관리 설명서

AWS AppFabric

AWS AppFabric: 관리 설명서

Table of Contents

AWS AppFabric이란 무엇인가요?

AWS AppFabric은 조직 전체에서 서비스형 소프트웨어(SaaS) 애플리케이션을 빠르게 연결하므로 IT 및 보안 팀은 표준 스키마를 사용하여 애플리케이션을 쉽게 관리하고 보호할 수 있으며 직원은 생성형 AI를 사용하여 일상적인 작업을 더 빠르게 완료할 수 있습니다.

주제

Products

AWS AppFabric의 두 가지 측면, 즉 간소화된 관리 및 보안을 위해 설계된 AppFabric for security와 생성형 AI 기능으로 향상된 생산성을 위한 AppFabric(미리 보기)을 살펴보세요. 자세한 내용은 다음 항목을 참조하세요.

- AWS AppFabric for security란 무엇인가요?
- 생산성을 위한 AWS AppFabric이란 무엇입니까?

이점

AppFabric 앱을 사용하면 다음 작업을 수행할 수 있습니다.

- 몇 분 만에 애플리케이션을 연결하고 운영 비용을 절감할 수 있습니다.
- SaaS 애플리케이션 데이터에 대한 가시성을 높여 보안 태세를 강화합니다.
- 생성형 AI로 애플리케이션 전반에 걸쳐 자동으로 작업을 촉진할 예정입니다.

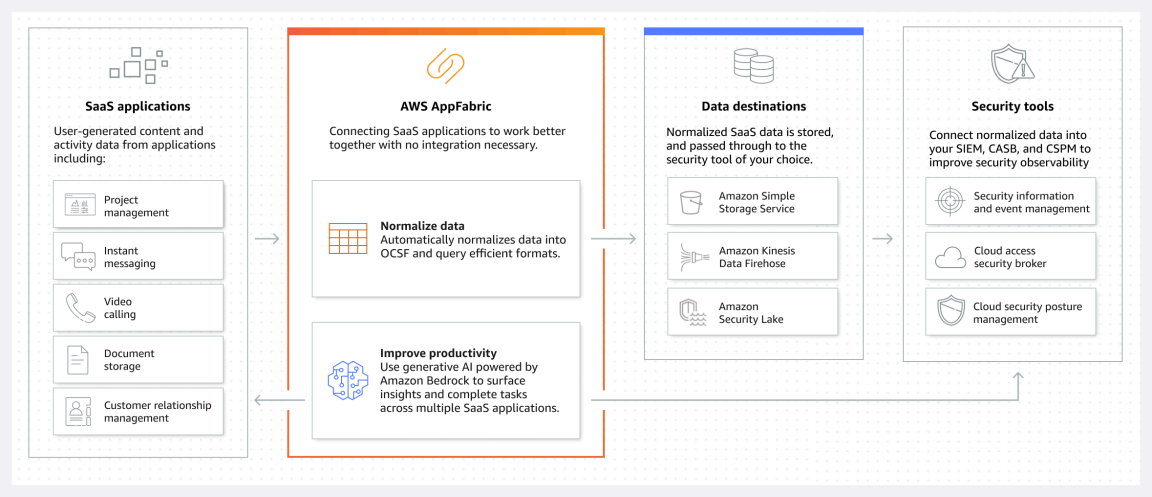
사용 사례

AppFabric으로 다음을 수행할 수 있습니다.

- SaaS 애플리케이션을 빠르게 연결
  - AppFabric for security는 최상위 SaaS 생산성 및 보안 애플리케이션을 서로 기본적으로 연결하여 완벽하게 관리되는 SaaS 상호 운용성 솔루션을 제공합니다.
- 보안 태세 강화
  - 애플리케이션 데이터가 자동으로 정규화되므로 관리자는 공통 정책을 설정하고, 보안 알림을 표준화하고, 여러 애플리케이션에서 사용자 액세스를 쉽게 관리할 수 있습니다.
- 생산성의 재구상
  - AppFabric for security는 일반적인 생성형 AI 어시스턴트를 통해 직원들이 신속하게 답변을 얻고, 작업 관리를 자동화하고, SaaS 생산성 애플리케이션 전반에서 인사이트를 확보할 수 있도록 지원합니다.

AppFabric 작동 방식

AppFabric은 생산성과 보안 향상을 위해 코딩이 필요하지 않은 여러 SaaS 애플리케이션을 빠르게 연결합니다. 다음 다이어그램은 AppFabric의 이점을 보여 줍니다.



> **Note**
>
> 생산성을 위한 AppFabric은 현재 평가판으로 출시되었으며 미국 동부(버지니아 북부) AWS 리전에서 사용할 수 있습니다. 에 대한 자세한 내용은의 AppFabric 엔드포인트 및 할당량을 AWS 리전참조하세요AWS 일반 참조. AWS AppFabric

가격 책정

AppFabric 요금 세부 정보 및 예제는 AWS AppFabric 요금을 참조하십시오.

가용성

AppFabric에 대해 현재 지원되는 AWS 리전 및 엔드포인트를 보려면 AWS 일반 참조의 AWS AppFabric 엔드포인트 및 할당량을 참조하세요.

AWS AppFabric for security란 무엇인가요?

AWS AppFabric for security는 조직 전체에서 서비스형 소프트웨어(SaaS) 애플리케이션을 빠르게 연결하므로 IT 및 보안 팀은 표준 스키마를 사용하여 애플리케이션을 쉽게 관리하고 보호할 수 있습니다.

주제

이점

AppFabric for security를 사용하여 다음을 수행할 수 있습니다.

- 몇 분 만에 애플리케이션을 연결하고 운영 비용을 절감할 수 있습니다.
- SaaS 애플리케이션 데이터에 대한 가시성을 높여 보안 태세를 강화합니다.

사용 사례

AppFabric for security를 다음에 사용할 수 있습니다.

- SaaS 애플리케이션을 빠르게 연결
  - AppFabric for security는 최상위 SaaS 생산성 및 보안 애플리케이션을 서로 기본적으로 연결하여 완벽하게 관리되는 SaaS 상호 운용성 솔루션을 제공합니다.
- 보안 태세 강화

- 애플리케이션 데이터가 자동으로 정규화되므로 관리자는 공통 정책을 설정하고, 보안 알림을 표준화하고, 여러 애플리케이션에서 사용자 액세스를 쉽게 관리할 수 있습니다.

AppFabric for security에 액세스

AppFabric for security는 미국 동부(버지니아 북부), 유럽(아일랜드) 및 아시아 태평양(도쿄)에서 사용할 수 있습니다 AWS 리전. 에 대한 자세한 내용은의 AppFabric 엔드포인트 및 할당량을 AWS 리전참조하세요AWS 일반 참조. AWS AppFabric

각 리전에서 다음 방법 중 하나를 사용하여 AppFabric for security에 액세스할 수 있습니다.

AWS Management Console

는 리소스를 생성하고 관리하는 AWS 데 사용할 수 있는 브라우저 기반 인터페이스 AWS Management Console 입니다. AppFabric 콘솔은 AppFabric 리소스에 대한 액세스를 제공합니다. AppFabric 콘솔을 사용하여 모든 AppFabric 리소스를 생성하고 관리할 수 있습니다.

AppFabric API

AppFabric에 프로그래밍 방식으로 액세스하려면 AppFabric API를 사용하고 HTTPS 요청을 서비스에 직접 발급합니다. 자세한 내용을 알아보려면 AWS AppFabric API 참조를 참조하십시오.

AWS Command Line Interface (AWS CLI)

를 사용하면 시스템의 명령줄에서 명령을 실행하여 AppFabric 및 기타와 상호 작용 AWS CLI할 수 있습니다 AWS 서비스. 태스크를 수행하는 스크립트를 작성하려면 명령줄 도구도 유용합니다. 설치 및 사용에 대한 자세한 내용은 버전 2 사용 설명서를 AWS CLI참조하세요. AWS Command Line Interface AppFabric AWS CLI 명령에 대한 자세한 내용은 참조의 AppFabric 섹션을 참조하세요 AWS CLI.

관련 서비스

AWS 서비스 AppFabric for security에서 다음을 사용할 수 있습니다.

Amazon Data Firehose

Amazon Data Firehose는 스트리밍 데이터를 안정적으로 캡처하고 변환하여 데이터 레이크, 데이터 스토어 및 분석 서비스에 제공하는 추출, 변환 및 로드(ETL) 서비스입니다. AppFabric을 사용하는 경우 Open Cybersecurity Schema Framework(OCSF) 정규화 또는 원시 감사 로그를 대상으로 Firehose 스트림에 JSON 형식으로 출력하도록 선택할 수 있습니다. 자세한 내용은 Firehose에서 출력 위치 생성을 참조하세요.

Amazon Security Lake

Amazon Security Lake는 AWS 환경, SaaS 공급자, 온프레미스 및 클라우드 소스의 보안 데이터를 계정에 저장된 전용 데이터 레이크로 자동으로 중앙 집중화합니다. Amazon Data Firehose를 대상으로 선택하고 Security Lake에서 올바른 형식과 경로로 데이터를 전송하도록 Firehose를 구성하여 AppFabric 감사 로그 데이터를 Security Lake와 통합할 수 있습니다. 자세한 내용은 Amazon Security Lake 사용 설명서의 사용자 지정 소스에서 데이터 수집을 참조하십시오.

Amazon Simple Storage Service

Amazon Simple Storage Service(S3)는 업계 최고의 확장성, 데이터 가용성, 보안 및 성능을 제공하는 객체 스토리지 서비스입니다. AppFabric을 사용하는 경우 대상으로 새 또는 기존 Amazon S3 버킷에 OCSF 정규화(JSON 또는 Apache Parquet) 또는 원시(JSON) 감사 로그를 출력하도록 선택할 수 있습니다. 자세한 내용을 알아보려면 Amazon S3에서 출력 위치 생성을 참조하십시오.

Amazon Quick

Quick은 대규모 통합 비즈니스 인텔리전스(BI)를 통해 데이터 기반 조직을 지원합니다. Quick을 사용하면 모든 사용자가 최신 대화형 대시보드, 페이지가 매겨진 보고서, 임베디드 분석 및 자연어 쿼리를 통해 동일한 정보 소스에서 다양한 분석 요구 사항을 충족할 수 있습니다. AppFabric 로그가 소스로 저장되는 Amazon S3 버킷을 선택하여 Quick에서 AppFabric 감사 로그 데이터를 분석할 수 있습니다. 자세한 내용은 빠른 사용 설명서의 Amazon S3 파일을 사용하여 데이터 세트 생성을 참조하세요. Amazon S3의 AppFabric 데이터를 Amazon Athena로 가져오고 Quick에서 Amazon Athena를 데이터 소스로 선택할 수도 있습니다. 자세한 내용은 빠른 사용 설명서의 Amazon Athena 데이터를 사용하여 데이터 세트 생성을 참조하세요.

AWS Key Management Service

AWS Key Management Service (AWS KMS)를 사용하면 애플리케이션 및 간에 암호화 키를 생성, 관리 및 제어할 수 있습니다 AWS 서비스. AppFabric에서 앱 번들을 생성할 때는 인증된 애플리케이션 데이터를 안전하게 보호하기 위한 암호화 키를 설정합니다. 이 키는 AppFabric 서비스 내의 데이터를 암호화합니다. AppFabric은 사용자를 대신하여 AppFabric에서 AWS 소유 키 생성하고 관리하는 또는 사용자가 생성하고 관리하는 고객 관리형 키를 사용할 수 있습니다 AWS KMS. 자세한 내용은 AWS KMS 키 생성을 참조하세요.

