe von vordefinierten Abfragen, die typische Anwendungsfälle wie die Analyse der Gesamtbetriebskosten und die Netzwerk-Visualisierung ausführen. Sie können diese Abfragen unverändert verwenden oder sie Ihren Anforderungen entsprechend anpassen.

So verwenden Sie eine vordefinierte Abfrage

1. Wählen Sie in der AWS Migration Hub Konsole im Navigationsbereich Server aus.
2. Um die Amazon Athena-Konsole zu öffnen, wählen Sie Explore data in Amazon Athena.

3. Prüfen Sie auf der Seite Query Editor (Abfrage-Editor) im Navigationsbereich unter Database (Datenbank), ob `application_discovery_service_database` ausgewählt ist.
4. Wählen Sie das Pluszeichen (+) im Abfrage-Editor aus, um eine Registerkarte für eine neue Abfrage zu erstellen.
5. Kopieren Sie eine der Abfragen aus [Vordefinierte Abfragen](#).
6. Fügen Sie die Abfrage in den Abfragebereich der neuen Abfrage-Registerkarte ein, die Sie gerade erstellt haben.
7. Klicken Sie auf Run Query (Abfrage ausführen).

Vordefinierte Abfragen

Wählen Sie einen Titel aus, um Informationen über die Abfrage anzuzeigen.

Besorgen Sie sich IP-Adressen und Hostnamen für Server

Diese Ansichts-Hilfsfunktion ruft die IP-Adressen und Hostnamen für einen bestimmten Server ab. Sie können diese Ansicht bei anderen Abfragen verwenden. Informationen zum Erstellen einer Ansicht finden Sie unter [CREATE VIEW](#) im Amazon Athena Athena-Benutzerhandbuch.

```
CREATE OR REPLACE VIEW hostname_ip_helper AS
SELECT DISTINCT
  "os"."host_name"
, "nic"."agent_id"
, "nic"."ip_address"
FROM
  os_info_agent os
, network_interface_agent nic
WHERE ("os"."agent_id" = "nic"."agent_id");
```

Identifizieren Sie Server mit oder ohne Agenten

Diese Abfrage kann bei der Datenvalidierung helfen. Wenn Sie auf einer Reihe von Servern in Ihrem Netzwerk Agenten bereitgestellt haben, können Sie diese Abfrage verwenden, um zu erfahren, ob es weitere Server in Ihrem Netzwerk ohne Agenten gibt. In dieser Abfrage wird der ein- und ausgehende Netzwerkdatenverkehr untersucht und der Datenverkehr ausschließlich nach privaten IP-Adressen gefiltert. Dies sind IP-Adressen, die mit 192, 10 oder 172 beginnen.

```
SELECT DISTINCT "destination_ip" "IP Address" ,
```

```

        (CASE
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "destination_ip") ) = 0) THEN
            'no'
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "destination_ip") ) > 0) THEN
            'yes' END) "agent_running"
        FROM outbound_connection_agent
        WHERE (((("destination_ip" LIKE '192.%')
        OR ("destination_ip" LIKE '10.%'))
        OR ("destination_ip" LIKE '172.%'))
        UNION
        SELECT DISTINCT "source_ip" "IP ADDRESS" ,
        (CASE
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "source_ip") ) = 0) THEN
            'no'
        WHEN (
        (SELECT "count"(*)
        FROM network_interface_agent
        WHERE ("ip_address" = "source_ip") ) > 0) THEN
            'yes' END) "agent_running"
        FROM inbound_connection_agent
        WHERE (((("source_ip" LIKE '192.%')
        OR ("source_ip" LIKE '10.%'))
        OR ("source_ip" LIKE '172.%')));

```

Analysieren Sie die Systemleistungsdaten für Server mit Agenten

Mit dieser Abfrage können Sie die Systemleistung und Nutzungsmusterdaten für Ihre lokalen Server mit installierten Agenten analysieren. Die Abfrage kombiniert die Tabellen `system_performance_agent` und `os_info_agent`, um den Hostnamen für die einzelnen Server zu identifizieren. Diese Abfrage gibt die Zeitreihen-Nutzungsdaten (in 15-Minuten-Intervallen) für alle Server zurück, auf denen Agenten ausgeführt werden.

```

SELECT "OS"."os_name" "OS Name" ,
       "OS"."os_version" "OS Version" ,

```

```

"OS"."host_name" "Host Name" ,
"SP"."agent_id" ,
"SP"."total_num_cores" "Number of Cores" ,
"SP"."total_num_cpus" "Number of CPU" ,
"SP"."total_cpu_usage_pct" "CPU Percentage" ,
"SP"."total_disk_size_in_gb" "Total Storage (GB)" ,
"SP"."total_disk_free_size_in_gb" "Free Storage (GB)" ,
("SP"."total_disk_size_in_gb" - "SP"."total_disk_free_size_in_gb") "Used
Storage" ,
"SP"."total_ram_in_mb" "Total RAM (MB)" ,
("SP"."total_ram_in_mb" - "SP"."free_ram_in_mb") "Used RAM (MB)" ,
"SP"."free_ram_in_mb" "Free RAM (MB)" ,
"SP"."total_disk_read_ops_per_sec" "Disk Read IOPS" ,
"SP"."total_disk_bytes_written_per_sec_in_kbps" "Disk Write IOPS" ,
"SP"."total_network_bytes_read_per_sec_in_kbps" "Network Reads (kbps)" ,
"SP"."total_network_bytes_written_per_sec_in_kbps" "Network Write (kbps)"
FROM "sys_performance_agent" "SP" , "OS_INFO_agent" "OS"
WHERE ("SP"."agent_id" = "OS"."agent_id") limit 10;

```

Verfolgen Sie die ausgehende Kommunikation zwischen Servern anhand der Portnummer und der Prozessdetails

Über diese Abfrage werden die Details zum ausgehenden Datenverkehr für jeden Dienst abgerufen, zusammen mit der Portnummer und den Prozessdetails.

Bevor Sie die Abfrage ausführen, müssen Sie, falls noch nicht geschehen, die `iana_service_ports_import`-Tabelle erstellen, die die von der IANA heruntergeladene Datenbank des IANA-Portregisters enthält. Weitere Informationen zum Erstellen dieser Tabelle finden Sie unter [Die Importtabelle für die IANA-Portregistrierung wird erstellt](#).

Nach der Erstellung der Tabelle `iana_service_ports_import` erstellen Sie zwei Ansichtshilfsfunktionen zur Verfolgung des ausgehenden Datenverkehrs. Informationen zum Erstellen einer Ansicht finden Sie unter [CREATE VIEW](#) im Amazon Athena Athena-Benutzerhandbuch.

So erstellen Sie Hilfsfunktionen für die Nachverfolgung des ausgehenden Datenverkehrs

1. Öffnen Sie die Athena-Konsole unter <https://console.aws.amazon.com/athena/>.
2. Erstellen Sie die `valid_outbound_ips_helper` Ansicht mithilfe der folgenden Hilfsfunktion, die alle unterschiedlichen ausgehenden Ziel-IP-Adressen auflistet.

```
CREATE OR REPLACE VIEW valid_outbound_ips_helper AS
```



```
SELECT DISTINCT "destination_ip"
FROM outbound_connection_agent;
```

3. Erstellen Sie die Ansicht `outbound_query_helper` über die folgende Hilfsfunktion, die die Häufigkeit der Kommunikation für den ausgehenden Datenverkehr ermittelt.

```
CREATE OR REPLACE VIEW outbound_query_helper AS
SELECT "agent_id" ,
       "source_ip" ,
       "destination_ip" ,
       "destination_port" ,
       "agent_assigned_process_id" ,
       "count(*) "frequency"
FROM outbound_connection_agent
WHERE (("ip_version" = 'IPv4')
      AND ("destination_ip" IN
          (SELECT *
           FROM valid_outbound_ips_helper )))
GROUP BY "agent_id", "source_ip", "destination_ip", "destination_port",
         "agent_assigned_process_id";
```

4. Nachdem Sie die `iana_service_ports_import`-Tabelle und Ihre zwei Hilfsfunktionen erstellt haben, können Sie die folgende Abfrage ausführen, um die Details zum ausgehenden Datenverkehr für die jeweiligen Dienste in Verbindung mit der Portnummer und den Prozessdetails abzurufen.

```
SELECT hip1.host_name "Source Host Name",
       outbound_connections_results0.source_ip "Source IP Address",
       hip2.host_name "Destination Host Name",
       outbound_connections_results0.destination_ip "Destination IP Address",
       outbound_connections_results0.frequency "Connection Frequency",
       outbound_connections_results0.destination_port "Destination Communication
Port",
       outbound_connections_results0.servicename "Process Service Name",
       outbound_connections_results0.description "Process Service Description"
FROM
  (SELECT DISTINCT o.source_ip,
                  o.destination_ip,
                  o.frequency,
                  o.destination_port,
                  ianap.servicename,
                  ianap.description
   FROM outbound_query_helper o, iana_service_ports_import ianap
```

```

WHERE o.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
outbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
  ON outbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
  ON outbound_connections_results0.destination_ip = hip2.ip_address

```

Verfolgen Sie die eingehende Kommunikation zwischen Servern anhand der Portnummer und der Prozessdetails

Über diese Abfrage werden die Informationen über den ausgehenden Datenverkehr für jeden Dienst abgerufen, zusammen mit der Portnummer und den Prozessdetails.

Bevor Sie diese Abfrage ausführen, müssen Sie, falls noch nicht geschehen, die `iana_service_ports_import`-Tabelle erstellen, die die von der IANA heruntergeladene Datenbank des IANA-Portregisters enthält. Weitere Informationen zum Erstellen dieser Tabelle finden Sie unter [Die Importtabelle für die IANA-Portregistrierung wird erstellt](#).

Nach der Erstellung der Tabelle `iana_service_ports_import` erstellen Sie zwei Ansichtshilfsfunktionen zur Verfolgung des eingehenden Datenverkehrs. Informationen zum Erstellen einer Ansicht finden Sie unter [CREATE VIEW](#) im Amazon Athena Athena-Benutzerhandbuch.

So erstellen Sie Hilfsfunktionen für die Nachverfolgung des Imports

1. Öffnen Sie die Athena-Konsole unter <https://console.aws.amazon.com/athena/>.
2. Erstellen Sie die Ansicht `valid_inbound_ips_helper` über die folgende Hilfsfunktion, die alle unterschiedlichen IP-Quelladressen für den eingehenden Datenverkehr auflistet.

```

CREATE OR REPLACE VIEW valid_inbound_ips_helper AS
SELECT DISTINCT "source_ip"
FROM inbound_connection_agent;

```

3. Erstellen Sie die Ansicht `inbound_query_helper` über die folgende Hilfsfunktion, die die Häufigkeit der Kommunikation für den eingehenden Datenverkehr ermittelt.

```

CREATE OR REPLACE VIEW inbound_query_helper AS
SELECT "agent_id" ,
       "source_ip" ,
       "destination_ip" ,
       "destination_port" ,

```

```

        "agent_assigned_process_id" ,
        "count"(*) "frequency"
FROM inbound_connection_agent
WHERE (("ip_version" = 'IPv4')
        AND ("source_ip" IN
            (SELECT *
             FROM valid_inbound_ips_helper )))
GROUP BY "agent_id", "source_ip", "destination_ip", "destination_port",
        "agent_assigned_process_id";

```

4. Nachdem Sie die `iana_service_ports_import`-Tabelle und Ihre zwei Hilfsfunktionen erstellt haben, können Sie die folgende Abfrage ausführen, um die Details zum eingehenden Datenverkehr für die jeweiligen Dienste in Verbindung mit der Portnummer und den Prozessdetails abzurufen.

```

SELECT hip1.host_name "Source Host Name",
       inbound_connections_results0.source_ip "Source IP Address",
       hip2.host_name "Destination Host Name",
       inbound_connections_results0.destination_ip "Destination IP Address",
       inbound_connections_results0.frequency "Connection Frequency",
       inbound_connections_results0.destination_port "Destination Communication
Port",
       inbound_connections_results0.servicename "Process Service Name",
       inbound_connections_results0.description "Process Service Description"
FROM
    (SELECT DISTINCT i.source_ip,
                     i.destination_ip,
                     i.frequency,
                     i.destination_port,
                     ianap.servicename,
                     ianap.description
     FROM inbound_query_helper i, iana_service_ports_import ianap
     WHERE i.destination_port = TRY_CAST(ianap.portnumber AS integer)) AS
inbound_connections_results0 LEFT OUTER
JOIN hostname_ip_helper hip1
    ON inbound_connections_results0.source_ip = hip1.ip_address LEFT OUTER
JOIN hostname_ip_helper hip2
    ON inbound_connections_results0.destination_ip = hip2.ip_address

```

Identifizieren Sie die laufende Software anhand der Portnummer

Mit dieser Abfrage wird die ausgeführte Software basierend auf den Portnummern identifiziert.

Bevor Sie diese Abfrage ausführen, müssen Sie, falls noch nicht geschehen, die `iana_service_ports_import`-Tabelle erstellen, die die von der IANA heruntergeladene Datenbank des IANA-Portregisters enthält. Weitere Informationen zum Erstellen dieser Tabelle finden Sie unter [Die Importtabelle für die IANA-Portregistrierung wird erstellt](#).

Mit der folgenden Abfrage können Sie die ausgeführte Software basierend auf Portnummern identifizieren.

```
SELECT o.host_name "Host Name",
       ianap.servicename "Service",
       ianap.description "Description",
       con.destination_port,
       con.cnt_dest_port "Destination Port Count"
FROM   (SELECT agent_id,
               destination_ip,
               destination_port,
               Count(destination_port) cnt_dest_port
        FROM   inbound_connection_agent
        GROUP  BY agent_id,
                  destination_ip,
                  destination_port) con,
       (SELECT agent_id,
               host_name,
               Max("timestamp")
        FROM   os_info_agent
        GROUP  BY agent_id,
                  host_name) o,
       iana_service_ports_import ianap
WHERE  ianap.transportprotocol = 'tcp'
       AND con.destination_ip NOT LIKE '172%'
       AND con.destination_port = ianap.portnumber
       AND con.agent_id = o.agent_id
ORDER BY cnt_dest_port DESC;
```

Die Importtabelle für die IANA-Portregistrierung wird erstellt

Für einige der vordefinierten Abfragen ist eine Tabelle namens `iana_service_ports_import` erforderlich, die von der IANA (Internet Assigned Numbers Authority) heruntergeladene Informationen enthält.