Open Cybersecurity Schema Framework for AWS AppFabric

Open Cybersecurity Schema Framework(OCSF)는 사이버 보안 업계의 AWS 및 주요 파트너가 공동으로 수행하는 오픈 소스 작업입니다. OCSF는 일반적인 보안 이벤트에 대한 표준 스키마를 제공하고, 스

키마 진화를 촉진하기 위한 버전 관리 기준을 정의하며, 보안 로그 생성자와 소비자를 위한 자체 거버넌스 프로세스를 포함합니다. OCSF의 공개 소스 코드는 GitHub에서 호스팅됩니다.

AppFabric의 OCSF 기반 스키마

AWS AppFabric for security OCSF 1.1 기반 스키마는 서비스형 소프트웨어(SaaS) 포트폴리오의 정규화되고 일관되며 노력이 적은 관찰성에 대한 요구 사항을 충족하도록 특별히 조정되었습니다. AppFabric은 각 필드 및 이벤트에 적합한 매핑을 결정합니다. AppFabric은 OCSF 오픈 소스 커뮤니티와 협력하여 OCSF를 SaaS 애플리케이션 이벤트에 적용할 수 있도록 새로운 OCSF 이벤트 카테고리, 이벤트 클래스, 활동 및 오브젝트를 도입했습니다. AppFabric은 SaaS 애플리케이션에서 수신하는 감사 이벤트를 자동으로 정규화하고이 데이터를의 Amazon Simple Storage Service(Amazon S3) 또는 Amazon Data Firehose 서비스로 전송합니다 AWS 계정. Amazon S3 대상의 경우 두 개의 정규화 옵션(OCSF 또는 원시) 과 두 가지 데이터 형식 옵션(JSON 또는Parquet) 중에서 선택할 수 있습니다. Firehose로 전송할 때 두 정규화 옵션(OCSF 또는 원시) 중에서 선택할 수도 있지만 데이터 형식은 JSON으로 제한됩니다.

AWS AppFabric을 사용하기 위한 사전 조건 및 권장 사항

신규 AWS 고객인 경우 보안을 위한 AWS AppFabric 사용을 시작하기 전에이 페이지에 나열된 설정 사전 조건을 완료하세요. 이러한 설정 절차에는 (AWS Identity and Access Management IAM) 서비스를 사용합니다. IAM에 대한 전체 내용은 IAM 사용 설명서를 참조하십시오.

주제

- 에 가입 AWS 계정
- (필수) 완전한 애플리케이션 사전 요구 사항
- (선택 사항) 출력 위치 생성
- (선택 사항) AWS KMS 키 생성

에 가입 AWS 계정

시작하려면이 AWS필요합니다 AWS 계정. 생성에 대한 자세한 AWS 계정내용은 AWS Account Management 참조 안내서의 시작하기 AWS 계정를 참조하세요.

(필수) 완전한 애플리케이션 사전 요구 사항

AppFabric for security를 사용하여 애플리케이션으로부터 사용자 정보 및 감사 로그를 수신하려면 많은 애플리케이션에 특정 역할 및 계획 유형이 있어야 합니다. AppFabric for security로 인증하려는 각

애플리케이션의 사전 조건을 검토하고 적절한 계획과 역할을 갖추고 있는지 확인합니다. 애플리케이션별 사전 조건에 대한 자세한 내용은 지원되는 애플리케이션을 참조하거나 다음 애플리케이션별 주제 중 하나를 선택하십시오.

- AppFabric1Password에 대한 구성
- AppFabricAsana에 대한 구성
- AppFabricAzure Monitor에 대한 구성
- AppFabricAtlassian Confluence에 대한 구성
- AppFabricAtlassian Jira suite에 대한 구성
- AppFabricBox에 대한 구성
- AppFabricCisco Duo에 대한 구성
- AppFabricDropbox에 대한 구성
- AppFabricGenesys Cloud에 대한 구성
- AppFabricGitHub에 대한 구성
- AppFabricGoogle Analytics에 대한 구성
- AppFabricGoogle Workspace에 대한 구성
- AppFabricHubSpot에 대한 구성
- AppFabricIBM Security® Verify에 대한 구성
- AppFabricJumpCloud에 대한 구성
- AppFabric용 Microsoft 365 구성
- AppFabricMiro에 대한 구성
- AppFabricOkta에 대한 구성
- AppFabricOneLogin by One Identity에 대한 구성
- AppFabricPagerDuty에 대한 구성
- AppFabricPing Identity에 대한 구성
- AppFabricSalesforce에 대한 구성
- AppFabricServiceNow에 대한 구성
- AppFabricSingularity Cloud에 대한 구성
- AppFabricSlack에 대한 구성
- AppFabricSmartsheet에 대한 구성

- AppFabricTerraform Cloud에 대한 구성
- AppFabricWebex by Cisco에 대한 구성
- AppFabricZendesk에 대한 구성
- AppFabricZoom에 대한 구성

(선택 사항) 출력 위치 생성

AppFabric for security는 감사 로그 수집 대상으로 Amazon Simple Storage Service(Amazon S3) 및 Amazon Data Firehose를 지원합니다.

Amazon S3

수집 대상을 생성할 때 AppFabric 콘솔을 사용하여 새 Amazon S3 버킷을 생성할 수 있습니다. Amazon S3 서비스를 사용하여 S3 버킷을 생성할 수도 있습니다. Amazon S3 서비스를 사용하여 버킷을 생성하기로 선택한 경우 AppFabric 수집 대상을 생성하기 전에 버킷을 생성한 다음, 수집 대상을 생성할 때 버킷을 선택해야 합니다. 기존 버킷에 대한 다음 요구 사항을 충족하는 한 AWS 계정에서 기존 Amazon S3 버킷을 사용하도록 선택할 수 있습니다.

- AppFabric for security를 사용하려면 Amazon S3 버킷이 Amazon S3 리소스와 동일한 AWS 리전 에 있어야 합니다.
- 는 다음 중 하나를 사용하여 버킷을 암호화할 수 있습니다.
  - Amazon S3 관리형 키를 사용한 서버 측 암호화(SSE-S3)
  - 기본 AWS Key Management Service (AWS KMS)을 사용한 () 키를 사용한 서버 측 암호화 AWS 관리형 키 (SSE-KMS).`aws/s3`

Amazon Data Firehose

Amazon Data Firehose를 AppFabric for security 데이터의 수집 대상으로 사용하도록 선택할 수 있습니다. Firehose를 사용하려면 수집을 생성하기 AWS 계정 전에 또는 AppFabric에서 수집 대상을 생성하는 동안에서 Firehose 전송 스트림을 생성할 수 있습니다. AWS Management Console, AWS CLI또는 AWS APIs 또는 SDKs. 스트림 구성 지침은 다음 주제를 참조하십시오.

- AWS Management Console 지침 - Amazon Data Firehose 개발자 안내서의 Amazon Data Firehose 전송 스트림 생성
- AWS CLI 지침 - AWS CLI 명령 참조create-delivery-stream의
- AWS APIs 및 SDKs 지침 - Amazon Data Firehose API 참조CreateDeliveryStream의

Amazon Data Firehose를 AppFabric for security 출력 대상으로 사용할 때의 요구 사항은 다음과 같습니다.

- AppFabric for security 리소스 AWS 리전 와 동일한에서 스트림을 생성해야 합니다.
- 다이렉트 PUT을 소스로 선택해야 합니다.
- AmazonKinesisFirehoseFullAccess AWS 관리형 정책을 사용자에게 연결하거나 다음 권한을 사용자에게 연결합니다.

```
{
    "Sid": "TagFirehoseDeliveryStream",
    "Effect": "Allow",
    "Action": ["firehose:TagDeliveryStream"],
    "Condition": {
        "ForAllValues:StringEquals": {"aws:TagKeys": "AWSAppFabricManaged"}
    },
    "Resource": "arn:aws:firehose:*:*:deliverystream/*"
}
```

Firehose는 Splunk 및와 같은 다양한 타사 보안 도구와의 통합을 지원합니다Logz.io. 이러한 도구에 데이터를 출력하도록 Amazon Kinesis를 올바르게 구성하는 방법에 대한 자세한 내용은 Amazon Data Firehose 개발자 안내서의 대상 설정을 참조하세요.

(선택 사항) AWS KMS 키 생성

AppFabric for security 앱 번들을 생성하는 과정에서 모든 인증된 애플리케이션으로부터 데이터를 안전하게 보호할 수 있는 암호화 키를 선택하거나 설정합니다. 이 키를 사용하여 AppFabric 서비스 내에서 데이터를 암호화합니다.

AppFabric for security는 기본적으로 데이터를 암호화합니다. AppFabric for security는 AWS 소유 키 사용자를 대신하여 AppFabric에서 생성하고 관리하는 또는 사용자가 생성하고 관리하는 고객 관리형 키 AWS Key Management Service (AWS KMS)를 사용할 수 있습니다. AWS 소유 키 는가 여러에서 사용하기 위해 AWS 서비스 소유하고 관리하는 AWS KMS 키 모음입니다 AWS 계정. 고객 관리형 키는 AWS 계정 사용자가 생성, 소유 및 관리하는의 AWS KMS 키입니다. AWS 소유 키 및 고객 관리형 키에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 키 및 AWS 키를 참조하세요.

AppFabric for security 내에서 고객 관리형 키를 사용하여 인증 토큰과 같은 데이터를 암호화하려면 AWS KMS를 사용하여 데이터를 생성할 수 있습니다. 에서 고객 관리형 키에 대한 액세스 권한을 부여하는 권한 정책에 대한 자세한 내용은이 가이드의 키 정책 섹션을 AWS KMS참조하세요.

보안을 위한 AWS AppFabric 시작하기

보안을 위한 AWS AppFabric을 시작하려면 먼저 앱 번들을 생성한 다음 애플리케이션을 승인하고 앱 번들에 연결해야 합니다. 앱 인증이 애플리케이션에 연결되면 감사 로그 수집 및 사용자 액세스와 같은 AppFabric for security 기능을 사용할 수 있습니다.

이 섹션에서는에서 AppFabric 사용을 시작하는 방법을 설명합니다 AWS Management Console.

주제

사전 조건

시작하기 전에 먼저를 생성해야 합니다 AWS 계정. 자세한 내용은 에 가입 AWS 계정 단원을 참조하십시오.

1단계: 앱 번들 생성

앱 번들에는 AppFabric for security 앱 인증 및 수집이 모두 저장됩니다. 앱 번들을 생성하려면 인증된 애플리케이션 데이터를 안전하게 보호할 수 있는 암호화 키를 설정합니다.

1. https://console.aws.amazon.com/appfabric/에서 AppFabric 콘솔을 엽니다.
2. 페이지 오른쪽 상단에 있는 리전 선택 선택기에서 AWS 리전을 선택하십시오. AppFabric은 미국 동부(버지니아 북부), 유럽(아일랜드) 및 아시아 태평양(도쿄) 리전에서만 사용할 수 있습니다.
3. 시작하기를 선택합니다.
4. 시작하기 페이지에서 1단계를 수행합니다. 앱 번들 생성에서 앱 번들 생성을 선택합니다.
5. 암호화 섹션에서 모든 승인된 애플리케이션으로부터 데이터를 안전하게 보호할 수 있는 암호화 키를 설정합니다. 이 키를 사용하여 AppFabric for security 서비스 내에서 데이터를 암호화합니다.

AppFabric for security는 기본적으로 데이터를 암호화합니다. AppFabric은 사용자를 대신하여 AppFabric에서 AWS 소유 키 생성하고 관리하는 또는 ()에서 AWS Key Management Service 생성하고 관리하는 고객 관리형 키를 사용할 수 있습니다AWS KMS.

6. AWS KMS 키에서 사용 AWS 소유 키 또는 고객 관리형 키를 선택합니다.

   고객 관리형 키를 사용하기로 선택한 경우, 사용하려는 Amazon 리소스 이름(ARN) 또는 기존 키의 키 ID를 입력하거나 AWS KMS 키 생성을 선택합니다.

   AWS 소유 키 또는 고객 관리형 키를 선택할 때는 다음 사항을 고려하세요.

   - AWS 소유 키는가 여러에서 사용하기 위해 AWS 서비스 소유하고 관리하는 AWS Key Management Service (AWS KMS) 키의 모음입니다 AWS 계정. AWS 소유 키 는에 없지만 AWS 계정는를 AWS 소유 키 사용하여 계정의 리소스를 보호할 AWS 서비스 수 있습니다. 계정의 AWS KMS 할당량에 포함되지 AWS 소유 키 않습니다. 키 또는 키 정책을 만들거나 유지하지 않아도 됩니다. 의 교체는 서비스마다 AWS 소유 키 다릅니다. AppFabric의 AWS 소유 키 교체에 대한 자세한 내용은 저장 중 암호화를 참조하십시오.
   - 고객 관리형 키는 AWS 계정 사용자가 생성, 소유 및 관리하는의 KMS 키입니다. 이러한 AWS KMS 키를 완전히 제어할 수 있습니다. 키 정책, AWS Identity and Access Management IAM (정책), 권한 부여를 설정하고 관리할 수 있습니다. 이를 활성화 및 비활성화하고, 암호화 구성 요소를 교체하고, 태그를 추가하고, AWS KMS 키를 참조하는 별칭을 생성하고, AWS KMS 키 삭제를 예약할 수 있습니다. 고객 관리형 키는 AWS Management Console 의 고객 관리형 키 페이지에 표시됩니다 AWS KMS.

     고객 관리형 키를 명확하게 식별하려면 `DescribeKey` 작업을 사용합니다. 고객 관리형 키에서는 `DescribeKey` 응답의 `KeyManager` 필드 값이 `CUSTOMER`입니다. 고객 관리형 키를 암호화 작업에 사용하고 AWS CloudTrail 로그에서 사용량을 감사할 수 있습니다. 와 통합 AWS 서비스되는 많은 AWS KMS에서 고객 관리형 키를 지정하여 저장 및 관리되는 데이터를 보호할 수 있습니다. 고객 관리형 키에는 월별 요금과 AWS 프리 티어를 초과하는 사용 요금이 부과됩니다. 고객 관리형 키는 계정의 AWS KMS 할당량에 포함됩니다.

   AWS 소유 키 및 고객 관리형 키에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 키 및 AWS 키를 참조하세요.

   > **Note**
   >
   > 앱 번들이 생성되면 AppFabric은 AWS 계정 에서 AppFabric for security의 서비스 연결 역할(SLR)이라는 특별한 IAM 역할도 생성합니다. 이를 통해 서비스는 Amazon CloudWatch

에 지표를 전송할 수 있습니다. 감사 로그 대상을 추가한 후 SLR은 AWS 리소스(Amazon S3 버킷, Amazon Data Firehose 전송 스트림)에 대한 AppFabric for security 서비스 액세스를 허용합니다. 자세한 내용은 AppFabric에 서비스 연결 역할 사용 단원을 참조하십시오.

7. (선택 사항) 태그의 경우 앱 번들에 태그를 추가할 수 있습니다. 태그는 생성한 리소스에 메타데이터를 할당하는 키-값 쌍입니다. 자세한 내용은 Tag Editor 사용 설명서의 AWS 리소스 태그 지정을 참조하세요. AWS
8. 앱 번들을 생성하려면 앱 번들 생성을 선택합니다.

2단계: 애플리케이션 인증

앱 번들이 성공적으로 생성되면 이제 AppFabric for security를 인증하여 각 애플리케이션에 연결하고 상호 작용할 수 있습니다. 인증된 애플리케이션은 암호화되어 앱 번들에 저장됩니다. 앱 번들당 여러 앱 인증을 설정하려면 각 애플리케이션에 필요에 따라 앱 인증 단계를 반복합니다.

애플리케이션 인증 단계를 시작하기 전에 AppFabric for security에서 지원되는 애플리케이션에서 각 애플리케이션의 사전 요구 사항(예: 필요한 계획 유형)을 검토하고 확인하십시오.

1. 시작하기 페이지의 2단계 애플리케이션 인증에서 앱 인증 생성을 선택합니다.
2. 앱 인증 섹션의 애플리케이션 드롭다운에서 AppFabric for security에 연결할 권한을 부여하려는 애플리케이션을 선택합니다. 표시된 애플리케이션은 현재 AppFabric for security에서 지원하는 애플리케이션입니다.
3. 애플리케이션을 선택하면 필수 정보 필드가 나타납니다. 이러한 필드에는 테넌트 ID 및 테넌트 이름이 포함되며 클라이언트 ID, 클라이언트 암호 또는 개인 액세스 토큰도 포함될 수 있습니다. 이러한 필드의 입력 값은 애플리케이션에 따라 다릅니다. 이러한 값을 찾는 방법에 대한 자세한 애플리케이션별 지침은 AppFabric for security에서 지원되는 애플리케이션을 참조하십시오.
4. (선택 사항) 태그의 경우 앱 인증에 태그를 추가할 수 있습니다. 태그는 생성한 리소스에 메타데이터를 할당하는 키-값 쌍입니다. 자세한 내용은 Tag Editor 사용 설명서의 AWS 리소스 태그 지정을 참조하세요. AWS
5. 앱 인증 생성을 선택합니다.
6. 팝업 창이 나타나면(연결 중인 애플리케이션에 따라 다름) 허용을 선택하여 AppFabric for security가 애플리케이션에 연결할 수 있도록 인증합니다.

   앱 인증에 성공하면 시작하기 페이지에 연결된 앱 인증 성공 메시지가 표시됩니다.

7. 탐색 창의 각 애플리케이션 상태 아래에 있는 앱 인증 페이지에서 언제든지 앱 인증 상태를 확인할 수 있습니다. 연결됨 상태는 AppFabric for security가 애플리케이션에 연결할 수 있도록 앱 인증이 부여되었으며 완료되었음을 의미합니다.
8. 관련 오류를 수정하기 위해 취할 수 있는 문제 해결 단계를 포함하여 가능한 앱 인증 상태가 다음 표에 나와 있습니다.

상태 이름	상태 설명	문제 해결 단계
보류중	보류중 상태는 애플리케이션에 대한 앱 인증이 생성되었지만 AppFabric for security가 아직 애플리케이션에 연결되지 않았음을 의미합니다.	이 상태가 표시되면 앱 인증 페이지의 작업 드롭다운에서 연결을 선택하여 연결을 시작합니다. 이 오류가 계속되면 브라우저의 팝업 차단기가 비활성화되어 있는지 확인하십시오. 팝업 창에 400 Bad Request와 같은 오류 메시지가 표시되는 경우 테넌트 ID, 클라이언트 ID, 클라이언트 암호와 같은 모든 정보가 올바르게 입력되었는지 확인하십시오. 애플리케이션의 앱 인증이 제대로 생성되지 않을 수도 있습니다. 자세한 내용은 지원되는 애플리케이션을 참조하세요.
연결 검증 실패	연결 검증 실패 상태는 AppFabric for security가 애플리케이션과의 앱 인증 연결을 검증할 수 없음을 의미합니다.	테넌트 ID, 클라이언트 ID, 클라이언트 암호와 같은 모든 정보가 앱 인증을 위해 올바르게 입력되었는지 확인하십시오.
토큰 자동 교체 실패	토큰 자동 교체 실패 상태는 앱 인증이 성공적으로 연결된 후 OAuth 새로 고침 토큰이 실패했음을 의미합니다.	이 오류가 계속되면 애플리케이션의 인증 애플리케이션을 확인하십시오. 자세한 내용은

상태 이름	상태 설명	문제 해결 단계
		지원되는 애플리케이션을 참조하십시오.

9. 추가 애플리케이션을 승인하려면 필요에 따라 1~8단계를 반복합니다.

3단계: 감사 로그 수집 설정

앱 번들에서 앱 인증을 하나 이상 생성했으면 이제 감사 로그 통합을 설정할 수 있습니다. 감사 로그 수집은 승인된 애플리케이션의 감사 로그를 사용하고 이를 개방형 사이버 보안 스키마 프레임워크(OCSF)로 정규화합니다. 그런 다음 AWS에 있는 한 개 이상의 목적지로 전송합니다. 원시 JSON 파일을 목적지로 전송하도록 선택할 수도 있습니다.

1. 시작하기 페이지에서 3단계를 수행하십시오. 감사 로그 통합 설정 섹션에서 통합 빠른 설정을 선택합니다.

> **Note**
>
> 더 빠르게 설정하려면 시작하기 페이지에서만 액세스할 수 있는 수집 빠른 설정 페이지를 사용하여 동일한 수집 대상으로 한 번에 여러 앱 인증에 대한 수집을 생성합니다. 예를 들어 동일한 Amazon S3 버킷 또는 Amazon Data Firehose 데이터 스트림입니다.
> 탐색 창에서 액세스할 수 있는 수집 페이지에서도 수집을 생성할 수 있습니다. 수집 페이지에서 한 번에 하나의 수집을 설정하여 대상을 구분할 수 있습니다. 수집 페이지에서 수집에 대한 태그를 만들 수도 있습니다. 다음 지침은 수집 빠른 설정 페이지를 위한 것입니다.

2. 앱 인증 선택에서 감사 로그 수집을 만들 때 사용할 앱 인증을 선택합니다. 앱 인증 드롭다운에 나타나는 테넌트 이름은 이전에 AppFabric for security로 앱 인증을 생성한 애플리케이션의 테넌트 이름입니다.
3. 대상 추가에서 선택한 애플리케이션의 감사 로그 수집 대상을 선택합니다. 대상 옵션에는 Amazon S3 - 기존 버킷, Amazon S3 - 새 버킷 또는 Amazon Data Firehose가 포함됩니다. 여러 테넌트 이름을 선택하는 경우 선택한 대상이 각 앱 인증 수집에 적용됩니다.
4. 대상을 선택하면 추가 필수 필드가 나타납니다.

   a. Amazon S3 - 새 버킷을 대상으로 선택하는 경우 생성하려는 S3 버킷의 이름을 입력해야 합니다. Amazon S3 버킷을 생성하는 방법에 대한 자세한 지침은 출력 대상 생성을 참조하십시오.

b. Amazon S3 - 기존 버킷을 대상으로 선택한 경우, 사용하려는 Amazon S3 버킷 이름을 선택합니다.

c. Amazon Data Firehose를 대상으로 선택하는 경우 Firehose 전송 스트림 이름 드롭다운 목록에서 전송 스트림의 이름을 선택합니다. Amazon Data Firehose 전송 스트림을 생성하는 방법에 대한 자세한 지침은 출력 대상 생성을 참조하고 AppFabric for security에 필요한 권한 정책을 기록해 둡니다.

5. 스키마 및 형식의 경우 감사 로그를 Amazon S3 버킷의 경우 원시 - JSON, OCSF - JSON, OCSF - 또는 Firehose의 경우 원시 - JSON 또는 OCSF-JSON에 저장하도록 선택할 수 있습니다. Parquet Amazon S3

   원시 데이터 형식은 감사 로그 데이터를 일련의 데이터에서 JSON으로 변환하여 제공합니다. OCSF 데이터 형식은 감사 로그 데이터를 AppFabric for security 개방형 사이버 보안 스키마 프레임워크(OCSF) 스키마로 정규화합니다. AppFabric이 OCSF를 사용하는 방법에 대한 자세한 내용은 Open Cybersecurity Schema Framework for AWS AppFabric을 참조하십시오. 수집을 위해 한 번에 하나의 스키마 및 형식 데이터 유형만 선택할 수 있습니다. 추가 스키마 및 데이터 형식을 추가하려는 경우 통합 생성 프로세스를 반복하여 추가 통합 대상을 설정할 수 있습니다.