So erstellen Sie die iana_service_ports_import-Tabelle

1. Laden Sie die IANA Portregister-Datenbank-CSV-Datei vom [Service Name and Transport Protocol Port Number Registry](#) auf iana.org herunter.
2. Laden Sie die Datei auf Amazon S3 hoch. Weitere Informationen finden Sie unter [Wie lade ich Dateien und Ordner in einen S3-Bucket hoch?](#).
3. Erstellen Sie in Athena eine neue Tabelle mit dem Namen `iana_service_ports_import`. Anweisungen finden Sie unter [Tabelle erstellen](#) im Amazon Athena Benutzerhandbuch. Im folgenden Beispiel müssen Sie `my_bucket_name` durch den Namen des S3-Buckets ersetzen, in den Sie die CSV-Datei im vorherigen Schritt hochgeladen haben.

```
CREATE EXTERNAL TABLE IF NOT EXISTS iana_service_ports_import (  
    ServiceName STRING,  
    PortNumber INT,  
    TransportProtocol STRING,  
    Description STRING,  
    Assignee STRING,  
    Contact STRING,  
    RegistrationDate STRING,  
    ModificationDate STRING,  
    Reference STRING,  
    ServiceCode STRING,  
    UnauthorizedUseReported STRING,  
    AssignmentNotes STRING  
)  
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe'  
WITH SERDEPROPERTIES (  
    'serialization.format' = ',',  
    'quoteChar' = '"',  
    'field.delim' = ','  
) LOCATION 's3://my_bucket_name/'  
TBLPROPERTIES ('has_encrypted_data'='false','skip.header.line.count'='1');
```

Daten mit der AWS Migration Hub Konsole ermitteln

AWS Application Discovery Service (Application Discovery Service) ist in AWS Migration Hub (Migration Hub) integriert, und Kunden können ihre Datensammler, Server und Anwendungen in Migration Hub einsehen und verwalten. Wenn Sie die Application Discovery Service Service-Konsole verwenden, werden Sie zur Migration Hub Hub-Konsole weitergeleitet. Für die Arbeit mit der Migration Hub Hub-Konsole sind keine zusätzlichen Schritte oder Einstellungen Ihrerseits erforderlich.

In diesem Abschnitt erfahren Sie, wie Sie Application Discovery Service Agentless Collector (Agentless Collector) und AWS Application Discovery Agent (Discovery Agent) mithilfe der Konsole verwalten und überwachen.

Themen

- [Daten im Konsolen-Dashboard anzeigen AWS Migration Hub](#)
- [Datensammler in der AWS Migration Hub Konsole starten und stoppen](#)
- [Datensammelpunkte in der AWS Migration Hub Konsole sortieren](#)
- [Server in der Konsole anzeigen AWS Migration Hub](#)
- [Server in der AWS Migration Hub Konsole sortieren](#)
- [Kennzeichnen von Servern in der Konsole AWS Migration Hub](#)
- [Wird AWS Migration Hub zum Exportieren von Serverdaten verwendet](#)
- [Gruppierung von Servern in der Konsole AWS Migration Hub](#)

Daten im Konsolen-Dashboard anzeigen AWS Migration Hub

Um das Haupt-Dashboard anzuzeigen, wählen Sie im Navigationsbereich der Konsole AWS Migration Hub (Migration Hub) die Option Dashboard aus. Im Haupt-Dashboard von Migration Hub können Sie allgemeine Statistiken zu Servern, Anwendungen und Datensammelpunkten wie Application Discovery Service Agentless Collector (Agentless Collector) und AWS Application Discovery Agent (Discovery Agent) einsehen.

Das Haupt-Dashboard sammelt Daten aus den Dashboards Discover (Erkennen) und Migrate (Migrieren) an einem zentralen Ort. Es verfügt über vier Status- und Informationsbereiche und eine Liste von Links, um schnellen Zugriff zu ermöglichen. Über die Bereiche erhalten Sie eine Zusammenfassung des Status Ihres zuletzt aktualisierten Anwendungen. Außerdem können

Sie schnell auf jede Ihrer Anwendungen zugreifen, einen Überblick über Anwendungen mit unterschiedlichem Status erhalten und den Fortschritt der Migration im Laufe der Zeit verfolgen.

Um das Haupt-Dashboard anzuzeigen, wählen Sie im Navigationsbereich, der sich auf der linken Seite der Startseite der Migration Hub Hub-Konsole befindet, die Option Dashboard aus.

Datensammler in der AWS Migration Hub Konsole starten und stoppen

Application Discovery Service Agentless Collector (Agentless Collector) und AWS Application Discovery Agent (Discovery Agent) sind die Datenerfassungstools, mit denen AWS Application Discovery Service (Application Discovery Service) Ihnen hilft, Ihre bestehende Infrastruktur zu ermitteln. In den folgenden Schritten wird erklärt, wie Sie diese Tools zur Erfassung von Discovery-Daten herunterladen und bereitstellen, [Stellen Sie Agentless Collector bereit](#) und [AWS Agent zur Anwendungserkennung](#)

Diese Datenerfassungstools speichern ihre Daten im Repository des Application Discovery Service und bieten Informationen zu jedem Server und den darauf ausgeführten Prozessen. Wenn eines dieser Tools bereitgestellt wird, können Sie die gesammelten Daten über die Konsole AWS Migration Hub (Migration Hub) starten, beenden und anzeigen.

Nachdem der AWS Application Discovery Agent (Discovery Agent) bereitgestellt wurde, können Sie den Datenerfassungsprozess auf der Seite Data Collectors der Konsole AWS Migration Hub (Migration Hub) starten oder beenden.

So starten oder beenden Sie die Tools zur Datensammlung

1. Melden Sie sich mit Ihrem AWS Konto bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole unter Discover die Option Datensammler aus.
3. Wählen Sie die Registerkarte Agents (Agenten).
4. Aktivieren Sie das Kontrollkästchen des Sammlungstools, das Sie starten oder beenden möchten.
5. Wählen Sie Start data collection (Beginnen der Datensammlung) oder Stop data collection (Beenden der Datensammlung).

Datensammelpunkte in der AWS Migration Hub Konsole sortieren

Wenn Sie viele Datensammelpunkte bereitgestellt haben, können Sie die angezeigte Liste der bereitgestellten Datensammler auf der Seite Datensammler der Konsole sortieren. Sie sortieren die Liste, indem Sie Filter in der Suchleiste anwenden. Sie können die meisten in der Liste Data Collectors (Datensammler) angegebenen Kriterien suchen und filtern.

Die folgende Tabelle zeigt die Suchkriterien, die Sie für Agenten verwenden können, einschließlich Operatoren, Werten und einer Definition der Werte.

Suchkriterium	Operator	Wert: Definition
Kundendienstmitarbeiter-ID	==	Jede Agenten-ID, die aus der vorab ausgefüllten Liste ausgewählt wurde, aus der ein Erfassungstool installiert ist.
Hostname	== !=	Für Agenten ein beliebiger Host-Namen aus der vorausgefüllten Liste von Hosts, auf denen ein Agent installiert ist.
Sammlungsstatus	== !=	Gestartet: Daten werden gesammelt und an den Application Discovery Service gesendet Start scheduled (Start geplant): Der Start der Datensammlung ist geplant. Beim nächsten Ping werden Daten an den Application Discovery Service gesendet, und der Status ändert sich auf Gestartet.

Suchkriterium	Operator	Wert: Definition
		Beendet: Es werden keine Daten gesammelt oder an den Application Discovery Service gesendet. Stop scheduled (Beenden geplant): Das Beenden der Datensammlung ist geplant. Beim nächsten Ping werden keine Daten mehr an den Application Discovery Service gesendet, und der Status ändert sich in Gestoppt.

Suchkriterium	Operator	Wert: Definition
Gesundheit	==	Healthy (Fehlerfrei): Datensammlung ist nicht eingeschaltet. Das Tool funktioniert normal.
	!=	Unhealthy (Fehlerhaft): Das Tool befindet sich in einem Fehlerzustand. Es werden keine Daten gesammelt oder gemeldet. Unknown (Unbekannt): Seit über eine Stunde wurde keine Verbindung mehr hergestellt. Shutdown (Herunterfahren): Das Tool hat zuletzt gemeldet, dass es aufgrund des Herunterfahrens eines Systems, Service oder Daemon heruntergefahren wird. Wenn ein Neustart stattfand oder ein Tool aktualisiert wurde, ändert sich der Status beim ersten Meldezyklus in einen anderen Status. Running (Läuft): Die Datensammlung ist eingeschaltet. Das Tool funktioniert normal.

Suchkriterium	Operator	Wert: Definition
IP-Adresse	==	Eine beliebige IP-Adresse aus der vorausgefüllten Liste, an der ein Sammlungstool installiert ist.
	!=	

Die folgende Tabelle zeigt die Suchkriterien, die Sie für Agentless-Collectors verwenden können, einschließlich Operatoren, Werten und einer Definition der Werte.

Suchkriterium	Operator	Wert: Definition
ID (ID)	==	Jede Agentenlose Collector-ID, die aus der vorab ausgefüllten Liste ausgewählt wurde, aus der ein Erfassungstool installiert ist.
Hostname	==	Bei Collectors ohne Agenten jeder Hostname, der aus der vorab ausgefüllten Liste der Hosts ausgewählt wurde, auf denen ein agentenloser Collector installiert ist.
	!=	
Status	==	Daten sammeln: Die Datenerfassung ist aktiviert. Das Tool funktioniert normal.
	!=	Bereit zur Konfiguration — Die Datenerfassung ist nicht aktiviert. Das Tool funktioniert normal. Erfordert Aufmerksamkeit — Das Tool befindet sich in

Suchkriterium	Operator	Wert: Definition
		einem Fehlerstatus und muss behoben werden. Unknown (Unbekannt): Seit über eine Stunde wurde keine Verbindung mehr hergestellt. Herunterfahren: Das Tool hat zuletzt gemeldet, dass es aufgrund des Herunterfahrens eines Systems, Dienstes oder Daemons heruntergefahren wurde. Wenn ein Neustart stattfand oder ein Tool aktualisiert wurde, ändert sich der Status beim ersten Meldezyklus in einen anderen Status.
IP-Adresse	== !=	Eine beliebige IP-Adresse aus der vorausgefüllten Liste, an der ein Sammlungstool installiert ist.

So sortieren Sie Datensammler durch Anwenden von Suchfiltern

1. Melden Sie sich mit Ihrem AWS Konto bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole unter Discover die Option Data Collectors aus.
3. Wählen Sie entweder die Registerkarte Agentless Collectors oder Agents.
4. Klicken Sie auf die Suchleiste und wählen Sie ein Suchkriterium aus der Liste aus.
5. Wählen Sie einen Operator aus der Liste aus.
6. Wählen Sie einen Wert aus der Liste aus.

Server in der Konsole anzeigen AWS Migration Hub

Die Seite Servers (Server) enthält Daten über die Systemkonfiguration und Leistung zu jeder Server-Instance, die den Datensammlungstools bekannt ist. Sie können Serverinformationen anzeigen, Servern mithilfe von Filtern sortieren, Servern mit Schlüssel-Wert-Paaren markieren und detaillierte Server- und Systeminformationen exportieren.

Sie können eine allgemeine Ansicht und eine detaillierte Ansicht der Server erhalten, die mit den Datensammlungstools erkannt werden.

So zeigen Sie erkannte Server an

1. Melden Sie sich mit Ihrem AWS Konto bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole unter Discover die Option Servers aus. Die erkannten Server erscheinen in der Serverliste.
3. Um weitere Informationen zu einem Server zu erhalten, wählen Sie seinen Link in der Spalte Server info (Server-Info) aus. Dadurch wird ein Bildschirm mit einer Beschreibung des Servers angezeigt.

Der Bildschirm mit Details zum Server zeigt Systeminformationen und Leistungsmetriken an. Sie finden dort auch eine Schaltfläche zum Exportieren von Netzwerkabhängigkeiten und Prozessinformationen. Weitere Informationen zum Exportieren detaillierter Serverinformationen finden Sie unter [Wird AWS Migration Hub zum Exportieren von Serverdaten verwendet](#).

Server in der AWS Migration Hub Konsole sortieren

Um auf einfache Weise bestimmte Server zu finden, können Sie zum Sortieren aller mit den Sammlungstools erkannten Server Suchfilter anwenden. Sie können nach zahlreichen Kriterien suchen und filtern.

So sortieren Sie Server durch Anwenden von Suchfiltern

1. Melden Sie sich mit Ihrem AWS Konto bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole unter Discover die Option Servers aus.

3. Klicken Sie auf die Suchleiste und wählen Sie ein Suchkriterium aus der Liste aus.
4. Wählen Sie einen Operator aus der Liste aus.
5. Geben Sie unter Beachtung der Groß-/Kleinschreibung einen Wert für das ausgewählte Suchkriterium ein und drücken Sie die Eingabetaste.
6. Es können mehrere Filter angewendet werden, indem Sie die Schritte 2 bis 4 wiederholen.

Kennzeichnen von Servern in der Konsole AWS Migration Hub

Zur Unterstützung der Migrationsplanung und zur Erleichterung der Organisation können Sie für jeden Server mehrere Tags erstellen. Tags sind benutzerdefinierte Schlüssel-Wert-Paare, mit denen beliebige benutzerdefinierte Daten oder Metadaten zu Servern gespeichert werden können. Sie können einen einzelnen Server oder mehrere Server in einem einzigen Vorgang taggen. AWS Application Discovery Service (Application Discovery Service) -Tags ähneln AWS Tags, aber die beiden Tag-Typen können nicht synonym verwendet werden.

Sie können mehrere Tags für einen oder mehrere Server auf der Servers (Server)-Hauptseite hinzufügen oder entfernen. Auf der Detailseite eines Servers können Sie einen oder mehrere Tags für den ausgewählten Server hinzufügen oder entfernen. Sie können jede Art von Tagging-Aufgabe mit mehreren Servern oder Tags in einer einzigen Operation durchführen. Außerdem können Sie Tags entfernen.