6. (선택 사항) 수집에 태그를 추가하려면 탐색 창에서 수집 페이지로 이동하십시오. 수집 세부 정보 페이지로 이동하려면 테넌트 이름을 선택합니다. 태그의 경우 수집에 태그를 추가할 수 있습니다. 태그는 생성한 리소스에 메타데이터를 할당하는 키-값 쌍입니다. 자세한 내용은 Tag Editor 사용 설명서의 AWS 리소스 태그 지정을 참조하세요. AWS

7. 수집 설정을 선택합니다.

   수집을 성공적으로 설정하면 시작하기 페이지에 생성된 수집 성공 메시지가 표시됩니다.

8. 또한 탐색 창의 수집 페이지에서 언제든지 수집 상태 및 수집 대상의 상태를 확인할 수 있습니다. 이 페이지에서는 앱 인증을 생성할 때 생성된 테넌트 이름, 대상 및 수집 상태를 확인할 수 있습니다. 수집이 활성화됨 상태는 수집이 활성화되었음을 의미합니다. 이 페이지에서 앱 인증의 테넌트 이름을 선택하면 대상 세부 정보 및 상태를 포함하여 해당 앱 인증에 대한 세부 정보 페이지를 볼 수 있습니다. 수집 대상의 활성 상태는 대상이 올바르게 설정되고 활성화되었음을 의미합니다. 앱 인증이 연결됨 상태이고 통합 대상 상태가 활성인 경우 감사 로그를 처리하고 전달해야 합니다. 앱 인증 상태 또는 수집 대상 상태가 실패 상태인 경우 수집 상태가 활성 상태이더라도 감사 로그가 처리되거나 전달되지 않습니다. 앱 인증 실패를 해결하려면 2단계 애플리케이션 인증을 참조하십시오.

9. 가능한 수집 및 수집 대상 상태는 오류 상태를 해결하기 위해 수행할 수 있는 문제 해결 단계와 함께 다음 표에 나와 있습니다.

상태 또는 상태 이름	설명	문제 해결 단계
비활성화됨	수집이 비활성 상태이면 수집이 비활성화되었음을 의미합니다.	수집 페이지의 작업 드롭다운에서 활성화를 선택하여 수집을 활성화할 수 있습니다.
실패	수집 대상의 실패함 상태는 수집 대상이 감사 로그를 수락하지 않음을 의미합니다. 예를 들어, 저장소 위치가 꽉 차면 이 상태가 발생할 수 있습니다.	이러한 문제를 해결하려면 Amazon S3 또는 Firehose 콘솔로 이동합니다.

4단계: 사용자 액세스 도구 사용

보안 및 IT 관리 팀은 AppFabric for security 사용자 액세스 도구를 통해 직원의 회사 이메일 주소를 사용하여 간단한 검색을 실행함으로써 특정 애플리케이션에 액세스할 수 있는 사용자를 빠르게 확인할 수 있습니다. 이 접근 방식은 SaaS 애플리케이션 전체에서 사용자의 액세스를 수동으로 확인하거나 감사해야 하는 사용자 프로비저닝 해제와 같은 작업에 소요되는 시간을 줄이는 데 도움이 될 수 있습니다. 사용자가 발견되면 AppFabric for security는 애플리케이션에서의 사용자 이름과 애플리케이션에서 제공하는 경우 인앱 사용자 상태(예: 활성)를 제공합니다. AppFabric for security는 앱 번들에서 승인된 모든 애플리케이션을 검색하여 사용자가 액세스할 수 있는 애플리케이션 목록을 반환합니다.

1. 시작하기 페이지에서 4단계를 수행합니다. 사용자 액세스 도구 사용에서 사용자 찾기를 선택합니다.
2. 이메일 주소 필드에 사용자의 이메일 주소를 입력하고 검색을 선택합니다.
3. 검색 결과 섹션에는 사용자가 액세스할 수 있는 모든 승인된 애플리케이션 목록이 표시됩니다. 애플리케이션에 있는 사용자 이름과 상태(사용 가능한 경우)를 표시하려면 검색 결과를 선택합니다.
4. 검색 결과 열에 사용자 발견 메시지가 표시되면 해당 사용자는 목록에 있는 앱에 액세스할 수 있습니다. 다음 표에는 가능한 검색 결과, 오류 및 해당 오류를 해결하기 위해 취할 수 있는 조치가 나와 있습니다.

검색 결과	설명
사용자를 찾을 수 없음	사용된 이메일 주소를 가진 사용자를 찾을 수 없습니다.
인증 토큰을 찾을 수 없습니다. 애플리케이션에 대한 앱 인증을 연결합니다.	테넌트 ID, 클라이언트 ID, 클라이언트 암호와 같은 모든 정보가 앱 인증을 위해 올바르게 입력되었는지 확인하십시오.
인증 토큰이 취소되었습니다. 애플리케이션에 대한 앱 인증을 연결합니다.	테넌트 ID, 클라이언트 ID, 클라이언트 암호와 같은 모든 정보가 앱 인증을 위해 올바르게 입력되었는지 확인하십시오.
인증 토큰을 교체할 수 없었습니다. 애플리케이션에 대한 앱 인증을 연결합니다.	앱 인증이 성공적으로 연결된 후 OAuth 새로 고침 토큰이 실패했습니다. 이 오류가 계속되면 애플리케이션의 인증 애플리케이션을 확인하십시오. 자세한 내용은 지원되는 애플리케이션을 참조하십시오.
필요한 권한을 찾을 수 없습니다. 애플리케이션에 대한 앱 인증을 연결합니다.	테넌트 ID, 클라이언트 ID, 클라이언트 암호와 같은 모든 정보가 앱 인증을 위해 올바르게 입력되었는지 확인하십시오.
앱 승인이 유효하지 않습니다.	테넌트 ID, 클라이언트 ID, 클라이언트 암호와 같은 모든 정보가 앱 인증을 위해 올바르게 입력되었는지 확인하십시오.
권한이 부족하여 애플리케이션 API를 호출할 수 없습니다.	테넌트 ID, 클라이언트 ID, 클라이언트 암호와 같은 모든 정보가 앱 인증을 위해 올바르게 입력되었는지 확인하십시오.
애플리케이션 요청 제한을 초과했습니다.	애플리케이션에서 받은 오류 메시지입니다. 나중에 이메일 주소를 검색해 볼 수 있습니다.
애플리케이션에서 내부 서버 오류가 발생했습니다.	애플리케이션에서 받은 오류 메시지입니다. 나중에 이메일 주소를 검색해 볼 수 있습니다.

검색 결과	설명
애플리케이션에서 잘못된 게이트웨이 오류가 발생했습니다.	애플리케이션에서 받은 오류 메시지입니다. 나중에 이메일 주소를 검색해 볼 수 있습니다.
애플리케이션이 요청을 처리할 준비가 되지 않았습니다.	애플리케이션에서 받은 오류 메시지입니다. 나중에 이메일 주소를 검색해 볼 수 있습니다.
애플리케이션에서 잘못된 요청 오류가 발생했습니다.	애플리케이션에서 받은 오류 메시지입니다. 나중에 이메일을 다시 검색해 볼 수 있습니다.
애플리케이션에서 서비스를 사용할 수 없음 오류가 발생했습니다.	애플리케이션에서 받은 오류 메시지입니다. 나중에 이메일을 다시 검색해 볼 수 있습니다.

5단계: 보안 도구 및 기타 대상에 AppFabric for security 데이터 연결

AppFabric의 정규화된(또는 원시) 애플리케이션 데이터는 , , , Barracuda XDR, , DynatraceLogz.io, 등의 보안 도구 Netskope NetWitness Rapid7 Splunk또는 독점 보안 솔루션을 포함하여 Amazon S3의 데이터 수집 및 Firehose와의 통합을 지원하는 모든 도구와 호환됩니다. AppFabric에서 정규화된(또는 원시) 애플리케이션 데이터를 가져오려면 이전 1단계~3단계를 따릅니다. 특정 보안 도구 및 서비스를 설정하는 방법에 대한 자세한 내용은 호환되는 보안 도구 및 서비스를 참조하십시오.

AppFabric for security에서 지원되는 애플리케이션

AWS AppFabric for security는 다음 애플리케이션과의 통합을 지원합니다. AppFabric for security를 설정하여 연결하는 방법에 대한 자세한 내용을 보려면 애플리케이션 이름을 선택합니다.

주제

- AppFabric1Password에 대한 구성
- AppFabricAsana에 대한 구성
- AppFabricAzure Monitor에 대한 구성
- AppFabricAtlassian Confluence에 대한 구성
- AppFabricAtlassian Jira suite에 대한 구성
- AppFabricBox에 대한 구성
- AppFabricCisco Duo에 대한 구성
- AppFabricDropbox에 대한 구성

- AppFabricGenesys Cloud에 대한 구성
- AppFabricGitHub에 대한 구성
- AppFabricGoogle Analytics에 대한 구성
- AppFabricGoogle Workspace에 대한 구성
- AppFabricHubSpot에 대한 구성
- AppFabricIBM Security® Verify에 대한 구성
- AppFabricJumpCloud에 대한 구성
- AppFabric용 Microsoft 365 구성
- AppFabricMiro에 대한 구성
- AppFabricOkta에 대한 구성
- AppFabricOneLogin by One Identity에 대한 구성
- AppFabricPagerDuty에 대한 구성
- AppFabricPing Identity에 대한 구성
- AppFabricSalesforce에 대한 구성
- AppFabricServiceNow에 대한 구성
- AppFabricSingularity Cloud에 대한 구성
- AppFabricSlack에 대한 구성
- AppFabricSmartsheet에 대한 구성
- AppFabricTerraform Cloud에 대한 구성
- AppFabricWebex by Cisco에 대한 구성
- AppFabricZendesk에 대한 구성
- AppFabricZoom에 대한 구성

AppFabric1Password에 대한 구성

1Password는 모든 온라인 계정에 대한 강력한 암호를 생성, 저장 및 사용하는 데 도움이 되는 암호 관리자입니다. 또한 암호화로 데이터를 보호하고, 위반에 대해 경고하고, 암호를 공유할 수 있습니다.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고1Password, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

1Password에 대한 AppFabric 지원

AppFabric은 1Password에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 1Password로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 활성 유료 1Password 비즈니스 또는 엔터프라이즈 구독 플랜이 있어야 합니다. 자세한 내용은 1Password 웹 사이트의 1Password Enterprise를 참조하세요.
- 1Password 계정에 관리자 역할 또는 팀 소유자가 있어야 합니다. 자세한 내용은 1Password 지원 웹 사이트의 그룹을 참조하세요.

속도 제한 고려 사항

1Password AuditLog Events API는 분당 600개, 시간당 최대 30,000개로 요청을 제한합니다. 이러한 제한을 초과하면 오류가 반환됩니다. 자세한 내용은 이벤트 1Password API 참조의 API 속도 제한을 참조하세요. 1Password

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 1Password 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 1Password을 사용하여 인증해야 합니다. 1Password을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

개인 1Password 액세스 토큰 생성

1Password는 퍼블릭 클라이언트에 대한 개인 액세스 토큰을 지원합니다. 다음 단계를 완료하여 개인 액세스 토큰을 생성합니다.

1. 1Password 계정에 로그인합니다.

2. 탐색 창에서 통합을 선택합니다.
3. 기존 통합이 있는 경우 디렉터리를 선택합니다. 그렇지 않다면 계속해서 다음 단계로 이동하십시오.
4. 이벤트 보고 통합에서 기타를 선택합니다.
5. 통합 추가 페이지에서 보안 정보 및 이벤트 관리(SIEM) 시스템 이름(예: AppFabric Secure)을 입력합니다.
6. 통합 추가를 선택한 다음 토큰 설정 페이지에서 다음 단계를 완료합니다.

    a. AppFabric 보안 환경에서 사용할 토큰 이름을 제공합니다.
    b. 만료 후 드롭다운 목록에서 안 함을 선택하는 것이 좋습니다. 다른 값을 선택하면 만료 시간이 경과한 후가 토큰을 1Password 취소합니다.
    c. 보고할 이벤트 섹션에서 로그인 시도, 항목 사용 이벤트 및 감사 이벤트를 선택합니다.
7. 토큰 발급을 선택하여 토큰을 생성합니다.
8. 저장을 1Password 선택하고 다음 단계를 완료합니다.

    a. 제목은 시스템 및 토큰 이름에 따라 자동으로 채워집니다.
    b. 볼트 선택에서 프라이빗을 선택합니다.
    c. 저장을 선택합니다.

자세한 내용은 1Password 웹 사이트의 1Password 이벤트 보고 시작하기를 참조하세요.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 1Password 로그인 주소입니다. 테넌트 ID를 찾으려면 다음 단계를 완료하세요.

1. 1Password 계정에 로그인합니다.
2. 탐색 창에서 설정을 선택합니다.
3. 1Password 로그인이 페이지에 나열됩니다. 예: example-account.1password.com.

테넌트 이름

이 고유한 1Password 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

서비스 계정 토큰

AppFabric 1Password 앱 인증을 입력하려면 1Password 서비스 계정의 서비스 계정 토큰이 있어야 합니다. 서비스 계정 토큰이 없는 경우에는 다음 지침을 따르십시오.

AppFabric은 서비스 계정 토큰을 요청합니다. AppFabric의 서비스 계정 토큰은 생성한 개인 액세스 토큰입니다. 1Password 포털에서 다음 단계를 완료하여 개인 액세스 토큰을 찾습니다.

1. 대시보드를 선택합니다.
2. 사람을 선택합니다.
3. 계정 소유자 이름을 선택합니다.
4. 프라이빗을 선택합니다.
5. 볼트 보기를 선택합니다.
6. 토큰 이름을 선택합니다.

클라이언트 권한 부여

테넌트 ID, 테넌트 이름 및 서비스 계정 토큰을 사용하여 AppFabric에서 앱 권한 부여를 생성합니다. 그런 다음 연결을 선택하여 권한 부여를 활성화합니다.

AppFabricAsana에 대한 구성

Asana은 개인, 팀, 조직이 일상 업무부터 부서 간 전략적 이니셔티브에 이르기까지 업무를 조율할 수 있도록 지원하는 업무 관리 플랫폼입니다. 이는 모든 사람이 의사소통하고, 협업하고, 업무를 조정할 수 있는 명확하고 생생한 시스템을 제공합니다. Asana를 사용하면 팀이 중요한 비즈니스 도구를 한 곳으로 통합하여 어디서든 업무를 진행할 수 있습니다.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Asana, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Asana에 대한 AppFabric 지원
- AppFabric을 Asana 계정에 연결

Asana에 대한 AppFabric 지원

AppFabric은 Asana에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Asana로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Asana가 있는 엔터프라이즈 계정이 있어야 합니다. Asana 엔터프라이즈 계정을 만들거나 업그레이드하는 방법에 대한 자세한 내용은 Asana 웹 사이트의 Asana 엔터프라이즈를 참조하십시오.
- Asana 계정에 수퍼 관리자 역할을 가진 사용자가 있어야 합니다. 역할에 대한 자세한 내용은 Asana 웹사이트의 Asana에서의 관리자 및 수퍼 관리자 역할을 참조하십시오.

속도 제한 고려 사항

Asana는 Asana API에 속도 제한을 적용합니다. Asana API 속도 제한에 대한 자세한 내용은 Asana 개발자 가이드 웹사이트의 속도 제한을 참조하십시오. AppFabric과 기존 Asana 애플리케이션의 조합이 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Asana 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Asana을 사용하여 인증해야 합니다. AppFabric으로 Asana을 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID를 Asana의 도메인 ID라고 합니다. 도메인 ID를 찾으려면 Asana 홈 화면에서 다음 지침을 따르십시오.

1. 계정 프로필 사진을 선택하고 관리 콘솔을 선택합니다.
2. 그리고 설정을 선택합니다.
3. 도메인 설정으로 스크롤합니다.
4. 이 섹션의 도메인 ID를 AppFabric 테넌트 ID 구성에 입력합니다.

테넌트 이름

이 고유한 Asana 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

서비스 계정 토큰

AppFabric Asana 앱 인증을 입력하려면 Asana 서비스 계정의 서비스 계정 토큰이 있어야 합니다. 서비스 계정 토큰이 없는 경우에는 다음 지침을 따르십시오.

1. 서비스 계정을 만들려면 Asana 가이드 웹사이트의 서비스 계정에 있는 지침을 따릅니다.
2. 서비스 계정 추가 페이지를 처음 볼 때 서비스 계정 추가 페이지 하단에서 토큰을 복사하여 저장합니다.
3. 토큰을 저장하기 전에 서비스 계정 추가 페이지를 닫는 경우 서비스 계정을 편집하고 새 토큰을 생성하여 저장해야 합니다.

AppFabricAzure Monitor에 대한 구성

Azure Monitor는 클라우드 및 온프레미스 환경에서 모니터링 데이터를 수집, 분석 및 응답하기 위한 포괄적인 모니터링 솔루션입니다. Azure Monitor를 사용하여 애플리케이션 및 서비스의 가용성과 성능을 극대화할 수 있습니다. 이를 통해 애플리케이션의 성능을 이해하고 시스템 이벤트에 수동 및 프로그래밍 방식으로 대응할 수 있습니다.

Azure Monitor는 여러 Azure 및 비 Azure 구독 및 테넌트에 걸쳐 시스템의 모든 계층 및 구성 요소에서 데이터를 수집하고 집계합니다. 데이터를 상호 연관, 분석, 시각화 및/또는 응답할 수 있는 공통 도구 집합에서 사용할 수 있도록 공통 데이터 플랫폼에 저장합니다. 다른 Microsoft 및 Microsoft가 아닌 도구를 통합할 수도 있습니다. Azure Monitor 활동 로그는 구독 수준 이벤트에 대한 인사이트를 제공하는 플랫폼 로그입니다. 활동 로그에는 리소스가 수정되거나 가상 머신이 시작된 시기와 같은 정보가 포함됩니다.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Azure Monitor, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Azure Monitor에 대한 AppFabric 지원
- AppFabric을 Azure Monitor 계정에 연결

Azure Monitor에 대한 AppFabric 지원

AppFabric은 다음 Azure Monitor 서비스에서 사용자 정보 및 감사 로그를 수신할 수 있습니다.

- Azure Monitor
- API Management
- Microsoft Sentinel
- Security Center

사전 조건

AppFabric을 사용하여 Azure Monitor로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 무료 평가판 또는 pay-as-you-go 구독이 있는 Microsoft Azure 계정이 있어야 합니다.
- 해당 구독 내에서 이벤트를 가져오려면 하나 이상의 구독이 필요합니다.

속도 제한 고려 사항

Azure Monitor는 요청을 하는 보안 주체(사용자 또는 애플리케이션)와 구독 ID 또는 테넌트 ID에 속도 제한을 적용합니다. Azure Monitor API 속도 제한에 대한 자세한 내용은 Azure Monitor 개발자 웹 사이트의가 요청을 Azure Resource Manager 제한하는 방법 이해를 참조하세요.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Azure Monitor 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Azure Monitor을 사용하여 인증해야 합니다. Azure Monitor을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth2를 Azure Monitor 사용하여와 통합됩니다. 다음 단계를 완료하여에서 OAuth2 애플리케이션을 생성합니다. Azure Monitor

1. Microsoft Azure 포털로 이동하여 로그인합니다.
2. Microsoft Entra ID로 이동합니다.
3. 앱 등록을 선택합니다.
4. 새 등록에서를 선택합니다.
5. Azure Monitor OAuth 클라이언트와 같은 클라이언트의 이름을 입력합니다. 등록된 애플리케이션의 이름이 됩니다.
6. 지원되는 계정 유형이 단일 테넌트로 설정되어 있는지 확인합니다.
7. 리디렉션 URI에서 웹을 플랫폼으로 선택하고 리디렉션 URI를 추가합니다. 리디렉션 URI에 다음 형식을 사용합니다.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   해당 주소에서 *<region>*는 AppFabric 앱 번들을 구성한 AWS 리전 의 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 us-east-1입니다. 해당 리전의 리디렉션 URL은 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2입니다.

   사용자를 성공적으로 인증하면 인증 응답이 제공된 URI로 전송됩니다. 지금 제공하는 것은 선택 사항이며 나중에 변경할 수 있지만 대부분의 인증 시나리오에는 값이 필요합니다.
8. 등록을 선택합니다.
9. 등록된 앱에서 인증서 및 보안 암호를 선택한 다음 새 클라이언트 보안 암호를 선택합니다.
10. 보안 암호에 대한 설명을 추가합니다.
11. 보안 암호 만료 기간을 선택합니다. 드롭다운에서 사전 설정 기간을 선택하거나 사용자 지정 기간을 설정할 수 있습니다.
12. 추가를 선택합니다. 클라이언트 보안 암호 값은 생성 직후에만 볼 수 있습니다. 페이지를 떠나기 전에 보안 암호를 안전한 곳에 저장해야 합니다.

필수 권한

OAuth 애플리케이션에 다음 권한을 추가해야 합니다. 권한을 추가하려면 Microsoft Entra 개발자 안내서의 웹 API에 액세스할 수 있는 권한 추가 섹션의 지침을 따르세요.

- Microsoft Graph 사용자 액세스 API > User.Read.All(위임 유형 선택)
- Microsoft Graph 사용자 액세스 API > offline_access(위임 유형 선택)
- Azure 서비스 관리 감사 로그 API > user_impersonation(위임 유형 선택)

권한을 추가한 후 권한에 대한 관리자 동의를 부여하려면 Microsoft Entra 개발자 안내서의 관리자 동의 버튼 섹션에 있는 지침을 따르세요.

앱 인증

AppFabric은 Azure Monitor 계정에서 사용자 정보 및 감사 로그 수신을 지원합니다. 에서 감사 로그와 사용자 데이터를 모두 수신하려면 두 개의 앱 권한 부여를 생성Azure Monitor해야 합니다. 하나는 앱 권한 부여 드롭다운 목록에 Azure Monitor 이름이 지정되어 있고 다른 하나는 앱 권한 부여 드롭다운 목록에 Azure Monitor 감사 로그라는 이름이 지정되어 있습니다. 두 앱 인증 모두에 동일한 테넌트 ID, 클라이언트 ID 및 클라이언트 암호를 사용할 수 있습니다. 에서 감사 로그를 수신하려면 Azure Monitor 및 Azure Monitor Audit Logs 앱 인증이 모두 Azure Monitor 필요합니다. 사용자 액세스 도구만 사용하려면 Azure Monitor 앱 권한 부여만 필요합니다.

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. Azure Monitor에서 클라이언트 ID를 찾으려면 다음 단계를 완료하세요.

1. Microsoft Azure 포털로 이동합니다.
2. Azure Active Directory로 이동합니다.
3. 앱 등록 섹션에서 이전에 생성한 앱을 선택합니다.
4. 개요 섹션의 디렉터리(테넌트) ID 필드에서 테넌트 ID를 복사합니다.

테넌트 이름

이 고유한 Azure Monitor 구독을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

> **Note**
>
> 테넌트 이름은 숫자, 소문자/대문자, 마침표(.), 밑줄(_), 대시(-) 및 공백 등의 특수 문자로 구성된 최대 2,048자여야 합니다.

클라이언트 ID입니다

AppFabric은 클라이언트 ID를 요청합니다. 에서 클라이언트 ID를 찾으려면 Azure Monitor다음 절차를 완료하세요.