So fügen Sie Tags zu einem oder mehreren Servern hinzu

1. Melden Sie sich mit Ihrem AWS Konto bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole unter Discover die Option Servers aus.
3. Wählen Sie in der Spalte Server info (Server-Info) den Server-Link für den Server aus, für den Sie Tags hinzufügen möchten. Um zu mehr als einem Server gleichzeitig Tags hinzuzufügen, klicken Sie auf das Kontrollkästchen für mehrere Server.
4. Wählen Sie Tags hinzufügen und dann Neues Tag hinzufügen aus.
5. Geben Sie im Dialogfeld einen Schlüssel in das Feld Schlüssel und optional einen Wert in das Feld Wert ein.

Fügen Sie weitere Tags hinzu, indem Sie Neues Tag hinzufügen wählen und weitere Informationen hinzufügen.

6. Wählen Sie Speichern.

So entfernen Sie Tags von einem oder mehreren Servern

1. Melden Sie sich mit Ihrem AWS Konto bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole unter Discover die Option Servers aus.
3. Wählen Sie in der Spalte Server info (Server-Info) den Server-Link für den Server aus, von dem Sie Tags entfernen möchten. Aktivieren Sie die Kontrollkästchen mehrerer Server, um Tags von mehreren Servern gleichzeitig zu entfernen.
4. Wählen Sie Tags entfernen.
5. Wählen Sie jedes Tag aus, das Sie entfernen möchten.
6. Wählen Sie Bestätigen aus.

Wird AWS Migration Hub zum Exportieren von Serverdaten verwendet

In diesem Thema wird erklärt, wie Serverdaten mithilfe der AWS-Managementkonsole AWS Command Line Interface, oder der API exportiert werden.

Um den zu verwenden AWS-Managementkonsole , um Serverdaten für alle Server zu exportieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
2. Wählen Sie im linken Navigationsbereich unter Discover die Option Servers aus.
3. Wählen Sie Aktionen und anschließend Discovery-Daten exportieren aus.
4. Wählen Sie im Bereich Exports (Exporte) unten auf dem Bildschirm Export server details (Serverdetails exportieren) aus. Diese Aktion generiert eine ZIP-Datei, die die in der folgenden Tabelle beschriebenen CSV-Dateien enthält.

Dateiname	Description
{account_id} _Application.csv	Details zu jeder Anwendung, einschließlich Serveranzahl, Name und Beschreibung.
{Account-ID} _ .csv ApplicationResourceAssociation	Die Beziehung zwischen Servern und Anwendungen.
{account_id} _ ImportTemplate	Die Zusammenfassung der Anwendungen und Tags der einzelnen Server. Diese Datei kann geändert und erneut importiert werden, um die dem Server zugeordnete Anwendung zu aktualisieren.
{Konto_ID} _ .csv NetworkInterface	Details zu jeder Netzwerkschnittstelle, einschließlich des zugehörigen Servers, der Adresse und des Switches.
{account_id} _Server.csv	Details zu jedem Server, einschließlich Betriebssystem, Hostname und Hypervisor.
{Konto_ID} _ .csv SystemPerformance	Details zu jedem Server, einschließlich CPU-, Arbeitsspeicher- und Speicherkonfiguration sowie Leistung.
{account_id} _Tags.csv	Details zu jedem Tag, der einem Server zugeordnet ist.
{account_id} _ Info.csv VMware	Details zu jeder VMware Konfiguration, einschließlich MoRef, VMName und vCenter.

Um den zu verwenden AWS-Managementkonsole , um Agentendaten für einen bestimmten Server zu exportieren

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
2. Wählen Sie im linken Navigationsbereich unter Discover die Option Servers aus.

3. Platzieren Sie den Cursor im Suchfeld unter Server. Eine Dropdownliste wird angezeigt. Wählen Sie in dieser Liste unter Eigenschaften die Option Quelle, dann den Operator = und anschließend Quelle = Agent aus.
4. Wählen Sie in den Suchergebnissen den Namen des Servers aus, für den Sie Daten exportieren möchten. Mit dieser Aktion gelangen Sie zur Detailseite für diesen Server.
5. Geben Sie eine Start- und eine Endzeit ein und wählen Sie dann Exportieren. Die exportierte ZIP-Datei enthält die CSV-Dateien, die in der folgenden Tabelle beschrieben werden.

{account_id} _ .csv destinationProcess Connection	Details der eingehenden Verbindungen zum Server.
{account_id} _networkInterface.csv	Details zu jeder Netzwerkschnittstelle, einschließlich Adresse, Maske und Name
{account_id} _osInfo.csv	Einzelheiten zum Betriebssystem, einschließlich CPU-Typ, Hypervisor und Betriebssystemname.
{account_id} _process.csv	Details zu den Prozessen, die auf dem Server laufen.
{Konto_ID} _ .csv sourceProcessConnection	Details der ausgehenden Verbindung, die vom Server ausgeht.
{account_id} _systemPerformance.csv	Einzelheiten zur CPU-, Arbeitsspeicher- und Speicherkonfiguration und -leistung für den Server.

Um die AWS Command Line Interface oder die API zum Exportieren von Serverdaten zu verwenden

1. Führen Sie [start-export-task](#). Die entsprechende API-Operation ist [StartExportTask](#)
2. Führen Sie [describe-export-tasks](#). Die entsprechende API-Operation ist [DescribeExportTasks](#).

Gruppierung von Servern in der Konsole AWS Migration Hub

Einige Ihrer erkannten Server müssen möglicherweise gemeinsam migriert werden, um funktionsfähig zu bleiben. In diesem Fall können Sie die erkannten Server logisch definieren und Gruppen in Anwendungen gruppieren.

Im Rahmen der Gruppierung können Sie Tags suchen, filtern und hinzufügen.

So gruppieren Sie Server in eine neue oder vorhandene Anwendung

1. Melden Sie sich mit Ihrem AWS Konto bei der an AWS-Managementkonsole und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub/>.
2. Wählen Sie im Navigationsbereich der Migration Hub Hub-Konsole unter Discover die Option Servers aus.
3. Wählen Sie in der Serverliste die einzelnen Server aus, die Sie in eine neue oder vorhandene Anwendung gruppieren möchten.

Um die Auswahl von Servern für Ihre Gruppe zu erleichtern, können Sie beliebige Kriterien, die Sie in der Serverliste angeben, suchen und filtern. Klicken Sie auf die Suchleiste und wählen Sie ein Element aus der Liste aus, wählen Sie einen Operator aus der nächsten Liste aus und geben Sie dann in Ihrer Kriterien ein.

4. Optional: Wählen Sie für jeden ausgewählten Server Add tag (Tag hinzufügen) und geben Sie einen Wert für Key (Schlüssel) und optional einen Wert für Value (Wert) ein.
5. Wählen Sie Group as application (Als Anwendung gruppieren), um Ihre Anwendung zu erstellen oder zu einer vorhandenen hinzuzufügen.
6. Wählen Sie im Dialogfeld Group as application (Als Anwendung gruppieren) die Option Group as a new application (Als neue Anwendung gruppieren) oder Add to an existing application (Zu einer vorhandenen Anwendung hinzufügen).
- a. Wenn Sie Group as a new application (Als neue Anwendung gruppieren) gewählt haben, geben Sie einen Namen für Application name (Anwendungsname) ein. Optional können Sie eine Beschreibung für Application description (Anwendungsbeschreibung) eingeben.
- b. Wählen Sie bei Wahl von Add to an existing application (Zu einer vorhandenen Anwendung hinzufügen) in der Liste den Namen der Anwendung aus, zu der Sie hinzufügen möchten.
7. Wählen Sie Speichern.

Abfragen von erkannten Konfigurationselementen mithilfe der Application Discovery Service API

Ein Konfigurationselement ist ein IT-Asset, das in Ihrem Rechenzentrum von einem Agenten oder durch einen Import entdeckt wurde. Wenn Sie AWS Application Discovery Service (Application Discovery Service) verwenden, verwenden Sie die API, um Filter anzugeben und spezifische Konfigurationselemente für Server-, Anwendungs-, Prozess- und Verbindungsressourcen abzufragen. Informationen zur API finden Sie unter [Application Discovery Service API-Referenz](#).

In den Tabellen in den folgenden Abschnitten sind die verfügbaren Eingabefilter und Ausgabesortieroptionen für zwei Application Discovery Service Service-Aktionen aufgeführt:

- `DescribeConfigurations`
- `ListConfigurations`

Die Filter- und Sortieroptionen sind nach dem Asset-Typ (Server, Anwendung, Prozess oder Verbindung) organisiert.

Important

Die von `DescribeConfigurations`, `ListConfigurations`, zurückgegebenen Ergebnisse enthalten `StartExportTask` möglicherweise keine aktuellen Aktualisierungen. Weitere Informationen finden Sie unter [the section called “Letztendliche Datenkonsistenz”](#).

Verwenden der **DescribeConfigurations** Aktion

Die `DescribeConfigurations` Aktion ruft Attribute für eine IDs Konfigurationsliste ab. Alle angegebenen Daten IDs müssen für denselben Asset-Typ (Server, Anwendung, Prozess oder Verbindung) verwendet werden. Ausgabefelder sind für den gewählten Komponententyp spezifisch. Beispiel: Die Ausgabe für ein Server-Konfigurationselement enthält eine Liste von Attributen zum Server, z. B. den Host-Namen, das Betriebssystem und die Anzahl der Netzwerkkarten. Weitere Hinweise zur Befehlssyntax finden Sie unter [DescribeConfigurations](#).

Die `DescribeConfigurations`-Aktion unterstützt keine Filterung.

Ausgabefelder für **DescribeConfigurations**

In den folgenden nach Asset-Typ geordneten Tabellen sind die unterstützten Ausgabefelder der DescribeConfigurations-Aktion aufgeführt. Zwingend erforderliche Felder sind immer in der Ausgabe vorhanden.

Serverressourcen

Feld	zwingend erforderlich
<code>server.agentId</code>	
<code>server.applications</code>	
<code>server.applications.hasMoreValues</code>	
<code>server.configurationId</code>	x
<code>server.cpuType</code>	
<code>server.hostName</code>	
<code>server.hypervisor</code>	
<code>server.networkInterfaceInfo</code>	
<code>server.networkInterfaceInfo.hasMoreValues</code>	
<code>server.osName</code>	
<code>server.osVersion</code>	
<code>server.tags</code>	
<code>server.tags.hasMoreValues</code>	
<code>server.timeOfCreation</code>	x
<code>server.type</code>	

Feld	zwingend erforderlich
<code>server.performance.avgCpuUsagePct</code>	
<code>server.performance.avgDiskReadIOPS</code>	
<code>server.performance.avgDiskReadsPerSecondInKB</code>	
<code>server.performance.avgDiskWriteIOPS</code>	
<code>server.performance.avgDiskWritesPerSecondInKB</code>	
<code>server.performance.avgFreeRAMInKB</code>	
<code>server.performance.avgNetworkReadsPerSecondInKB</code>	
<code>server.performance.avgNetworkWritesPerSecondInKB</code>	
<code>server.performance.maxCpuUsagePct</code>	
<code>server.performance.maxDiskReadIOPS</code>	
<code>server.performance.maxDiskReadsPerSecondInKB</code>	
<code>server.performance.maxDiskWriteIOPS</code>	
<code>server.performance.maxDiskWritesPerSecondInKB</code>	

Feld	zwingend erforderlich
<code>server.performance.maxNetworkReadsPerSecondInKB</code>	
<code>server.performance.maxNetworkWritesPerSecondInKB</code>	
<code>server.performance.minFreeRAMInKB</code>	
<code>server.performance.numCores</code>	
<code>server.performance.numCpus</code>	
<code>server.performance.numDisks</code>	
<code>server.performance.numNetworkCards</code>	
<code>server.performance.totalRAMInKB</code>	

Verarbeitungs-Assets

Feld	zwingend erforderlich
<code>process.commandLine</code>	
<code>process.configurationId</code>	x
<code>process.name</code>	
<code>process.path</code>	
<code>process.timeOfCreation</code>	x

Anwendungs-Assets

Feld	zwingend erforderlich
application.configurationId	x
application.description	
application.lastModifiedTime	x
application.name	x
application.serverCount	x
application.timeOfCreation	x

Die **ListConfigurations** Aktion verwenden

Die ListConfigurations-Aktion ruft eine Liste von Konfigurationselementen nach den Kriterien ab, die Sie in einem Filter angeben. Weitere Hinweise zur Befehlssyntax finden Sie unter [ListConfigurations](#).

Ausgabefelder für **ListConfigurations**

In den folgenden nach Asset-Typ geordneten Tabellen sind die unterstützten Ausgabefelder der ListConfigurations-Aktion aufgeführt. Zwingend erforderliche Felder sind immer in der Ausgabe vorhanden.

Serverressourcen

Feld	zwingend erforderlich
server.configurationId	x
server.agentId	
server.hostName	
server.osName	
server.osVersion	

Feld	zwingend erforderlich
<code>server.timeOfCreation</code>	x
<code>server.type</code>	

Verarbeitungs-Assets

Feld	zwingend erforderlich
<code>process.commandLine</code>	
<code>process.configurationId</code>	x
<code>process.name</code>	
<code>process.path</code>	
<code>process.timeOfCreation</code>	x
<code>server.agentId</code>	
<code>server.configurationId</code>	x

Anwendungs-Assets

Feld	zwingend erforderlich
<code>application.configurationId</code>	x
<code>application.description</code>	
<code>application.name</code>	x
<code>application.serverCount</code>	x
<code>application.timeOfCreation</code>	x
<code>application.lastModifiedTime</code>	x

Verbindungs-Assets

Feld	zwingend erforderlich
<code>connection.destinationIp</code>	x
<code>connection.destinationPort</code>	x
<code>connection.ipVersion</code>	x
<code>connection.latestTimestamp</code>	x
<code>connection.occurrence</code>	x
<code>connection.sourceIp</code>	x
<code>connection.transportProtocol</code>	
<code>destinationProcess.configurationId</code>	
<code>destinationProcess.name</code>	
<code>destinationServer.configurationId</code>	
<code>destinationServer.hostName</code>	
<code>sourceProcess.configurationId</code>	
<code>sourceProcess.name</code>	
<code>sourceServer.configurationId</code>	
<code>sourceServer.hostName</code>	

Unterstützte Filter für **ListConfigurations**

In den folgenden nach Asset-Typ geordneten Tabellen sind die unterstützten Filter für die **ListConfigurations**-Aktion aufgeführt. Filter und Werte stehen in einer key/value Beziehung,

die durch eine der unterstützten logischen Bedingungen definiert ist. Sie können die Ausgabe der angegebenen Filter sortieren.