1. Microsoft Azure 포털로 이동합니다.
2. Azure Active Directory로 이동합니다.
3. 앱 등록 섹션에서 이전에 생성한 앱을 선택합니다.
4. 개요 섹션의 애플리케이션(클라이언트) ID 필드에서 클라이언트 ID를 복사합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. 등록된 OAuth 앱의 클라이언트 보안 암호는 OAuth 앱 생성 섹션의 11단계에서 생성한 암호입니다. OAuth 앱 생성 중에 생성된 클라이언트 보안 암호를 분실한 경우 OAuth 앱 생성 섹션의 8~11단계를 반복하여 새 보안 암호를 다시 생성합니다.

API 인증

AppFabric에서 앱 인증을 생성한 후 Microsoft Azure에서 인증을 승인하라는 팝업창이 뜹니다. 창에서 계정에 로그인하고 허용을 선택하여 AppFabric 인증을 승인합니다.

AppFabricAtlassian Confluence에 대한 구성

모든 작업을 한 곳에서 만들고, 협업하고, 정리하세요. Confluence는 지식과 협업이 만나는 팀 작업 공간입니다. 동적 페이지를 통해 팀은 모든 프로젝트 또는 아이디어를 생성하고, 캡처하고, 협업할 수 있습니다. 스페이스는 팀이 작업을 구조화, 구성 및 공유하는 데 도움이 되므로 모든 팀원이 제도적 지식을 파악하고 작업을 가장 잘 수행하는 데 필요한 정보에 액세스할 수 있습니다.

보안용 AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고Confluence, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Atlassian Confluence에 대한 AppFabric 지원
- AppFabric을 Atlassian Confluence 계정에 연결

Atlassian Confluence에 대한 AppFabric 지원

AppFabric은 Atlassian Confluence에서 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Atlassian Confluence로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 감사 로그에 액세스하려면 표준, 프리미엄 또는 엔터프라이즈 계정이 있어야 합니다. 해당 Confluence 플랜 유형을 만들거나 업그레이드하는 방법에 대한 자세한 내용은 Atlassian 웹 사이트의 Confluence 요금을 참조하세요.
- 감사 로그에 액세스하려면 계정에 대한 관리자 권한이 있어야 합니다. 역할에 대한 자세한 내용은 Atlassian 지원 웹사이트에서 사용자에게 관리자 권한 부여를 참조하십시오.

속도 제한 고려 사항

Confluence는 Atlassian Confluence API에 속도 제한을 적용합니다. AppFabric과 기존 Atlassian Confluence API 애플리케이션의 조합이 Atlassian Confluence의 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Atlassian Confluence 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Atlassian Confluence을 사용하여 인증해야 합니다. Atlassian Confluence을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth을 사용하여 Atlassian Confluence과 통합됩니다. Atlassian Confluence에서 OAuth 애플리케이션을 생성하려면 다음 단계를 사용합니다.

1. Atlassian 개발자 콘솔로 이동합니다.
2. 오른쪽 상단에서 프로필 아이콘을 선택하고 개발자 콘솔을 선택합니다.
3. 내 앱 옆의 생성, OAuth 2.0 통합을 선택합니다.
4. 왼쪽 탐색 창에서 권한을 선택하고 Confluence API 옆의 추가를 선택합니다.
5. 클래식 범위에서 사용자 읽기(`read:confluence-user`)를 선택합니다.
6. 세분화된 범위에서 감사 기록 보기(`read:audit-log:confluence`)를 선택합니다.
7. 왼쪽 탐색 창에서 인증을 선택하고 OAuth 2.0(3LO) 옆의 추가를 선택합니다.

8. 콜백 URL 텍스트 상자에 다음 형식의 리디렉션 URL을 사용하고 변경 내용 저장을 선택합니다.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

이 URL에서 *<region>*은 AppFabric 앱 번들을 구성한 AWS 리전 에 대한 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 us-east-1입니다. 해당 리전의 리디렉션 URL은 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2입니다.

필수 범위

Atlassian Confluence OAuth 애플리케이션에 다음 범위 중 하나를 추가해야 합니다. 범위에 대한 자세한 내용은 Atlassian 개발자 웹 사이트의 OAuth 2.0(3LO) 및 Forge 앱용 범위를 참조하세요. 가능한 경우 클래식 범위를 사용합니다.

- 클래식 범위:
  - read:confluence-user
- 세분화된 범위:
  - read:audit-log:confluence

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Atlassian Confluence 인스턴스 하위 도메인입니다. https://와 .atlassian.net 사이의 브라우저 주소 표시줄에서 Atlassian Confluence 인스턴스 하위 도메인을 찾을 수 있습니다.

테넌트 이름

이 고유한 Atlassian Confluence 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. Atlassian Confluence에서 클라이언트 ID를 찾으려면 다음 단계를 사용하십시오.

1. Atlassian 개발자 콘솔로 이동합니다.

2. 오른쪽 상단에서 프로필 아이콘을 선택하고 개발자 콘솔을 선택한 후, 내 앱을 선택합니다.
3. AppFabric을 연결하는 데 사용하는 OAuth 애플리케이션을 선택합니다.
4. 설정 페이지의 클라이언트 ID를 AppFabric의 클라이언트 ID 필드에 입력합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. Atlassian Confluence에서 클라이언트 암호를 찾으려면 다음 단계를 사용합니다.

1. Atlassian 개발자 콘솔로 이동합니다.
2. 오른쪽 상단에서 프로필 아이콘을 선택하고 개발자 콘솔을 선택한 후, 내 앱을 선택합니다.
3. AppFabric을 연결하는 데 사용하는 OAuth 애플리케이션을 선택합니다.
4. 설정 페이지의 암호를 AppFabric의 클라이언트 암호 필드에 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Atlassian Confluence에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricAtlassian Jira suite에 대한 구성

Atlassian은 모든 팀의 잠재력을 최대한 활용합니다. 그들의 애자일 및 DevOps, IT 서비스 관리 및 작업 관리 소프트웨어는 팀이 공유 작업을 구성, 논의 및 완료하는 데 도움이 됩니다. NASA, Kiva, Deutsche Bank 및 Salesforce 등 Fortune 500대 기업 중 대다수와 전 세계 24만 개 이상의 기업들은 Atlassian 솔루션을 사용하여 팀이 더 효율적으로 협력하고 제 시간에 고품질 결과를 제공할 수 있도록 지원합니다. Atlassian에서 Jira Software, Confluence, Jira Service Management, Trello, Bitbucket, Jira Align를 포함한 Atlassian 제품에 대해 자세히 알아봅니다.

AWS AppFabric for security를 사용하여 Jira suite (이외의)에서 로그 및 사용자 데이터를 감사하고 Jira Align, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Jira suite에 대한 AppFabric 지원
- AppFabric을 Jira 계정에 연결

Jira suite에 대한 AppFabric 지원

AppFabric은 Jira Align를 제외하고 Jira suite로부터 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Jira suite로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Jira Standard 요금제 이상이 있어야 합니다. Jira 요금제의 기능에 대한 자세한 내용은 Jira 소프트웨어, Jira 서비스 관리, Jira 작업 관리 및 Jira 제품 검색 가격 책정 페이지를 참조하십시오.
- Jira 계정에 조직 관리자 역할을 가진 사용자가 있어야 합니다. 역할에 대한 자세한 내용은 Atlassian 지원 웹사이트에서 사용자에게 관리자 권한 부여를 참조하십시오.

속도 제한 고려 사항

이 Jira 제품군은 Jira API에 속도 제한을 부과합니다. Jira suite API 속도 제한에 대한 자세한 내용은 Atlassian 개발자 안내서 웹사이트의 속도 제한을 참조하십시오. AppFabric과 기존 Jira API 애플리케이션의 조합이 한도를 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Jira 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Jira을 사용하여 인증해야 합니다. Jira을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth를 사용하여 Jira suite와 통합됩니다. Jira에서 OAuth 애플리케이션을 생성하려면 다음 단계를 사용하십시오.

1. Atlassian 개발자 콘솔로 이동합니다.
2. 내 앱 옆의 생성, OAuth 2.0 통합을 선택합니다.
3. 앱 이름을 지정한 다음 생성을 선택합니다.
4. 인증 섹션으로 이동한 다음 OAuth 2.0 옆의 추가를 선택합니다.

5. 콜백 URL 필드에 다음 형식의 URL을 사용하고 변경 내용 저장을 선택합니다.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

이 URL에서 *<region>*은 AppFabric 앱 번들을 구성한 AWS 리전 에 대한 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 `us-east-1`입니다. 해당 리전의 리디렉션 URL은 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`입니다.

6. 설정 섹션으로 이동하여 클라이언트 ID와 클라이언트 암호를 복사한 다음 AppFabric 앱 인증에 사용할 수 있도록 저장합니다.

필수 범위

Jira OAuth 애플리케이션의 권한 페이지에 다음 범위를 추가해야 합니다.

- 클래식 범위에서:
  - Jira API > `read:jira-user`
- 세분화된 범위 사용 시:
  - Jira API > `read:audit-log:jira`
  - Jira API > `read:user:jira`

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Jira 인스턴스 하위 도메인입니다. https://와 .atlassian.net 사이의 브라우저 주소 표시줄에서 Jira 인스턴스 하위 도메인을 찾을 수 있습니다.

테넌트 이름

이 고유 Jira 서버를 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. Jira에서 클라이언트 ID를 찾으려면 다음 단계를 사용하십시오.

1. Atlassian 개발자 콘솔로 이동합니다.

2. AppFabric을 연결하는 데 사용하는 OAuth 애플리케이션을 선택합니다.
3. 설정 페이지의 클라이언트 ID를 AppFabric의 클라이언트 ID 필드에 입력합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. AppFabric의 클라이언트 암호는 Jira 내부의 암호입니다. Jira에서 암호를 찾으려면 다음 단계를 사용하십시오.

1. Atlassian 개발자 콘솔로 이동합니다.
2. AppFabric을 연결하는 데 사용하는 OAuth 애플리케이션을 선택합니다.
3. 설정 페이지의 암호를 AppFabric의 클라이언트 암호 필드에 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Jira에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricBox에 대한 구성

Box는 조직이 전체 콘텐츠 수명 주기를 관리하고, 어디서나 안전하게 작업하고, best-of-breed 앱 간에 통합할 수 있도록 지원하는 단일 플랫폼인 선도적인 Content Cloud입니다.

AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고Box, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, 데이터를 Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림으로 출력할 수 있습니다.

주제

- Box에 대한 AppFabric 지원
- AppFabric을 Box 계정에 연결

Box에 대한 AppFabric 지원

AppFabric은 Box에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Box로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 감사 로그에 액세스하려면 Business, Business Plus, Enterprise 또는 Enterprise Plus 플랜에 대한 활성 유료 구독이 있어야 합니다.
- 관리자 권한이 있는 사용자가 있어야 합니다.
- 구성 탭에서 애플리케이션의 클라이언트 암호를 보고 복사하려면 Box 계정에 2단계 인증이 활성화되어 있어야 합니다.

속도 제한 고려 사항

Box는 Box API에 속도 제한을 적용합니다. Box API 속도 제한에 대한 자세한 내용은 Box 개발자 안내서 웹 사이트의 속도 제한을 참조하세요. AppFabric과 기존 Box 애플리케이션의 조합이 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 대상으로 전달되기까지 최대 30분의 지연이 발생할 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 그러나 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Box 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는를 사용하여 AppFabric에 권한을 부여해야 합니다 Box. Box을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth를 사용하여 Box과 통합됩니다. 다음 단계에 따라에서 OAuth 애플리케이션을 생성합니다Box. 자세한 내용은 Box 웹 사이트의 OAuth 앱 생성을 참조하세요.

1. 에 로그인Box하고 개발자 콘솔로 이동합니다.
2. 새 앱 생성을 선택합니다.
3. 애플리케이션 유형 목록에서 사용자 지정 앱을 선택합니다. 다음 단계를 선택하라는 메시지가 표시되는 모달이 나타납니다.
4. 앱 이름과 설명을 입력합니다.
5. 목적 드롭다운 목록에서 통합을 선택합니다.
    a. 범주 드롭다운 목록에서 보안 및 규정 준수를 선택합니다.
    b. 어떤 외부 시스템과 통합하나요? 텍스트 상자에 AWS AppFabric Secure를 입력합니다.

6. 클라이언트 ID 및 클라이언트 보안 암호로 애플리케이션 자격 증명을 확인하려면 서버 인증(클라이언트 자격 증명 부여)을 선택합니다.
7. 앱 생성을 선택합니다.
8. 구성 탭을 선택합니다.
9. 페이지의 앱 액세스 수준 섹션에서 앱 + 엔터프라이즈 액세스를 선택합니다.
10. 페이지의 애플리케이션 범위 섹션에서 사용자 관리 및 엔터프라이즈 속성 관리를 선택합니다.
11. 변경 사항 저장(Save Changes)을 선택합니다.

    Box 애플리케이션을 사용하려면 먼저 관리자가 Box 관리 콘솔 내에서 애플리케이션을 승인해야 합니다. 권한 부여를 요청하려면 다음 단계를 완료하세요.

    a. 개발자 콘솔에서 애플리케이션의 권한 부여 탭을 선택합니다.
    b. 검토 및 제출을 선택하여 승인을 위해 Box 엔터프라이즈 관리자에게 이메일을 보냅니다. 자세한 내용은 Box 안내서의 권한 부여를 참조하세요.

    > **Note**
    >
    > 제출 후 변경 사항이 있는 경우 앱을 다시 제출해야 합니다.

필수 범위

다음 애플리케이션 범위가 필요합니다. 범위에 대한 자세한 내용은 Box 설명서 웹 사이트의 범위를 참조하세요.

- 엔터프라이즈 속성 관리(`manage_enterprise_properties`)
- 사용자 관리(`manage_managed_users`)

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Box 엔터프라이즈 ID입니다. Box 엔터프라이즈 ID는 관리자 콘솔의 계정 및 결제 > 계정 정보 > 엔터프라이즈 ID에서 찾을 수 있습니다. 자세한 내용은 Box 설명서 웹 사이트의 엔터프라이즈 ID를 참조하세요.

테넌트 이름

이 고유한 Box 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 권한 부여 및 앱 권한 부여에서 생성된 수집에 레이블을 지정합니다.

클라이언트 ID 및 클라이언트 보안 암호

1. 에 로그인Box하고 개발자 콘솔로 이동합니다.
2. 탐색 메뉴에서 내 앱을 선택합니다.
3. AppFabric을 연결하는 데 사용하는 OAuth 애플리케이션을 선택합니다.
4. 구성 탭을 선택합니다.
5. 페이지의 Oauth 2.0 자격 증명 섹션으로 스크롤합니다.
6. OAuth 클라이언트 ID의 클라이언트 ID를 AppFabric의 클라이언트 ID 필드에 입력합니다.
7. 클라이언트 보안 암호 가져오기를 선택합니다.
8. OAuth 클라이언트 보안 암호의 클라이언트 보안 암호를 AppFabric의 클라이언트 보안 암호 필드에 입력합니다.

AppFabricCisco Duo에 대한 구성

Cisco Duo는에서 합법적인 사용자를 허용하고 악의적인 행위자를 차단하는 강력한 다중 계층 방어 및 혁신적인 기능을 제공하는 선도적인 액세스 관리 제품군을 통해 침해로부터 보호합니다. 위반이 우려되고 솔루션이 빠르게 필요한 모든 조직의 경우 Cisco Duo 강력한 보안을 제공하는 동시에 사용자 생산성을 개선합니다.

보안용 AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고Cisco Duo, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Cisco Duo에 대한 AppFabric 지원
- Cisco Duo 계정에 AppFabric 연결

Cisco Duo에 대한 AppFabric 지원

AppFabric은 Cisco Duo에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Cisco Duo로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 감사 로그에 액세스하려면 Duo Essentials, Duo Advantage 또는 Duo Premier 에디션에 대한 활성 구독이 있어야 합니다. 또는 Advantage 또는 Premier 평가판을 사용하는 신규 고객도에 액세스할 수 있습니다. Cisco Duo 에디션에 대한 자세한 내용은 에디션 및 요금을 참조하세요.
- 관리자 API를 생성하거나 수정하려면 소유자 역할이 있는 관리자여야 합니다.
- 관리자 API에서 감사 로그에 액세스하려면 읽기 로그 리소스 부여" 권한을 추가해야 합니다.

속도 제한 고려 사항

Cisco Duo는 Cisco Duo API에 속도 제한을 적용합니다. Cisco Duo API 속도 제한에 대한 자세한 내용은 인증 로그의 속도 제한을 참조하세요. AppFabric과 기존 Cisco Duo API 애플리케이션의 조합이 Cisco Duo의 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다. 속도 제한 증가가 필요한 경우 Cisco Duo에 문의하세요.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

Cisco Duo 계정에 AppFabric 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Cisco Duo을 사용하여 인증해야 합니다. Cisco Duo을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

Cisco Duo 관리자 API 애플리케이션 생성

AppFabric은 API 서비스 토큰을 Cisco Duo 사용하여와 통합됩니다. 에서 애플리케이션을 생성하려면 다음 단계를 Cisco Duo사용합니다.

- Cisco Duo 관리자 API 애플리케이션을 생성하려면 Cisco Duo 관리자 API의 첫 번째 단계에 있는 지침을 따릅니다.

필수 권한

Cisco Duo 애플리케이션에 다음 범위를 추가해야 합니다.

- 읽기 로그 부여
- 읽기 리소스 부여

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. 테넌트 ID는 Cisco Duo 호스트 이름에서 찾을 수 있습니다. 에서 호스트 이름을 찾으려면 다음 단계를 Cisco Duo따릅니다.

1. Cisco Duo 관리자 로그인 페이지로 이동하여 로그인합니다.
2. 애플리케이션으로 이동한 다음 애플리케이션 보호를 선택합니다.
3. 애플리케이션 목록에서 Admin API 항목을 찾은 다음 맨 오른쪽으로 보호를 선택하여 애플리케이션을 구성하고 API 호스트 이름을 가져옵니다.
4. API 호스트 이름의 형식은 이며`api-<tenant-id>.duosecurity.com`, 여기서는 테넌트 ID`<tenant-id>`입니다.

테넌트 이름

이 고유한 Cisco Duo 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

서비스 토큰

AppFabric은 서비스 토큰을 요청합니다. 서비스 토큰은 콜론으로 구분된 통합 키 및 다음 형식의 보안 키입니다.

```
integrationkey:secretkey
```

에서 통합 키와 보안 키를 찾으려면 다음 단계를 Cisco Duo사용합니다.

1. Cisco Duo 관리자 로그인 페이지로 이동하여 로그인합니다.
2. 애플리케이션으로 이동한 다음 애플리케이션 보호를 선택합니다.
3. “애플리케이션 보호를 클릭하고 애플리케이션 목록에서 Admin API에 대한 항목을 찾습니다. 맨 오른쪽에서 보호를 클릭하여 애플리케이션을 구성합니다. 범위 섹션까지 아래로 스크롤하여 **`Grant read log`** 및를 추가합니다**`Grant read resource`**.

AppFabricDropbox에 대한 구성

Dropbox는 직원들이 어떤 작업을 하고 있는지, 어디에서 작업을 하고 있는지, 어떤 종류의 도구를 사용하고 있는지에 관계없이 직원들을 한 곳에 모아 조직이 더 나은 작업을 빠르게 수행할 수 있도록 지원합니다. 이를 통해 사용자는 콘텐츠를 공유하는 간단하고 안전한 방법을 제공하여 혁신과 효율성을 가속화할 수 있습니다. Dropbox는 삶을 체계적으로 유지하고 업무를 원활하게 진행할 수 있는 곳입니다. 180개국에서 7억 명 이상의 등록 사용자를 보유한 Dropbox는 보다 현명한 업무 방식을 설계하는 것을 사명으로 삼고 있습니다.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Dropbox, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Dropbox에 대한 AppFabric 지원
- AppFabric을 Dropbox 계정에 연결

Dropbox에 대한 AppFabric 지원

AppFabric은 Dropbox에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Dropbox로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Dropbox 비즈니스 계정이 있어야 합니다. Dropbox 비즈니스 계정을 만들거나 업그레이드하는 방법에 대한 자세한 내용은 Dropbox 웹사이트의 Dropbox 비즈니스를 참조하십시오.
- Dropbox 계정에 팀 관리자 역할을 가진 사용자가 있어야 합니다. 역할에 대한 자세한 내용은 Dropbox 도움말 센터 웹사이트에서 Dropbox 팀의 관리자 권한을 변경하는 방법을 참조하십시오.

속도 제한 고려 사항

Dropbox은 Dropbox API에 속도 제한을 부과합니다. Dropbox API 속도 제한에 대한 자세한 내용은 Dropbox 성능 가이드 웹사이트의 속도 제한을 참조하십시오. AppFabric과 기존 Dropbox API 애플리케이션의 조합이 한도를 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Dropbox 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Dropbox을 사용하여 인증해야 합니다. Dropbox을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth을 사용하여 Dropbox과 통합됩니다. Dropbox에서 OAuth 애플리케이션을 생성하려면 다음 단계를 사용하십시오.

1. Dropbox 앱 콘솔 https://www.dropbox.com/developers/apps에서 앱 생성을 선택합니다.
2. 새 애플리케이션 구성 페이지에서 API에 대한 범위 지정 액세스를 선택합니다.
3. 그런 다음 액세스 유형으로 전체Dropbox를 선택합니다.
4. OAuth 애플리케이션의 이름을 지정한 다음 앱 생성을 선택하여 초기 OAuth 애플리케이션 설정을 완료합니다.
5. 애플리케이션 정보 페이지의 OAuth2 리디렉션 URI 필드에 다음 형식의 리디렉션 URL을 추가합니다.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   이 URL에서 *<region>*는 AppFabric 앱 번들을 구성한 AWS 리전 의 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 us-east-1입니다. 해당 리전의 리디렉션 URL은 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2입니다.
6. 추가를 선택합니다.
7. AppFabric 앱 인증에 사용할 앱 키와 앱 암호를 복사하고 저장합니다.
8. 설정 탭의 다른 모든 필드는 기본값을 그대로 둘 수 있습니다.

필수 범위

앱 정보 화면의 권한 탭을 사용하여 Dropbox 앱에 다음 범위를 추가해야 합니다.

- account_info.read
- team_data.member
- events.read
- members.read
- team_info.read

완료 후 제출을 선택합니다.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. 팀 이름과 같이 Dropbox 계정을 고유하게 식별하는 모든 값을 입력합니다.

테넌트 이름

이 고유 Dropbox 계정을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. AppFabric의 클라이언트 ID는 Dropbox 앱 키입니다. 다음 단계를 이용하여 Dropbox 앱 키를 찾을 수 있습니다.

1. https://www.dropbox.com/developers/apps 에서 Dropbox 앱 콘솔로 이동합니다.
2. AppFabric을 연결하는 데 사용하는 앱을 찾습니다.
3. 앱 정보 페이지의 상태 섹션에서 앱 키를 찾을 수 있습니다.
4. AppFabric의 클라이언트 ID 필드에 Dropbox앱의 앱 키를 입력합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. AppFabric의 클라이언트 암호는 Dropbox 앱 암호입니다. Dropbox 앱 암호를 찾으려면 다음 단계를 이용하십시오.