Serverressourcen

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
<code>server.configurationId</code>	• EQUALS • NOT_EQUALS • EQ • NE	• Jede gültige Serverkonfigurations-ID	Keine
<code>server.hostName</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	• ASC • DESC
<code>server.osName</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	• ASC • DESC
<code>server.osVersion</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	• ASC • DESC
<code>server.agentId</code>	• EQUALS	• Zeichenfolge	Keine

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
	• NOT_EQUALS • EQ • NE		
server.connectorId	• EQUALS • NOT_EQUALS • EQ • NE	• Zeichenfolge	Keine
server.type	• EQUALS • NOT_EQUALS • EQ • NE	String mit einem der folgenden Werte: • EC2 • OTHER • VMWARE_VM • VMWARE_HOST • VMWARE_VM_TEMPLATE	Keine
server.vmWareInfo.morefId	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
<code>server.vmWareInfo.vcenterId</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine
<code>server.vmWareInfo.hostId</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine
<code>server.networkInterfaceInfo.portGroupId</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine
<code>server.networkInterfaceInfo.portGroupName</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
server.networkInterfaceInfo.virtualSwitchName	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine
server.networkInterfaceInfo.ipAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine
server.networkInterfaceInfo.macAddress	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine
server.performance.avgCpuUsagePct	• GE • LE • GT • LT	• Prozentsatz	Keine
server.performance.totalDiskFreeSizeInKB	• GE • LE • GT • LT	• Double	Keine

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
<code>server.performance.avgFreeRAMInKB</code>	• GE • LE • GT • LT	• Double	Keine
<code>server.tag.value</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine
<code>server.tag.key</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine
<code>server.application.name</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
<code>server.application.description</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine
<code>server.application.configurationId</code>	• EQUALS • NOT_EQUALS • EQ • NE	• Jede gültige Anwendungskonfigurations-ID	Keine
<code>server.process.configurationId</code>	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	Keine
<code>server.process.name</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine
<code>server.process.commandLine</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	Keine

Anwendungs-Assets

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
application.configurationId	- EQUALS - NOT_EQUALS - EQ - NE	ApplicationId	Keine
application.name	- EQUALS - NOT_EQUALS - EQ - NE - CONTAINS - NOT_CONTAINS	Zeichenfolge	- ASC - DESC
application.description	- EQUALS - NOT_EQUALS - EQ - NE - CONTAINS - NOT_CONTAINS	Zeichenfolge	- ASC - DESC
application.serverCount	Filtern wird nicht unterstützt.	Filtern wird nicht unterstützt.	- ASC - DESC
application.timeOfCreation	Filtern wird nicht unterstützt.	Filtern wird nicht unterstützt.	- ASC - DESC

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
<code>application.lastModifiedTime</code>	Filtern wird nicht unterstützt.	Filtern wird nicht unterstützt.	• ASC • DESC
<code>server.configurationId</code>	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	Keine

Verarbeitungs-Assets

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
<code>process.configurationId</code>	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
<code>process.name</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	• ASC • DESC
<code>process.commandLine</code>	• EQUALS • NOT_EQUALS • EQ • NE	• Zeichenfolge	• ASC • DESC

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
	- CONTAINS - NOT_CONTAINS		
server.configurationId	- EQUALS - NOT_EQUALS - EQ - NE	ServerId	
server.hostName	- EQUALS - NOT_EQUALS - EQ - NE - CONTAINS - NOT_CONTAINS	Zeichenfolge	- ASC - DESC
server.osName	- EQUALS - NOT_EQUALS - EQ - NE - CONTAINS - NOT_CONTAINS	Zeichenfolge	- ASC - DESC
server.osVersion	- EQUALS - NOT_EQUALS - EQ - NE - CONTAINS - NOT_CONTAINS	Zeichenfolge	- ASC - DESC

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
<code>server.agentId</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	

Verbindungs-Assets

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
<code>connection.sourceIp</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
<code>connection.destinationIp</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• IP	• ASC • DESC
<code>connection.destinationPort</code>	• EQUALS • NOT_EQUALS • EQ • NE	• Ganzzahl	• ASC • DESC

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
<code>sourceServer.configurationId</code>	• EQUALS • NOT_EQUALS • EQ • NE	• ServerId	
<code>sourceServer.hostName</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	• ASC • DESC
<code>destinationServer.osName</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	• ASC • DESC
<code>destinationServer.osVersion</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	• ASC • DESC

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
<code>destinationServer.agentId</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	
<code>sourceProcess.configurationId</code>	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	
<code>sourceProcess.name</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	• ASC • DESC
<code>sourceProcess.commandLine</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	• ASC • DESC
<code>destinationProcess.configurationId</code>	• EQUALS • NOT_EQUALS • EQ • NE	• ProcessId	

Filter	Unterstützte Bedingungen	Unterstützte Werte	Unterstützte Sortierung
<code>destinationProcess.name</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	• ASC • DESC
<code>destinationProcess.commandLine</code>	• EQUALS • NOT_EQUALS • EQ • NE • CONTAINS • NOT_CONTAINS	• Zeichenfolge	• ASC • DESC

Eventuelle Konsistenz in der API AWS Application Discovery Service

Die folgenden Aktualisierungsvorgänge sind letztendlich konsistent. Aktualisierungen sind für die Lesevorgänge [StartExportTaskDescribeConfigurations](#), und möglicherweise nicht sofort sichtbar [ListConfigurations](#).

- [AssociateConfigurationItemsToApplication](#)
- [CreateTags](#)
- [DeleteApplications](#)
- [DeleteTags](#)
- [DescribeBatchDeleteConfigurationTask](#)
- [DescribeImportTasks](#)
- [DisassociateConfigurationItemsFromApplication](#)
- [UpdateApplication](#)

Vorschläge für die Verwaltung der eventuellen Konsistenz:

- Wenn Sie die Lesevorgänge oder [ListConfigurations](#) (oder die entsprechenden AWS CLI Befehle) aufrufen [StartExportTaskDescribeConfigurations](#), verwenden Sie einen exponentiellen Backoff-Algorithmus, damit alle vorherigen Aktualisierungsvorgänge genügend Zeit haben, um sich im System auszubreiten. Führen Sie dazu den Lesevorgang wiederholt aus, wobei Sie mit einer Wartezeit von zwei Sekunden beginnen und die Wartezeit schrittweise auf bis zu fünf Minuten erhöhen.
- Verlängert die Wartezeit zwischen aufeinanderfolgenden Vorgängen, auch wenn ein Aktualisierungsvorgang die Antwort 200 — OK zurückgibt. Wenden Sie einen exponentiellen Backoff-Algorithmus an, der mit einer Wartezeit von einigen Sekunden beginnt, und erhöhen Sie die Wartezeit schrittweise auf etwa fünf Minuten.

Zugriff AWS Application Discovery Service über einen Schnittstellenendpunkt (AWS PrivateLink)

Sie können AWS PrivateLink damit eine private Verbindung zwischen Ihrer VPC und AWS Application Discovery Service herstellen. Sie können auf den Application Discovery Service zugreifen, als ob er sich in Ihrer VPC befände, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder Direct Connect eine Verbindung verwenden zu müssen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf den Application Discovery Service zuzugreifen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellen-Endpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Dabei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Einstiegspunkt für den Traffic dienen, der für den Application Discovery Service bestimmt ist.

Weitere Informationen finden Sie unter [Zugriff auf AWS-Services über AWS PrivateLink](#) im AWS PrivateLink -Leitfaden.

Überlegungen zum Application Discovery Service

Bevor Sie einen Schnittstellenendpunkt für den Application Discovery Service einrichten, lesen Sie [den Artikel Zugriff auf einen AWS Dienst mithilfe eines VPC-Schnittstellen-Endpunkts](#) im AWS PrivateLink Handbuch.

Application Discovery Service unterstützt zwei Schnittstellen: Eine für Aufrufe aller API-Aktionen und eine zweite für den Agentless Collector und den AWS Application Discovery Agent zum Senden von Discovery-Daten.

Erstellen eines Schnittstellenendpunkts

Sie können einen Schnittstellenendpunkt für Lambda entweder über die Amazon-Connect-Konsole oder die AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie im AWS PrivateLink Handbuch unter [Zugreifen auf einen AWS Dienst über einen Schnittstellen-VPC-Endpunkt](#).

For Application Discovery Service

Erstellen Sie einen Schnittstellenendpunkt für Application Discovery Service mit dem folgenden Dienstnamen:

```
com.amazonaws.region.discovery
```

Wenn Sie privates DNS für den Schnittstellenendpunkt aktivieren, können Sie API-Anfragen an den Application Discovery Service stellen, indem Sie dessen standardmäßigen regionalen DNS-Namen verwenden. Beispiel, `discovery.us-east-1.amazonaws.com`.

For Agentless Collector and AWS Application Discovery Agent

Erstellen Sie einen Schnittstellenendpunkt mit dem folgenden Dienstnamen:

```
com.amazonaws.region.arsenal-discovery
```

Wenn Sie privates DNS für den Schnittstellenendpunkt aktivieren, können Sie API-Anfragen an Application Discovery Arsenal stellen, indem Sie dessen standardmäßigen regionalen DNS-Namen verwenden. Beispiel, `arsenal-discovery.us-east-1.amazonaws.com`.

Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie an einen Schnittstellen-Endpunkt anfügen können. Die standardmäßige Endpunktrichtlinie ermöglicht den vollen Zugriff auf einen AWS Dienst über den Schnittstellenendpunkt. Um den Zugriff auf einen AWS Dienst von Ihrer VPC aus zu kontrollieren, fügen Sie dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können (AWS-Konten, IAM-Benutzer und IAM-Rollen).
- Aktionen, die ausgeführt werden können

Weitere Informationen finden Sie unter [Steuern des Zugriffs auf Services mit Endpunktrichtlinien](#) im AWS PrivateLink -Leitfaden.

Beispiel: VPC-Endpunktrichtlinien

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellen-Endpunkt anhängen, gewährt sie allen Prinzipalen auf allen Ressourcen den Zugriff auf die aufgeführten -Aktionen.

Example policy for Application Discovery Service

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "discovery:action-1",
        "discovery:action-2",
        "discovery:action-3"
      ],
      "Resource": "*"
    }
  ]
}
```

Example policy for the Agentless Collector and AWS Application Discovery Agent

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource": "*"
    }
  ]
}
```

Verwenden des VPC-Endpunkts für den Agentless Collector und den AWS Application Discovery Agent

Der Agentless Collector und der AWS Application Discovery Agent unterstützen keine konfigurierbaren Endpunkte. Verwenden Sie stattdessen die private DNS-Funktion für den `arsenal-discovery` Amazon VPC-Endpunkt.

- Richten Sie die Direct Connect Routing-Tabelle ein, um private AWS-IP-Adressen an die VPC weiterzuleiten. Zum Beispiel Ziel = 10.0.0.0/8 und Ziel = lokal. Für dieses Setup benötigen Sie mindestens das Routing der privaten IP-Adressen des `arsenal-discovery` Amazon VPC-Endpunkts zur VPC.
- Verwenden Sie die private DNS-Funktion für `arsenal-discovery` Amazon VPC-Endpoints, da der Agentless Collector keine konfigurierbaren Arsenal-Endpunkte unterstützt.
- Richten Sie den `arsenal-discovery` Amazon VPC-Endpunkt in einem privaten Subnetz mit derselben VPC ein, zu der Sie den Datenverkehr weiterleiten. Direct Connect
- Richten Sie den `arsenal-discovery` Amazon VPC-Endpunkt mit einer Sicherheitsgruppe ein, die eingehenden Datenverkehr aus der VPC ermöglicht (z. B. 10.0.0.0/8).
- Richten Sie einen Amazon Route 53-Inbound-Resolver ein, um die DNS-Auflösung für den privaten DNS-Namen des `arsenal-discovery` Amazon VPC-Endpunkts weiterzuleiten, der in die private IP des VPC-Endpunkts aufgelöst wird. Wenn Sie das nicht tun, führt der Collector die DNS-Auflösung mithilfe des lokalen Resolvers durch und verwendet den öffentlichen Arsenal-Endpunkt, und der Datenverkehr wird nicht über die VPC geleitet.
- Wenn Sie den gesamten öffentlichen Verkehr deaktiviert haben, schlägt die automatische Aktualisierungsfunktion fehl. Das liegt daran, dass der Agentless Collector Updates abrufen, indem er Anfragen an den Amazon ECR-Endpunkt sendet. Damit die automatische Aktualisierungsfunktion funktioniert, ohne Anfragen über das öffentliche Internet zu senden, richten Sie einen VPC-Endpunkt für den Amazon ECR-Service ein und aktivieren Sie die private DNS-Funktion für diesen Endpunkt.

Sicherheit in AWS Application Discovery Service

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einem Rechenzentrum und einer Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Die Wirksamkeit unserer Sicherheitsfunktionen wird regelmäßig von externen Prüfern im Rahmen des [AWS -Compliance-Programms getestet und überprüft](#).
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. In Ihre Verantwortung fallen außerdem weitere Faktoren, wie z. B. die Vertraulichkeit der Daten, die Anforderungen Ihrer Organisation sowie geltende Gesetze und Vorschriften.

Um den AWS Application Discovery Agent oder den Application Discovery Service Agentless Collector verwenden zu können, müssen Sie Zugangsschlüssel für Ihr AWS Konto angeben. Diese Informationen werden dann in Ihrer lokalen Infrastruktur gespeichert. Im Rahmen des Modells der gemeinsamen Verantwortung sind Sie dafür verantwortlich, den Zugriff auf Ihre Infrastruktur zu sichern.

In dieser Dokumentation erfahren Sie, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Application Discovery Service anwenden können. In den folgenden Themen erfahren Sie, wie Sie den Application Discovery Service konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste verwenden können, die Ihnen helfen können, Ihre Application Discovery Service Service-Ressourcen zu überwachen und zu sichern.

Topics

- [Identity and Access Management für AWS Application Discovery Service](#)
- [Protokollieren von API-Aufrufen des Application Discovery Service mit AWS CloudTrail](#)

Identity and Access Management für AWS Application Discovery Service

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service, den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Application Discovery Service Service-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service, das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [Wie AWS Application Discovery Service funktioniert mit IAM](#)
- [AWS verwaltete Richtlinien für AWS Application Discovery Service](#)
- [AWS Application Discovery Service Beispiele für identitätsbasierte Richtlinien](#)
- [Verwenden von dienstverknüpften Rollen für den Application Discovery Service](#)
- [Problembehandlung bei AWS Application Discovery Service Identität und Zugriff](#)

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe [Problembehandlung bei AWS Application Discovery Service Identität und Zugriff](#)).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe [Wie AWS Application Discovery Service funktioniert mit IAM](#)).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe [AWS Application Discovery Service Beispiele für identitätsbasierte Richtlinien](#)).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter [So melden Sie sich bei Ihrem AWS-Konto an](#) im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter [AWS Signature Version 4 for API requests](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Tasks that require root user credentials](#) im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Erfordern, dass menschliche Benutzer für den Zugriff AWS mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter](#) verwenden müssen.

Eine [IAM-Gruppe](#) spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter [Anwendungsfälle für IAM-Benutzer](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie [von einer Benutzer-](#)

[zu einer IAM-Rolle \(Konsole\) wechseln](#) AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter [Methoden, um eine Rolle zu übernehmen](#) im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcen und unter welchen Bedingungen durchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter [Choose between managed policies and inline policies](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#).

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter [Übersicht über ACLs die Zugriffskontrollliste \(ACL\)](#) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- **Berechtigungsgrenzen** – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im -IAM-Benutzerhandbuch.
- **Richtlinien zur Dienstkontrolle (SCPs)** — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter [Service-Kontrollrichtlinien](#) im AWS Organizations -Benutzerhandbuch.
- **Richtlinien zur Ressourcenkontrolle (RCPs)** — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter [Richtlinien zur Ressourcenkontrolle \(RCPs\)](#).
- **Sitzungsrichtlinien** – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter [Bewertungslogik für Richtlinien](#) im IAM-Benutzerhandbuch.

Wie AWS Application Discovery Service funktioniert mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf den Application Discovery Service zu verwalten, sollten Sie wissen, welche IAM-Funktionen für die Verwendung mit Application Discovery Service verfügbar sind. Einen allgemeinen Überblick darüber, wie Application Discovery Service und andere AWS Dienste mit IAM zusammenarbeiten, finden Sie unter [AWS Services That Work with IAM](#) im IAM-Benutzerhandbuch.

Themen

- [Identitätsbasierte Richtlinien für den Application Discovery Service](#)
- [Ressourcenbasierte Richtlinien für den Application Discovery Service](#)
- [Autorisierung auf der Grundlage von Application Discovery Service Service-Tags](#)
- [IAM-Rollen für den Application Discovery Service](#)

Identitätsbasierte Richtlinien für den Application Discovery Service

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Der Application Discovery Service unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Richtlinienaktionen im Application Discovery Service verwenden das folgende Präfix vor der Aktion: `discovery:`. Richtlinienanweisungen müssen entweder ein `Action` oder ein `NotAction`-Element enthalten. Der Application Discovery Service definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

```
"Action": [  
    "discovery:action1",  
    "discovery:action2"
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "discovery:Describe*"
```

Eine Liste der Application Discovery Service Service-Aktionen finden Sie unter [Definierte Aktionen von AWS Application Discovery Service](#) im IAM-Benutzerhandbuch.

Ressourcen

Der Application Discovery Service unterstützt die Angabe von Ressourcen ARNs in einer Richtlinie nicht. Um den Zugriff zu trennen, erstellen und verwenden Sie ihn separat AWS-Konten.

Bedingungsschlüssel

Der Application Discovery Service stellt keine dienstspezifischen Bedingungsschlüssel bereit, unterstützt jedoch die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [AWS Globale Bedingungskontextschlüssel](#) im IAM-Benutzerhandbuch.

Beispiele

Beispiele für identitätsbasierte Richtlinien des Application Discovery Service finden Sie unter. [AWS Application Discovery Service Beispiele für identitätsbasierte Richtlinien](#)

Ressourcenbasierte Richtlinien für den Application Discovery Service

Der Application Discovery Service unterstützt keine ressourcenbasierten Richtlinien.

Autorisierung auf der Grundlage von Application Discovery Service Service-Tags

Der Application Discovery Service unterstützt weder das Markieren von Ressourcen noch das Steuern des Zugriffs auf der Grundlage von Tags.

IAM-Rollen für den Application Discovery Service

Eine [IAM-Rolle](#) ist eine Entität innerhalb Ihres AWS Kontos, die über bestimmte Berechtigungen verfügt.

Temporäre Anmeldeinformationen mit dem Application Discovery Service verwenden

Der Application Discovery Service unterstützt die Verwendung temporärer Anmeldeinformationen nicht.

Service-verknüpfte Rollen

Mit [dienstbezogenen Rollen](#) können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Der Application Discovery Service unterstützt dienstverknüpfte Rollen. Einzelheiten zum Erstellen oder Verwalten von mit dem Application Discovery Service verknüpften Rollen finden Sie unter [Verwenden von dienstverknüpften Rollen für den Application Discovery Service](#).

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer [Servicerolle](#) in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

Der Application Discovery Service unterstützt Dienstrollen.

AWS verwaltete Richtlinien für AWS Application Discovery Service

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um [von Kunden verwaltete IAM-Richtlinien zu erstellen](#), die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter [AWS Verwaltete Richtlinien](#).

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in [Verwaltete AWS -Richtlinien für Auftragsfunktionen](#) im IAM-Leitfaden.

AWS verwaltete Richtlinie: AWSApplicationDiscoveryServiceFullAccess

Die AWSApplicationDiscoveryServiceFullAccess Richtlinie gewährt einem IAM-Benutzerkonto Zugriff auf den Application Discovery Service und den Migration Hub APIs.

Ein IAM-Benutzerkonto, dem diese Richtlinie zugewiesen ist, kann den Application Discovery Service konfigurieren, Agenten starten und beenden, die agentenlose Erkennung starten und beenden und Daten aus der AWS Discovery Service-Datenbank abfragen. Ein Beispiel für diese Richtlinie finden Sie unter [Vollzugriff auf den Application Discovery Service gewähren](#).

AWS verwaltete Richtlinie: AWSApplicationDiscoveryAgentlessCollectorAccess

Die `AWSApplicationDiscoveryAgentlessCollectorAccess` verwaltete Richtlinie gewährt dem Application Discovery Service Agentless Collector (Agentless Collector) Zugriff, um sich zu registrieren und mit dem Application Discovery Service zu kommunizieren und mit anderen AWS Diensten zu kommunizieren.

Diese Richtlinie muss dem IAM-Benutzer zugewiesen werden, dessen Anmeldeinformationen zur Konfiguration des Agentless Collectors verwendet werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `arsenal`— Ermöglicht dem Collector, sich bei der Application Discovery Service Service-Anwendung zu registrieren. Dies ist notwendig, um gesammelte Daten an zurücksenden zu können AWS.
- `ecr-public`— Ermöglicht dem Collector, Aufrufe an das Amazon Elastic Container Registry Public (Amazon ECR Public) zu tätigen, wo die neuesten Updates für den Collector gefunden werden.
- `mgh`— Ermöglicht dem Collector, anzurufen AWS Migration Hub , um die Heimatregion des Kontos abzurufen, das zur Konfiguration des Collectors verwendet wurde. Dies ist notwendig, um zu wissen, in welche Region die gesammelten Daten gesendet werden sollen.
- `sts`— Ermöglicht dem Collector, ein Service Bearer-Token abzurufen, sodass der Collector Amazon ECR Public aufrufen kann, um die neuesten Updates zu erhalten.

JSON

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

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "ecr-public:DescribeImages"
      ],
      "Resource": "arn:aws:ecr-
public::446372222237:repository/6e5498e4-8c31-4f57-9991-13b4b992ff7b"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecr-public:GetAuthorizationToken"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mgh:GetHomeRegion"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sts:GetServiceBearerToken"
      ],
      "Resource": "*"
    }
  ]
}

```

AWS verwaltete Richtlinie: AWSApplication DiscoveryAgentAccess

Die `AWSApplicationDiscoveryAgentAccess` Richtlinie gewährt dem Application Discovery Agent Zugriff auf die Registrierung und Kommunikation mit dem Application Discovery Service.

Sie fügen diese Richtlinie jedem Benutzer hinzu, dessen Anmeldeinformationen vom Application Discovery Agent verwendet werden.

Diese Richtlinie gewährt dem Benutzer außerdem den Zugriff auf Arsenal. Arsenal ist ein Agentendienst, der von verwaltet und gehostet wird AWS. Arsenal leitet Daten an den Application Discovery Service in der Cloud weiter. Ein Beispiel für diese Richtlinie finden Sie unter [Discovery-Agents Zugriff gewähren](#).

AWS verwaltete Richtlinie: AWSAgentless DiscoveryService

Die AWSAgentlessDiscoveryService Richtlinie gewährt dem AWS Agentless Discovery Connector, der auf Ihrem VMware vCenter Server ausgeführt wird, Zugriff auf die Registrierung, Kommunikation und gemeinsame Nutzung von Connector-Integritätsmetriken mit Application Discovery Service.

Fügen Sie diese Richtlinie einem Benutzer an, dessen Anmeldeinformationen von dem Connector verwendet werden.

AWS verwaltete Richtlinie:

ApplicationDiscoveryServiceContinuousExportServiceRolePolicy

Wenn die AWSApplicationDiscoveryServiceFullAccess Richtlinie an Ihr IAM-Konto angehängt ApplicationDiscoveryServiceContinuousExportServiceRolePolicy ist, wird sie automatisch mit Ihrem Konto verknüpft, wenn Sie die Datenexploration in Amazon Athena aktivieren.

Diese Richtlinie ermöglicht AWS Application Discovery Service die Erstellung von Amazon Data Firehose-Streams zur Transformation und Übertragung von Daten, die von AWS Application Discovery Service Agenten gesammelt wurden, an einen Amazon S3 S3-Bucket in Ihrem AWS Konto.

Darüber hinaus erstellt diese Richtlinie eine AWS Glue Data Catalog mit einer neuen Datenbank namens application_discovery_service_database und Tabellenschemas für die Zuordnung von Daten, die von den Agenten gesammelt wurden. Ein Beispiel für diese Richtlinie finden Sie unter [Erteilen von Berechtigungen für die Erfassung von Agentendaten](#).

AWS verwaltete Richtlinie: AWSDiscovery ContinuousExportFirehosePolicy

Die AWSDiscoveryContinuousExportFirehosePolicy Richtlinie ist erforderlich, um die Datenexploration in Amazon Athena nutzen zu können. Es ermöglicht Amazon Data Firehose, Daten, die vom Application Discovery Service gesammelt wurden, in Amazon S3 zu schreiben. Weitere Informationen zur Verwendung dieser Richtlinie finden Sie unter [Die AWSApplication](#)

[DiscoveryServiceFirehose Rolle erstellen](#). Ein Beispiel für diese Richtlinie finden Sie unter [Erteilung von Berechtigungen für die Datenexploration](#).

Die AWSApplication DiscoveryServiceFirehose Rolle erstellen

Ein Administrator fügt Ihrem IAM-Benutzerkonto verwaltete Richtlinien hinzu. Wenn Sie die `AWSDiscoveryContinuousExportFirehosePolicy` Richtlinie verwenden, muss der Administrator zunächst eine Rolle `AWSApplicationDiscoveryServiceFirehose` mit dem Namen `Firehose` als vertrauenswürdige Entität erstellen und dann die `AWSDiscoveryContinuousExportFirehosePolicy` Richtlinie an die Rolle anhängen, wie im folgenden Verfahren gezeigt.

Um die `AWSApplicationDiscoveryServiceFirehose` IAM-Rolle zu erstellen

1. Wählen Sie in der IAM-Konsole im Navigationsbereich Rollen aus.
2. Wählen Sie Rolle erstellen aus.
3. Wählen Sie Kinesis.
4. Wählen Sie als Ihren Anwendungsfall Kinesis Firehose.
5. Wählen Sie Weiter: Berechtigungen aus.
6. Suchen Sie unter Richtlinien filtern nach `AWSDiscoveryContinuousExportFirehosePolicy`.
7. Wählen Sie das Feld daneben `AWSDiscoveryContinuousExportFirehosePolicy` aus und wählen Sie dann Weiter: Überprüfen aus.
8. Geben Sie `AWSApplicationDiscoveryServiceFirehose` als Rollennamen ein und wählen Sie dann Rolle erstellen aus.

Updates für AWS verwaltete Richtlinien durch den Application Discovery Service

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Application Discovery Service an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der [Dokumentenverlauf für AWS Application Discovery Service](#)-Seite.

Änderungen	Beschreibung	Date
AWSApplicationDiscoveryAgentlessCollectorAccess — Neue Richtlinie, die mit dem Start von Agentless Collector verfügbar gemacht wurde	Der Application Discovery Service hat die neue verwaltete Richtlinie hinzugefügt <code>awsApplicationDiscoveryAgentlessCollectorAccess</code> , die dem Agentless Collector Zugriff auf die Registrierung und Kommunikation mit dem Application Discovery Service sowie die Kommunikation mit anderen AWS Diensten gewährt.	16. August 2022
Application Discovery Service hat mit der Nachverfolgung von Änderungen begonnen	Der Application Discovery Service hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	1. März 2021

AWS Application Discovery Service Beispiele für identitätsbasierte Richtlinien

Standardmäßig sind IAM-Benutzer und -Rollen nicht berechtigt, Application Discovery Service Service-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit der AWS-Managementkonsole, AWS CLI, oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von Richtlinien auf der JSON-Registerkarte](#) im IAM-Benutzerhandbuch.

Themen

- [Best Practices für Richtlinien](#)
- [Vollzugriff auf den Application Discovery Service gewähren](#)
- [Discovery-Agents Zugriff gewähren](#)
- [Erteilen von Berechtigungen für die Erfassung von Agentendaten](#)
- [Erteilung von Berechtigungen für die Datenexploration](#)
- [Erteilen von Berechtigungen zur Verwendung des Netzwerkdiagramms der Migration Hub Hub-Konsole](#)

Best Practices für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Application Discovery Service Service-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) oder [Von AWS verwaltete Richtlinien für Auftragsfunktionen](#) im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können

auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.

- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtlinienvvalidierung mit IAM Access Analyzer](#) im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Sicherer API-Zugriff mit MFA](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Best Practices für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Vollzugriff auf den Application Discovery Service gewähren

Die `AWSApplicationDiscoveryServiceFullAccess` verwaltete Richtlinie gewährt dem IAM-Benutzerkonto Zugriff auf den Application Discovery Service und den Migration Hub APIs.

Ein IAM-Benutzer, dem diese Richtlinie mit seinem Konto verknüpft ist, kann den Application Discovery Service konfigurieren, Agents starten und beenden, die agentenlose Erkennung starten und beenden und Daten aus der AWS Discovery Service-Datenbank abfragen. Weitere Informationen zu dieser Richtlinie finden Sie unter [AWS verwaltete Richtlinien für AWS Application Discovery Service](#).

Example `AWSApplicationDiscoveryServiceFullAccess` Richtlinie

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

        "Action": [
            "mgh:*",
            "discovery:*"
        ],
        "Effect": "Allow",
        "Resource": "*"
    },
    {
        "Action": [
            "iam:GetRole"
        ],
        "Effect": "Allow",
        "Resource": "*"
    }
]
}

```

Discovery-Agents Zugriff gewähren

Die AWSApplication DiscoveryAgentAccess verwaltete Richtlinie gewährt dem Application Discovery Agent Zugriff auf die Registrierung und Kommunikation mit dem Application Discovery Service. Weitere Informationen zu dieser Richtlinie finden Sie unter [AWS verwaltete Richtlinien für AWS Application Discovery Service](#).

Ordnen Sie diese Richtlinie jedem Benutzer zu, dessen Anmeldeinformationen vom Application Discovery Agent verwendet werden.

Diese Richtlinie gewährt dem Benutzer außerdem den Zugriff auf Arsenal. Arsenal ist ein Agentendienst, der von verwaltet und gehostet wird AWS. Arsenal leitet Daten an den Application Discovery Service in der Cloud weiter.

Example AWSApplicationDiscoveryAgentAccess Richtlinie

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [

```

```

        "arsenal:RegisterOnPremisesAgent"
      ],
      "Resource": "*"
    }
  ]
}

```

Erteilen von Berechtigungen für die Erfassung von Agentendaten

Die `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy` verwaltete Richtlinie ermöglicht AWS Application Discovery Service die Erstellung von Amazon Data Firehose-Streams zur Transformation und Übertragung von Daten, die von Application Discovery Service Service-Agenten gesammelt wurden, an einen Amazon S3 S3-Bucket in Ihrem AWS Konto.

Darüber hinaus erstellt diese Richtlinie einen AWS Glue Datenkatalog mit einer neuen Datenbank namens `application_discovery_service_database` und Tabellenschemas für die Zuordnung von Daten, die von den Agenten gesammelt wurden.

Weitere Informationen zur Verwendung dieser Richtlinie finden Sie unter [AWS verwaltete Richtlinien für AWS Application Discovery Service](#).

Example `ApplicationDiscoveryServiceContinuousExportServiceRolePolicy`

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
  ],
}

```

```

    {
      "Action": [
        "firehose:DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-
discovery-service*"
    },
    {
      "Action": [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::aws-application-discovery-service*"
    },
    {
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::aws-application-discovery-service/*/"
    },
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutRetentionPolicy"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-
service/firehose*"
    },
    {
      "Action": [
        "iam:PassRole"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:iam:*:*:role/
AWSApplicationDiscoveryServiceFirehose",

```

```

        "Condition": {
            "StringLike": {
                "iam:PassedToService": "firehose.amazonaws.com"
            }
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
            "Condition": {
                "StringLike": {
                    "iam:PassedToService": "firehose.amazonaws.com"
                }
            }
        }
    ]
}

```

Erteilung von Berechtigungen für die Datenexploration

Die AWSDiscoveryContinuousExportFirehosePolicy Richtlinie ist erforderlich, um die Datenexploration in Amazon Athena nutzen zu können. Es ermöglicht Amazon Data Firehose, Daten, die vom Application Discovery Service gesammelt wurden, in Amazon S3 zu schreiben. Weitere Informationen zur Verwendung dieser Richtlinie finden Sie unter [Die AWSApplicationDiscoveryServiceFirehose Rolle erstellen](#).

Example AWSDiscoveryContinuousExportFirehosePolicy

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "glue:GetTableVersions"
            ]
        }
    ]
}

```

```

    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:AbortMultipartUpload",
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:ListBucket",
      "s3:ListBucketMultipartUploads",
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3::aws-application-discovery-service-*",
      "arn:aws:s3::aws-application-discovery-service-*/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/application-discovery-service/
firehose:log-stream:*"
    ]
  }
]
}

```

Erteilen von Berechtigungen zur Verwendung des Netzwerkdiagramms der Migration Hub Hub-Konsole

Um beim Erstellen einer identitätsbasierten Richtlinie, die den Zugriff auf Application Discovery Service oder Migration Hub erlaubt oder verweigert, Zugriff auf das AWS Migration Hub Konsolen-Netzwerkdiagramm zu gewähren, müssen Sie die `discovery:GetNetworkConnectionGraph` Aktion möglicherweise der Richtlinie hinzufügen.

Sie müssen die `discovery:GetNetworkConnectionGraph` Aktion in neuen Richtlinien verwenden oder ältere Richtlinien aktualisieren, wenn Folgendes für die Richtlinie zutrifft:

- Die Richtlinie erlaubt oder verweigert den Zugriff auf den Application Discovery Service oder den Migration Hub.
- Die Richtlinie gewährt Zugriffsberechtigungen mithilfe einer weiteren spezifischen Discovery-Aktion wie `discovery:action-name` stattdiscovery:*

Das folgende Beispiel zeigt, wie die `discovery:GetNetworkConnectionGraph` Aktion in einer IAM-Richtlinie verwendet wird.

Example

JSON

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

Informationen zum Migration Hub-Netzwerkdiagramm finden Sie unter [Netzwerkverbindungen in Migration Hub anzeigen](#).

Verwenden von dienstverknüpften Rollen für den Application Discovery Service

AWS Application Discovery Service verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte](#) Rollen. Eine dienstverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit dem Application Discovery Service verknüpft ist. Dienstbezogene Rollen sind vom Application Discovery Service vordefiniert und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstverknüpfte Rolle erleichtert die Einrichtung von Application Discovery Service, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Der Application Discovery Service definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert,

kann nur Application Discovery Service seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre Application Discovery Service Service-Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Topics

- [Dienstbezogene Rollenberechtigungen für Application Discovery Service](#)
- [Eine dienstverknüpfte Rolle für den Application Discovery Service erstellen](#)
- [Löschen einer dienstverknüpften Rolle für Application Discovery Service](#)

Informationen zu anderen Services, die serviceverknüpften Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#). Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rolle angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Dienstbezogene Rollenberechtigungen für Application Discovery Service

Der Application Discovery Service verwendet die dienstverknüpfte Rolle mit dem Namen `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`— Ermöglicht den Zugriff auf AWS Dienste und Ressourcen, die von AWS Application Discovery Service verwendet oder verwaltet werden.

Die `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` dienstverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `continuousexport.discovery.amazonaws.com`

Die Rollenberechtigungsrichtlinie ermöglicht es dem Application Discovery Service, die folgenden Aktionen durchzuführen:

glue

CreateDatabase

UpdateDatabase

CreateTable

UpdateTable

firehose

CreateDeliveryStream

DeleteDeliveryStream

DescribeDeliveryStream

PutRecord

PutRecordBatch

UpdateDestination

S3

CreateBucket

ListBucket

GetObject

Protokolle

CreateLogGroup

CreateLogStream

PutRetentionPolicy

iam

PassRole

Dies ist die vollständige Richtlinie, aus der hervorgeht, für welche Ressourcen die oben genannten Aktionen gelten:

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  

```

```

    {
      "Action": [
        "glue:CreateDatabase",
        "glue:UpdateDatabase",
        "glue:CreateTable",
        "glue:UpdateTable",
        "firehose:CreateDeliveryStream",
        "firehose:DescribeDeliveryStream",
        "logs:CreateLogGroup"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "firehose>DeleteDeliveryStream",
        "firehose:PutRecord",
        "firehose:PutRecordBatch",
        "firehose:UpdateDestination"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:firehose:*:*:deliverystream/aws-application-
discovery-service*"
    },
    {
      "Action": [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:PutBucketLogging",
        "s3:PutEncryptionConfiguration"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::aws-application-discovery-service*"
    },
    {
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::aws-application-discovery-service/*"
    },
    {
      "Action": [
        "logs:CreateLogStream",

```

```

        "logs:PutRetentionPolicy"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:logs:*:*:log-group:/aws/application-discovery-
service/firehose*"
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:iam:*:*:role/
AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  },
  {
    "Action": [
      "iam:PassRole"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:iam:*:*:role/service-role/
AWSApplicationDiscoveryServiceFirehose",
    "Condition": {
      "StringLike": {
        "iam:PassedToService": "firehose.amazonaws.com"
      }
    }
  }
]
}

```

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [serviceverknüpfte Rollenberechtigungen](#) im IAM-Benutzerhandbuch.

Eine dienstverknüpfte Rolle für den Application Discovery Service erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Die AWSService RoleForApplicationDiscoveryServiceContinuousExport dienstbezogene Rolle wird automatisch erstellt, wenn Continuous Export implizit aktiviert wird, indem a) die Optionen im Dialogfeld bestätigt werden, das auf der Seite Data Collectors angezeigt wird, nachdem Sie „Datenerfassung starten“ ausgewählt haben, oder indem Sie auf den Schieberegler mit der Bezeichnung „Datenexploration in Athena“ klicken, oder b) wenn Sie die StartContinuousExport API über die CLI aufrufen. AWS

Important

Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Weitere Informationen finden Sie unter [Eine neue Rolle ist in meinem IAM-Konto erschienen](#).

Die serviceverknüpfte Rolle von der Migration Hub Hub-Konsole aus erstellen

Sie können die Migration Hub Hub-Konsole verwenden, um die AWSService RoleForApplicationDiscoveryServiceContinuousExport serviceverknüpfte Rolle zu erstellen.

So erstellen die serviceverknüpfte Rolle (Konsole)

1. Klicken Sie im Navigationsbereich auf Data Collectors (Datensammler).
2. Wählen Sie die Registerkarte Agents (Agenten).
3. Stellen Sie den Schieberegler Datenexploration in Athena auf die Position Ein.
4. Klicken Sie in dem im vorherigen Schritt erstellten Dialogfeld auf das Kontrollkästchen, um sich mit den anfallenden Gebühren einverstanden zu erklären. Klicken Sie dann auf Continue (Fortfahren) oder Enable (Aktivieren).

Erstellen Sie die serviceverknüpfte Rolle aus dem AWS CLI

Sie können Application Discovery Service Service-Befehle von verwenden AWS Command Line Interface , um die AWSService RoleForApplicationDiscoveryServiceContinuousExport dienstverknüpfte Rolle zu erstellen.

Diese dienstverknüpfte Rolle wird automatisch erstellt, wenn Sie Continuous Export über starten AWS CLI (die AWS CLI muss zuerst in Ihrer Umgebung installiert werden).

Um die serviceverknüpfte Rolle (CLI) zu erstellen, indem Sie Continuous Export von der AWS CLI

1. Installieren Sie das AWS CLI für Ihr Betriebssystem (Linux, macOS oder Windows). Anweisungen finden Sie im [AWS Command Line Interface Benutzerhandbuch](#).
2. Öffnen Sie die Eingabeaufforderung (Windows) oder das Terminal (Linux oder macOS).
 - a. Geben Sie `aws configure` ein und drücken Sie die Eingabetaste.
 - b. Geben Sie Ihre AWS Zugangsschlüssel-ID und Ihren AWS geheimen Zugriffsschlüssel ein.
 - c. Geben Sie als standardmäßigen Regionsnamen `us-west-2` ein.
 - d. Geben Sie als Standard-Ausgabeformat `text` ein.
3. Geben Sie den folgenden Befehl ein:

```
aws discovery start-continuous-export
```

Sie können die IAM-Konsole auch verwenden, um eine dienstbezogene Rolle mit dem Anwendungsfall Discovery Service — Continuous Export zu erstellen. Erstellen Sie in der IAM-CLI oder der IAM-API eine serviceverknüpfte Rolle mit dem Servicenamen `continuousexport.discovery.amazonaws.com`. Weitere Informationen finden Sie unter [Erstellen einer serviceverknüpfte Rolle](#) im IAM-Leitfaden. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Löschen einer dienstverknüpften Rolle für Application Discovery Service

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Bereinigen der -serviceverknüpften Rolle

Bevor mit IAM eine serviceverknüpfte Rolle löschen können, müssen Sie zunächst alle von der Rolle verwendeten Ressourcen löschen.

 Note

Wenn der Application Discovery Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie Application Discovery Service Service-Ressourcen, die von der AWSService RoleForApplicationDiscoveryServiceContinuousExport serviceverknüpften Rolle verwendet werden, aus der Migration Hub Hub-Konsole

1. Klicken Sie im Navigationsbereich auf Data Collectors (Datensammler).
2. Wählen Sie die Registerkarte Agents (Agenten).
3. Stellen Sie den Schieberegler Datenexploration in Athena auf die Position Aus.

Um Application Discovery Service Service-Ressourcen zu löschen, die von der AWSService RoleForApplicationDiscoveryServiceContinuousExport serviceverknüpften Rolle verwendet werden, aus dem AWS CLI

1. Installieren Sie das AWS CLI für Ihr Betriebssystem (Linux, macOS oder Windows). Anweisungen finden Sie im [AWS Command Line Interface Benutzerhandbuch](#).
2. Öffnen Sie die Eingabeaufforderung (Windows) oder das Terminal (Linux oder macOS).
 - a. Geben Sie `aws configure` ein und drücken Sie die Eingabetaste.
 - b. Geben Sie Ihre AWS Zugangsschlüssel-ID und Ihren AWS geheimen Zugriffsschlüssel ein.
 - c. Geben Sie als standardmäßigen Regionsnamen `us-west-2` ein.
 - d. Geben Sie als Standard-Ausgabeformat `text` ein.
3. Geben Sie den folgenden Befehl ein:

```
aws discovery stop-continuous-export --export-id <export ID>
```

- Wenn Ihnen die Export-ID des fortlaufenden Exports, den Sie beenden möchten, nicht bekannt ist, geben Sie den folgenden Befehl ein, um die ID des fortlaufenden Exports anzuzeigen:

```
aws discovery describe-continuous-exports
```


4. Geben Sie den folgenden Befehl ein, um sicherzustellen, dass Continuous Export beendet wurde, indem Sie überprüfen, ob der Rückgabestatus „INAKTIV“ lautet:

```
aws discovery describe-continuous-export
```

Manuelles Löschen der serviceverknüpften Rolle

Sie können die `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport` serviceverknüpfte Rolle mithilfe der IAM-Konsole, der IAM-CLI oder der IAM-API löschen. Wenn Sie die Funktionen Discovery Service — Continuous Export, für die diese serviceverknüpfte Rolle erforderlich ist, nicht mehr verwenden müssen, empfehlen wir Ihnen, diese Rolle zu löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Leitfaden.

Note

Sie müssen Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie löschen können. Siehe [Bereinigen der -serviceverknüpften Rolle](#).

Problembehandlung bei AWS Application Discovery Service Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Application Discovery Service und IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, IAM durchzuführen: PassRole](#)

Ich bin nicht berechtigt, IAM durchzuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an den Application Discovery Service übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion im Application Discovery Service auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Protokollieren von API-Aufrufen des Application Discovery Service mit AWS CloudTrail

AWS Application Discovery Service ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Application Discovery Service ausgeführt wurden. Sie können CloudTrail damit Kontoaktivitäten zu Problembehebungs- und Prüfungszwecken protokollieren, kontinuierlich überwachen und speichern. CloudTrail bietet einen Ereignisverlauf Ihrer AWS Kontoaktivitäten, einschließlich der über die AWS Managementkonsole durchgeführten Aktionen und Befehlszeilentools. AWS SDKs

CloudTrail erfasst alle API-Aufrufe für den Application Discovery Service als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Application Discovery Service-Konsole und Codeaufrufen für die API-Operationen des Application Discovery Service.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für den Application Discovery Service. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an den Application Discovery Service, die IP-

Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

Informationen zum Application Discovery Service in CloudTrail

CloudTrail ist für Ihr AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn eine Aktivität im Application Discovery Service auftritt, wird diese Aktivität zusammen mit anderen CloudTrail AWS Dienstereignissen im Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem AWS Konto, einschließlich Ereignissen für den Application Discovery Service, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail Unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Alle Application Discovery Service-Aktionen werden von der [Application Discovery Service API-Referenz](#) protokolliert CloudTrail und sind in dieser Dokumentation dokumentiert. Beispielsweise generieren Aufrufe der GetDiscoverySummary Aktionen CreateTagsDescribeTags, und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.

- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter [CloudTrail userIdentity-Element](#).

Grundlegendes zu den Protokolldateieinträgen des Application Discovery Service

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die DescribeTags Aktion demonstriert.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AR0AJBHC4H6EKEXAMPLE:sample-user",
    "arn": "arn:aws:sts::444455556666:assumed-role/ReadOnly/sample-user",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDAJQABLZS4A3QDU576Q",
        "arn": "arn:aws:iam::444455556666:role/ReadOnly",
        "accountId": "444455556666",
        "userName": "sampleAdmin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-05-05T15:19:03Z"
      }
    }
  }
}
```

```
    }
  },
  "eventTime": "2020-05-05T17:02:40Z",
  "eventSource": "discovery.amazonaws.com",
  "eventName": "DescribeTags",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "20.22.33.44",
  "userAgent": "Coral/Netty4",
  "requestParameters": {
    "maxResults": 0,
    "filters": [
      {
        "values": [
          "d-server-0315rfdjreyqsq"
        ],
        "name": "configurationId"
      }
    ]
  },
  "responseElements": null,
  "requestID": "mgh-console-eb1cf315-e2b4-4696-93e5-b3a3b9346b4b",
  "eventID": "7b32b778-91c9-4c75-9cb0-6c852791b2eb",
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```

AWS Application Discovery Service ARN-Formate

Ein Amazon-Ressourcenname (ARN) ist eine Zeichenfolge, die eine AWS Ressource eindeutig identifiziert. AWS erfordert einen ARN, wenn Sie eine Ressource für alle eindeutig angeben möchten. AWS Application Discovery Service definiert Folgendes. ARNs

- Discovery-Agent: `arn:aws:discovery:region:account:agent/discovery-agent/agentId`
- Sammler ohne Agenten: `arn:aws:discovery:region:account:agent/agentless-collector/agentId`
- Sammler zur Bewertung von Migration: `arn:aws:discovery:region:account:agent/migration-evaluator-collector/agentId`
- Discovery-Konnektor: `arn:aws:discovery:region:account:agent/discovery-connector/agentId`

AWS Application Discovery Service Kontingente

Die Service Quotas Quotas-Konsole bietet Informationen zu AWS Application Discovery Service Kontingenten. Sie können die Servicekontingenten-Konsole verwenden, um die Standard-Servicekontingenten einzusehen oder um [Kontingenterhöhungen für anpassbare Kontingente anzufordern](#).

Derzeit sind importierte Server pro Konto das einzige Kontingent, das erhöht werden kann.

Der Application Discovery Service hat die folgenden Standardkontingente:

- 1.000 Anwendungen pro Konto.

Wenn Sie dieses Kontingent erreichen und neue Anwendungen importieren möchten, können Sie vorhandene Anwendungen mit der `DeleteApplications` API-Aktion löschen. Weitere Informationen finden Sie [DeleteApplications](#) in der API-Referenz für den Application Discovery Service.

- Jede Importdatei kann eine maximale Dateigröße von 10 MB haben.
- 25.000 importierte Serverdatensätze pro Konto.
- 25.000 Löschungen von Importdatensätzen pro Tag.
- 10.000 importierte Server pro Konto (Sie können eine Erhöhung dieses Kontingents beantragen).
- 1.000 aktive Agenten, die Daten sammeln und an den Application Discovery Service senden.
- 10.000 inaktive Agenten, die zwar reagieren, aber keine Daten sammeln.
- 400 Server pro Anwendung.
- 30 Tags pro Server.

Fehlerbehebung AWS Application Discovery Service

In diesem Abschnitt finden Sie Informationen dazu, wie häufige Probleme mit AWS Application Discovery Service behoben werden.

Themen

- [Stoppen Sie die Datenerfassung durch Datenerkundung](#)
- [Entfernen Sie die bei der Datenerkundung gesammelten Daten](#)
- [Beheben Sie häufig auftretende Probleme bei der Datenexploration in Amazon Athena](#)
- [Fehlerbehebung bei fehlgeschlagenen Datensätzen](#)

Stoppen Sie die Datenerfassung durch Datenerkundung

Um die Datenexploration zu beenden, können Sie entweder den Kippschalter in der Migration Hub Hub-Konsole unter Discover > Data Collectors > Agents ausschalten oder die `StopContinuousExport` API aufrufen. Es kann bis zu 30 Minuten dauern, bis die Datenerfassung beendet ist. Während dieser Phase wird auf dem Kippschalter an der Konsole und beim `DescribeContinuousExport` API-Aufruf der Status „Stopp In Progress“ angezeigt.

Note

Wenn sich der Schalter nach dem Aktualisieren der Konsolenseite nicht ausschaltet und eine Fehlermeldung ausgegeben wird oder die `DescribeContinuousExport` API den Status „Stop_Failed“ zurückgibt, können Sie es erneut versuchen, indem Sie den Kippschalter ausschalten oder die API aufrufen. `StopContinuousExport` Wenn die „Datenexploration“ weiterhin einen Fehler anzeigt und nicht erfolgreich beendet werden kann, wenden Sie sich bitte an den AWS Support.

Alternativ können Sie die Datensammlung manuell beenden, wie in den folgenden Schritten beschrieben.

Option 1: Beenden der Agent-Datensammlung

Wenn Sie die Erkennung bereits mit ADS-Agenten durchgeführt haben und im ADS Datenbank-Repository keine weiteren Daten mehr sammeln möchten:

1. Wählen Sie in der Migration Hub Hub-Konsole Discover > Data Collectors > Agents aus.
2. Wählen Sie alle vorhandenen laufenden Agenten aus und klicken Sie auf Stop Data Collection (Beenden der Datensammlung).

Dadurch wird sichergestellt, dass von den Agenten sowohl im ADS-Daten-Repository als auch in Ihrem S3-Bucket keine neuen Daten gesammelt werden. Ihre vorhandenen Daten bleiben verfügbar.

Option 2: Amazon Kinesis Data Streams von Data Exploration löschen

Wenn Sie weiterhin Daten von Agenten im ADS-Daten-Repository sammeln möchten, aber keine Daten in Ihrem Amazon S3 S3-Bucket mithilfe der Datenexploration sammeln möchten, können Sie die Amazon Data Firehose-Streams, die durch die Datenexploration erstellt wurden, manuell löschen:

1. Melden Sie sich über die AWS Konsole bei Amazon Kinesis an und wählen Sie im Navigationsbereich Data Firehose aus.
2. Löschen Sie die folgenden Streams, die mit der Funktion zur Datenerkundung erstellt wurden:
 - aws-application-discovery-service-id_mapping_agent
 - aws-application-discovery-service-inbound_connection_agent
 - aws-application-discovery-service-network_interface_agent
 - aws-application-discovery-service-os_info_agent
 - aws-application-discovery-service-outbound_connection_agent
 - aws-application-discovery-service-processes_agent
 - aws-application-discovery-service-sys_performance_agent

Entfernen Sie die bei der Datenerkundung gesammelten Daten

Um Daten zu entfernen, die bei der Datenexploration gesammelt wurden

1. Entfernen Sie die in Amazon S3 gespeicherten Discovery Agent-Daten.

Daten, die von AWS Application Discovery Service (ADS) gesammelt wurden, werden in einem S3-Bucket mit dem Namen gespeichert `aws-application-discover-discovery-service-uniqueid`.

 Note

Das Löschen des Amazon S3 S3-Buckets oder eines der Objekte darin, während die Datenexploration in Amazon Athena aktiviert ist, führt zu einem Fehler. Es sendet weiterhin neue Discovery-Agent-Daten an S3. Die gelöschten Daten werden auch in Athena nicht mehr zugänglich sein.

2. Entfernen AWS Glue Data Catalog.

Wenn die Datenexploration in Amazon Athena aktiviert ist, wird in Ihrem Konto ein Amazon S3 S3-Bucket erstellt, in dem die von ADS-Agenten in regelmäßigen Zeitabständen gesammelten Daten gespeichert werden. Darüber hinaus wird eine AWS Glue Data Catalog erstellt, mit der Sie die in einem Amazon S3-Bucket gespeicherten Daten von Amazon Athena abfragen können. Wenn Sie die Datenexploration in Amazon Athena deaktivieren, werden keine neuen Daten in Ihrem Amazon S3 S3-Bucket gespeichert, aber Daten, die zuvor gesammelt wurden, bleiben bestehen. Wenn Sie diese Daten nicht mehr benötigen und Ihr Konto in den Zustand zurückversetzen möchten, in dem die Datenexploration in Amazon Athena aktiviert wurde.

- a. Rufen Sie Amazon S3 von der AWS Konsole aus auf und löschen Sie manuell den Bucket mit dem Namen „aws-application-discovery-service-uniqueid“
- b. Sie können den AWS Glue Data Catalog zur Datenexploration manuell entfernen, indem Sie die Application-Discovery-Service-Database-Datenbank und all diese Tabellen löschen:
 - os_info_agent
 - network_interface_agent
 - sys_performance_agent
 - processes_agent
 - inbound_connection_agent
 - outbound_connection_agent
 - id_mapping_agent

Entfernen Sie Ihre Daten von AWS Application Discovery Service

Um all Ihre Daten aus dem Application Discovery Service entfernen zu lassen, wenden Sie sich an den [AWS Support](#) und fordern Sie die vollständige Datenlöschung an.

Beheben Sie häufig auftretende Probleme bei der Datenexploration in Amazon Athena

In diesem Abschnitt finden Sie Informationen zur Behebung häufiger Probleme bei der Datenexploration in Amazon Athena.

Themen

- [Die Datenexploration in Amazon Athena kann nicht initiiert werden, da serviceverknüpfte Rollen erforderlich sind AWS Ressourcen können nicht erstellt werden](#)
- [Neue Agentendaten werden in Amazon Athena nicht angezeigt](#)
- [Sie verfügen nicht über ausreichende Berechtigungen für den Zugriff auf Amazon S3, Amazon Data Firehose oder AWS Glue](#)

Die Datenexploration in Amazon Athena kann nicht initiiert werden, da serviceverknüpfte Rollen erforderlich sind AWS Ressourcen können nicht erstellt werden

Wenn Sie die Datenexploration in Amazon Athena aktivieren, wird in Ihrem Konto die serviceverknüpfte Rolle `AWSServiceRoleForApplicationDiscoveryServiceContinuousExport`, die es ihr ermöglicht, die erforderlichen AWS Ressourcen zu erstellen, um die vom Agenten gesammelten Daten in Amazon Athena zugänglich zu machen, einschließlich eines Amazon S3 S3-Buckets, Amazon Kinesis Kinesis-Streams und. AWS Glue Data Catalog Wenn Ihr Konto nicht über die erforderlichen Berechtigungen für die Datenexploration in Amazon Athena verfügt, um diese Rolle zu erstellen, kann sie nicht initialisiert werden. Weitere Informationen finden Sie unter [AWS verwaltete Richtlinien für AWS Application Discovery Service](#).

Neue Agentendaten werden in Amazon Athena nicht angezeigt

Wenn keine neuen Daten in Athena fließen, es mehr als 30 Minuten her ist, dass ein Agent gestartet wurde und der Status der Datenexploration Aktiv lautet, überprüfen Sie die unten aufgeführten Lösungen:

- AWS Discovery-Agenten

Stellen Sie sicher, dass der Status Collection (Sammlung) des Agenten als Started (Gestartet) und der Status Health (Zustand) als Running (Läuft) markiert ist.

- Kinesis-Rolle

Stellen Sie sicher, dass Sie in Ihrem Konto über die Rolle `AWSApplicationDiscoveryServiceFirehose` verfügen.

- Firehose-Status

Stellen Sie sicher, dass die Firehose Firehose-Lieferstreams ordnungsgemäß funktionieren:

- `aws-application-discovery-service/os_info_agent`
- `aws-application-discovery-service-network_interface_agent`
- `aws-application-discovery-service-sys_performance_agent`
- `aws-application-discovery-service-processes_agent`
- `aws-application-discovery-service-inbound_connection_agent`
- `aws-application-discovery-service-outbound_connection_agent`
- `aws-application-discovery-service-id_mapping_agent`

- AWS Glue Data Catalog

Stellen Sie sicher, dass die `application-discovery-service-database` Datenbank vorhanden ist. AWS Glue Stellen Sie sicher, dass die folgenden Tabellen in AWS Glue vorhanden sind:

- `os_info_agent`
- `network_interface_agent`
- `sys_performance_agent`
- `processes_agent`
- `inbound_connection_agent`
- `outbound_connection_agent`
- `id_mapping_agent`

- ~~Amazon S3 Bucket~~

Neue Agentendaten werden in Amazon Athena nicht angezeigt

Stellen Sie sicher, dass `aws-application-discovery-service-uniqueid` in Ihrem Konto ein Amazon S3 S3-Bucket benannt ist. Wenn Objekte im Bucket verschoben oder gelöscht wurden, werden sie in Athena nicht richtig angezeigt.

- Ihre lokalen Server

Stellen Sie sicher, dass Ihre Servern ausgeführt werden, sodass Ihr Agenten Daten sammeln und zu AWS Application Discovery Service senden können.

Sie verfügen nicht über ausreichende Berechtigungen für den Zugriff auf Amazon S3, Amazon Data Firehose oder AWS Glue

Wenn Sie Amazon Athena verwenden AWS Organizations und die Initialisierung für die Datenexploration in Amazon Athena fehlschlägt, kann dies daran liegen, dass Sie keine Zugriffsberechtigungen für Amazon S3, Amazon Data Firehose, Athena oder haben. AWS Glue

Sie benötigen einen IAM-Benutzer mit Administratorrechten, um Ihnen Zugriff auf diese Dienste zu gewähren. Ein Administrator kann diesen Zugriff über sein Konto gewähren. Siehe [AWS verwaltete Richtlinien für AWS Application Discovery Service](#).

Um sicherzustellen, dass die Datenexploration in Amazon Athena ordnungsgemäß funktioniert, dürfen Sie die AWS Ressourcen, die durch die Datenexploration in Amazon Athena erstellt wurden, einschließlich des Amazon S3-Buckets, Amazon Data Firehose Streams und, nicht ändern oder löschen. AWS Glue Data Catalog Wenn Sie diese Ressourcen versehentlich löschen oder ändern, können Sie Data Exploration anhalten und wieder fortsetzen, damit diese Ressourcen automatisch erneut erstellt werden. Wenn Sie den Amazon S3 S3-Bucket löschen, der durch Datenexploration erstellt wurde, verlieren Sie möglicherweise die Daten, die im Bucket gesammelt wurden.

Fehlerbehebung bei fehlgeschlagenen Datensätzen

Mit dem Migration Hub-Import können Sie Details Ihrer lokalen Umgebung direkt in Migration Hub importieren, ohne den Discovery Connector oder Discovery Agent zu verwenden. Dadurch haben Sie die Möglichkeit, die Migrationsprüfung und -planung direkt von Ihren importierten Daten aus durchzuführen. Sie können auch Ihre Geräte als Anwendungen gruppieren und deren Migrationsstatus nachverfolgen.

Wenn Sie Daten importieren, ist es möglich, dass Fehler auftreten. Typischerweise treten diese Fehler aus einem der folgenden Gründe auf:

- Ein importbezogenes Kontingent wurde erreicht — Mit Importaufgaben ist ein Kontingent verknüpft. Wenn Sie eine Importaufgabenanfrage stellen, die die Kontingente überschreiten würde, schlägt die Anfrage fehl und es wird ein Fehler zurückgegeben. Weitere Informationen finden Sie unter [AWS Application Discovery Service Kontingente](#).
- Ein zusätzliches Komma (,) wurde in die Importdatei eingefügt — Kommas in CSV-Dateien werden verwendet, um ein Feld vom nächsten zu unterscheiden. Kommata in einem Feld werden nicht unterstützt, da das Feld dadurch immer geteilt wird. Dies kann zu einer Kaskade von Formatierungsfehlern führen. Stellen Sie sicher, dass Kommata nur zwischen Feldern und nicht in anderer Weise in Ihren Importdateien verwendet werden.
- Ein Feld hat einen Wert außerhalb seines unterstützten Bereichs — Manche Felder, wie z. B., `CPU.NumberOfCores` müssen einen Wertebereich haben, den sie unterstützen. Wenn Sie der unterstützte Bereich unter- oder überschritten wird, wird der Datensatz nicht importiert.

Wenn bei Ihrer Importanfrage Fehler auftreten, können Sie diese beheben, indem Sie die fehlgeschlagenen Datensätze für Ihre Importaufgabe herunterladen, die Fehler in der CSV-Datei mit den fehlgeschlagenen Einträgen beheben und den Import erneut durchführen.

Console

So laden Sie das Archiv mit Ihren fehlgeschlagenen Datensätzen herunter:

1. Melden Sie sich bei an und öffnen Sie die Migration Hub Hub-Konsole unter <https://console.aws.amazon.com/migrationhub>. AWS-Managementkonsole
2. Wählen Sie im Navigationsbereich links unter Discover (Entdecken) die Option Tools.
3. Wählen Sie unter Discovery Tools die Option view imports (Importe anzeigen).
4. Wählen Sie im Imports (Importe) -Dashboard das mit einer Importanfrage verbundene Optionsfeld mit einer Anzahl von Failed records (Fehlgeschlagenen Datensätzen).
5. Wählen Sie Download failed records (Fehlgeschlagene Datensätze herunterladen) aus der Tabelle auf dem Dashboard aus. Dadurch wird das Download-Dialogfeld Ihres Browsers für den Download der Archivdatei geöffnet.

AWS CLI

So laden Sie das Archiv mit Ihren fehlgeschlagenen Datensätzen herunter:

1. Öffnen Sie ein Terminalfenster, und geben Sie den folgenden Befehl ein, wobei *ImportName* is the name of the import task with the failed entries that you want to correct.:

```
aws discovery describe-import-tasks - -name ImportName
```

2. Kopieren Sie aus der Ausgabe den gesamten Inhalt der für `errorsAndFailedEntriesZip` zurückgegebenen Wertes ohne die Anführungszeichen.
3. Öffnen Sie einen Webbrowser, fügen Sie den Inhalt in das URL-Textfeld ein, und betätigen Sie ENTER. Dadurch wird das Archiv der fehlgeschlagenen Datensätze im komprimierten .zip-Format heruntergeladen.

Nachdem Sie nun Ihr Archiv fehlgeschlagener Datensätze heruntergeladen haben, können Sie die beiden Dateien darin extrahieren und die Fehler korrigieren. Beachten Sie: Wenn Ihre Fehler durch servicebasierte Einschränkungen verursacht wurden, müssen Sie entweder eine Erweiterung dieser Beschränkungen beantragen oder eine ausreichende Menge der entsprechenden Ressourcen löschen, damit Ihr Konto die Grenzwerte wieder einhält. Das Archiv enthält die folgenden Dateien:

- `errors-file.csv` — Diese Datei ist Ihr Fehlerprotokoll und zeichnet die Zeile, den Spaltennamen und eine beschreibende Fehlermeldung für jeden fehlgeschlagenen Datensatz jedes fehlgeschlagenen Eintrags auf. `ExternalId`
- `failed-entries-file.csv` — Diese Datei enthält nur die fehlgeschlagenen Einträge aus Ihrer ursprünglichen Importdatei.

Verwenden Sie zur Korrektur der nicht auf Einschränkungen basierenden Fehler die Datei `errors-file.csv` zur Behebung der Probleme in der Datei `failed-entries-file.csv`, und importieren Sie diese dann. Eine Anleitung zum Importieren dieser Dateien finden Sie unter [Importieren von Daten](#).

Dokumentenverlauf für AWS Application Discovery Service

Letzte Aktualisierung der Dokumentation zum Benutzerhandbuch: 16. Mai 2023

In der folgenden Tabelle werden wichtige Änderungen am Application Discovery Service Service-Benutzerhandbuch nach dem 18. Januar 2019 beschrieben. Um Benachrichtigungen über Dokumentationsaktualisierungen zu erhalten, können Sie den RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Wartungsmodus	AWS Der Application Discovery Service steht Neukunden nicht mehr zur Verfügung. Verwenden Sie alternativ eines AWS Transform , das ähnliche Funktionen bietet. Weitere Informationen finden Sie unter Änderung der Verfügbarkeit von AWS Application Discovery Service .	7. November 2025
Übergang von Discovery Connector zu Agentless Collector	Wir empfehlen Kunden, die derzeit Discovery Connector verwenden, auf den neuen Agentless Collector umzusteigen. Ab dem 17. November 2025 AWS Application Discovery Service werden keine neuen Daten von Discovery Connectors mehr akzeptiert. Weitere Informationen finden Sie unter Discovery Connector .	12. November 2024
Das Agentless Collector Network Data Collector-Modul	Das Modul Network Data Collection ermöglicht es Ihnen,	8. November 2024

[zur Erfassung von Netzwerkdaten wurde veröffentlicht](#)

Abhängigkeiten zwischen Servern in Ihrem lokalen Rechenzentrum zu ermitteln. Weitere Informationen finden Sie unter [Verwenden des Netzwerkdatenerfassungsmoduls von Agentless Collector](#).

[Support für die Erfassung ohne Agenten für die Zuordnung von Abhängigkeiten](#)

Weitere Informationen finden Sie unter [Verwenden des VMware vCenter Agentless Collector-Datenerfassungsmoduls](#).

24. Oktober 2024

[Agentless Collector Version 2 auf Basis von Amazon Linux 2023 veröffentlicht](#)

Weitere Informationen finden Sie unter [Voraussetzungen für Agentless Collector](#).

26. September 2024

[Die Voraussetzungen für Agentless Collector wurden aktualisiert](#)

Weitere Informationen finden Sie unter [Voraussetzungen für Agentless Collector](#).

9. September 2024

[Eventuelle Konsistenz in der API](#)

Weitere Informationen finden Sie unter [Eventuelle Konsistenz in der AWS Application Discovery Service API](#).

20. Juni 2024

[Agentless Collector-Aktualisierungen](#)

Wir haben `sts.amazonaws.com` die Liste der Domains, für die ausgehender Zugriff erforderlich ist, erweitert. Weitere Informationen finden Sie unter [Firewall für ausgehenden Zugriff auf AWS-Domänen konfigurieren](#).

20. Juni 2024

[Um den Zugriff zu trennen, erstellen und verwenden Sie separate AWS-Konten.](#)

Weitere Informationen finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für AWS Application Discovery Service.](#)

5. April 2024

[Wir stellen das Agentless Collector Datenbank- und Analysedatenerfassungsmodul vor](#)

Das Modul zur Erfassung von Datenbank- und Analysedaten ist das neue Modul von Application Discovery Service Agentless Collector (Agentless Collector). Mit diesem Datenerfassungsmodul können Sie eine Verbindung zu Ihrer Umgebung herstellen und Metadaten und Leistungsmetriken von Ihren lokalen Datenbank- und Analyseservern sammeln. Weitere Informationen finden Sie unter [Modul zur Erfassung von Datenbank- und Analysedaten.](#)

16. Mai 2023

[Wir stellen vor: Application Discovery Service Agentless Collector](#)

Application Discovery Service Agentless Collector (Agentless Collector) ist die neue AWS Application Discovery Service lokale Anwendung, die mithilfe agentenloser Methoden Informationen über Ihre lokale Umgebung sammelt, um Sie bei der effektiven Planung Ihrer Migration zu unterstützen. AWS Cloud [Weitere Informationen finden Sie unter Agentless Collector.](#)

16. August 2022

[IAM-Update](#)

Die `discovery:GetNetworkConnectionGraph` Aktion AWS Identity and Access Management (IAM) ist jetzt verfügbar, um beim Erstellen einer identitätsbasierten Richtlinie Zugriff auf das AWS Migration Hub Konsolen-Netzwerkdiagramm zu gewähren. Weitere Informationen finden Sie unter [Erteilen von Berechtigungen zur Verwendung des Netzwerkdiagramms.](#)

24. Mai 2022

[Wir stellen vor: Die Heimatregion](#)

Die Heimatregion des Migration Hub bietet ein zentrales Repository mit Informationen zur Erkennung und Migrationsplanung für Ihr gesamtes Portfolio sowie eine zentrale Ansicht der Migrationen in mehrere AWS Regionen.

20. November 2019

[Einführung in die Importfunktion von Migration Hub](#)

Mit dem Migration Hub-Import können Sie Informationen über Ihre lokalen Server und Anwendungen in Migration Hub importieren, einschließlich Serverspezifikationen und Nutzungsdaten. Sie können diese Daten auch verwenden, um den Status der Anwendungsmigrationen zu verfolgen. Weitere Informationen finden Sie unter [Migration Hub Hub-Import](#).

18. Januar 2019

In der folgenden Tabelle werden Dokumentationsversionen für das Application Discovery Service User Guide vor dem 18. Januar 2019 beschrieben:

Änderungen	Beschreibung	Date
Neues Feature	Die Dokumente wurden aktualisiert, um die Datenexploration in Amazon Athena zu unterstützen, und es wurde ein Kapitel zur Fehlerbehebung hinzugefügt.	09. August 2018

Änderungen	Beschreibung	Date
Hauptrevidierung	Details zur Nutzung und Ausgabe wurden umgeschrieben; das gesamte Dokument wurde umstrukturiert.	25. Mai 2018
Discovery Agent 2.0	Ein neuer und verbesserter Application Discovery-Agent wurde veröffentlicht.	19. Oktober 2017
Konsole	Das AWS-Managementkonsole wurde hinzugefügt.	19. Dezember 2016
Agentenlose Erkennung	In dieser Version wird beschrieben, wie die agentenlose Erkennung eingerichtet und konfiguriert wird.	28. Juli 2016
Neue Details für Microsoft Windows Server und Korrekturen für Probleme mit Befehlen	Dieses Update bietet neue Details zu Microsoft Windows Server. Es dokumentiert auch Korrekturen verschiedener Probleme mit Befehlen.	20. Mai 2016
Erste Veröffentlichung	Dies ist die erste Version des Application Discovery Service User Guide.	12. Mai 2016

AWS Glossar

Die neueste AWS Terminologie finden Sie im [AWS Glossar](#) in der AWS-Glossar Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.