1. https://www.dropbox.com/developers/apps 에서 Dropbox 앱 콘솔로 이동합니다.
2. AppFabric을 연결하는 데 사용하는 앱을 찾습니다.

3. 앱 정보 페이지의 상태 섹션에서 앱 비밀번호를 찾을 수 있습니다.
4. AppFabric의 클라이언트 암호 필드에 Dropbox 앱의 앱 암호를 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Dropbox에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricGenesys Cloud에 대한 구성

Genesys Cloud는 간편한 올인원 인터페이스로 디지털 및 음성 채널 전반에서 원활하게 대화할 수 있습니다. 이를 통해 기업은 직원과 고객에게 탁월한 경험을 제공하고 신속한 배포, 복잡성 감소 및 간편한 관리의 이점을 누릴 수 있습니다.

보안용 AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고Genesys Cloud, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Genesys Cloud에 대한 AppFabric 지원
- AppFabric을 Genesys Cloud 계정에 연결

Genesys Cloud에 대한 AppFabric 지원

AppFabric은 Genesys Cloud에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Genesys Cloud로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Genesys Cloud 계정이 있어야 합니다.
- Genesys Cloud 계정에 관리자 역할을 가진 사용자가 있어야 합니다.

속도 제한 고려 사항

Genesys Cloud는 Genesys Cloud API에 속도 제한을 적용합니다. Genesys Cloud API 속도 제한에 대한 자세한 내용은 Genesys Cloud Developer 웹 사이트의 속도 제한을 참조하세요.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Genesys Cloud 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Genesys Cloud을 사용하여 인증해야 합니다. Genesys Cloud을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth을 사용하여 Genesys Cloud과 통합됩니다. Genesys Cloud에서 OAuth 애플리케이션을 생성하려면 다음 단계를 사용합니다.

1. Genesys Cloud 리소스 센터 웹 사이트의 OAuth 클라이언트 생성 지침을 따릅니다.

   권한 부여 유형에서는 코드 인증을 선택합니다.
2. 다음 형식의 리디렉션 URL을 권한 있는 리디렉션 URL로 사용합니다.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   이 URL에서 *<region>*은 AppFabric 앱 번들을 구성한 AWS 리전 에 대한 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 `us-east-1`입니다. 해당 리전의 리디렉션 URL은 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`입니다.
3. 범위 박스를 선택하면 앱에 사용할 수 있는 범위 목록이 표시됩니다. 범위 `audits:readonly` 및를 선택합니다`users:readonly`. 범위에 대한 자세한 내용은 Genesys Cloud 개발자 센터의 OAuth 범위를 참조하세요.
4. 저장을 선택합니다. Genesys Cloud는 클라이언트 ID와 클라이언트 암호(토큰)를 생성합니다.

필수 범위

Genesys Cloud OAuth 애플리케이션에 다음 범위를 추가해야 합니다.

- `audits:readonly`
- `users:readonly`

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Genesys Cloud 인스턴스 이름입니다. 브라우저의 주소 표시줄에서 테넌트 ID를 찾을 수 있습니다. 예를 들어, `usw2.pure.cloud` 는 다음 URL `https://login.usw2.pure.cloud`의 테넌트 ID입니다.

테넌트 이름

이 고유한 Genesys Cloud 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. Genesys Cloud에서 클라이언트 ID를 찾으려면 다음 단계를 사용합니다.

1. 관리자를 선택합니다.
2. 통합에서 OAuth를 선택합니다.
3. 클라이언트 ID를 가져올 OAuth 클라이언트를 선택합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. Genesys Cloud에서 클라이언트 암호를 찾으려면 다음 단계를 사용합니다.

1. 관리자를 선택합니다.
2. 통합에서 OAuth를 선택합니다.
3. 클라이언트 암호를 가져올 OAuth 클라이언트를 선택합니다.

AppFabricGitHub에 대한 구성

GitHub은 Git을 사용한 소프트웨어 개발 및 버전 제어를 위한 플랫폼 및 클라우드 기반 서비스로, 개발자가 코드를 저장하고 관리할 수 있도록 합니다. Git의 분산 버전 제어와 모든 프로젝트에 대한 액세스 제어, 버그 추적, 소프트웨어 기능 요청, 작업 관리, 지속적 통합 및 Wiki를 제공합니다.

보안용 AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고GitHub, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

GitHub에 대한 AppFabric 지원

AppFabric은 GitHub에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 GitHub로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 감사 로그에 액세스하려면 엔터프라이즈 계정이 있어야 합니다.
- 엔터프라이즈 감사 로그에 액세스하려면 엔터프라이즈 계정에 대한 관리자 역할이 있어야 합니다.
- 조직의 감사 로그를 가져오려면 조직 소유자여야 합니다.

속도 제한 고려 사항

GitHub는 GitHub API에 속도 제한을 부과합니다. GitHub API 속도 제한에 대한 자세한 내용은 GitHub 웹 사이트의 API 요청 제한 및 할당을 참조하십시오. AppFabric과 기존 GitHub API 애플리케이션의 조합이 GitHub's 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 GitHub 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 GitHub을 사용하여 인증해야 합니다. GitHub을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth를 사용하여 GitHub와 통합됩니다. 다음 단계를 사용하여 GitHub에서 OAuth 애플리케이션을 생성합니다. 자세한 내용은 GitHub 웹 사이트의 GitHub 앱 생성을 참조하세요.

1. 페이지 오른쪽 상단에 있는 프로필 사진을 선택한 다음 설정을 선택합니다.

2. 왼쪽 탐색 창에서 개발자 설정을 선택합니다.
3. 왼쪽 탐색 창에서 OAuth 앱을 선택합니다.
4. 새 OAuth 앱을 선택합니다.

> **Note**
>
> 이전에 OAuth 앱을 만든 적이 없는 경우 새 애플리케이션 등록이라는 라벨이 표시됩니다.

5. 애플리케이션 이름 텍스트 상자에 애플리케이션의 이름을 입력합니다.
6. 홈페이지 URL 텍스트 상자에 전체 애플리케이션 인스턴스 URL을 입력합니다.
7. (선택 사항) 애플리케이션 설명 텍스트 상자에 앱에 대한 설명을 입력합니다. 사용자는 이 설명을 볼 수 있습니다.
8. 승인 콜백 URL 텍스트 상자에 다음 형식의 URL을 입력합니다.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

이 URL에서 *<region>*은 AppFabric 앱 번들을 구성한 AWS 리전 의 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 `us-east-1`입니다. 해당 리전의 리디렉션 URL은 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`입니다.

9. OAuth 앱이 디바이스 흐름을 사용하여 사용자를 식별하고 승인하려면 디바이스 흐름 활성화를 선택합니다. 디바이스 흐름에 대한 자세한 내용은 GitHub 웹사이트에서 OAuth 앱 인증을 참조하십시오.
10. 애플리케이션 등록을 선택합니다.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. 테넌트 ID는 다음 형식 중 하나로 제공되어야 합니다.

엔터프라이즈 감사 로그:

엔터프라이즈 계정이 소유한 모든 조직의 활동을 집계하여 알고 싶다면 엔터프라이즈의 감사 로그를 사용하십시오.

엔터프라이즈 감사 로그를 사용하기 위한 테넌트 ID는 계정의 엔터프라이즈 ID입니다. 브라우저의 주소 표시줄에서 엔터프라이즈 ID를 찾을 수 있습니다. 예를 들어, *exampleenterprise* 는 다음 URL

에 있는 엔터프라이즈 `https://github.com/settings/enterprises/`*`examplenterprise`* ID입니다.

엔터프라이즈 감사 로그의 테넌트 ID를 지정할 때는 앞에 `enterprise:`를 붙여야 합니다. 따라서 이전 예를 `enterprise:examplenterprise`로 지정하십시오.

조직 감사 로그:

조직 구성원이 수행한 작업을 알고 싶다면 조직 관리자로서 조직의 감사 로그를 사용하십시오. 여기에는 누가 작업을 수행했는지, 어떤 작업을 수행했는지, 언제 수행했는지와 같은 세부 정보가 포함됩니다.

조직 감사 로그를 사용하려면 테넌트 ID가 조직 ID입니다. 브라우저의 주소 표시줄에서 조직 ID를 찾을 수 있습니다. 예를 들어, *`exampleorganization`* 는 다음 URL `https://github.com/settings/organizations/`*`exampleorganization`*의 조직 ID입니다.

조직 감사 로그의 테넌트 ID를 지정할 때는 앞에 `organization:`를 붙여야 합니다. 따라서 이전 예를 `organization:exampleorganization`로 지정하십시오.

테넌트 이름

이 고유한 GitHub 엔터프라이즈 또는 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. GitHub에서 클라이언트 ID를 찾으려면 다음 단계를 따르십시오.

1. 페이지 오른쪽 상단에 있는 프로필 사진을 선택한 다음 설정을 선택합니다.
2. 왼쪽 탐색 창에서 개발자 설정을 선택합니다.
3. 왼쪽 탐색 창에서 OAuth 앱을 선택합니다.
4. 특정 OAuth 앱을 선택한 다음 클라이언트 ID 값을 찾습니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. GitHub에서 클라이언트 암호를 찾으려면 다음 단계를 따르십시오.

1. 페이지 오른쪽 상단에 있는 프로필 사진을 선택한 다음 설정을 선택합니다.
2. 왼쪽 탐색 창에서 개발자 설정을 선택합니다.

3. 왼쪽 탐색 창에서 OAuth 앱을 선택합니다.
4. 특정 OAuth 앱을 선택한 다음 클라이언트 암호 값을 찾습니다. 기존 클라이언트 암호를 찾을 수 없는 경우 새 클라이언트 암호를 생성해야 할 수 있습니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 GitHub에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

OAuth 앱 액세스 제한이 활성화되어 있는 경우 조직에서 OAuth 앱에 대한 액세스 권한을 부여했는지 확인하십시오.

AppFabricGoogle Analytics에 대한 구성

Google Analytics는 검색 엔진 최적화(SEO) 및 마케팅 목적으로 통계 및 기본 분석 도구를 제공하는 웹 분석 서비스입니다. Google Analytics는 웹 사이트 성능을 추적하고 방문자 인사이트를 수집하는 데 사용됩니다. 이를 통해 조직은 사용자 트래픽의 상위 소스를 파악하고, 마케팅 활동 및 캠페인의 성공을 측정하고, 목표 완료(예: 구매, 장바구니에 제품 추가)를 추적하고, 사용자 참여의 패턴과 추세를 발견하고, 인구 통계와 같은 기타 방문자 정보를 얻을 수 있습니다. 중소 규모의 소매 웹 사이트는 마케팅 캠페인을 개선하고, 웹 사이트 트래픽을 유도하고, 방문자를 더 잘 유지하는 Google Analytics 데 사용할 수 있는 다양한 고객 행동 분석을 얻고 분석하는 데를 사용하는 경우가 많습니다.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Azure Monitor, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Google Analytics에 대한 AppFabric 지원
- AppFabric을 Google Analytics 계정에 연결

Google Analytics에 대한 AppFabric 지원

AppFabric은 Google Analytics에서 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Google Analytics로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Google Analytics 계정의 관리자여야 합니다.
- AppFabric이 로그를 전송하려면 Google Cloud 프로젝트에서 Google Analytics 관리자 API를 활성화해야 합니다. Google Analytics OAuth 애플리케이션을 설정할 때 새 프로젝트를 사용해야 합니다.

속도 제한 고려 사항

Google Analytics는 Google Analytics API에 속도 제한을 적용합니다. Google Analytics API 속도 제한에 대한 자세한 내용은 Google Analytics 웹 사이트의 제한 및 할당량을 참조하세요. AppFabric과 기존 Google Analytics API 애플리케이션의 조합이 제한을 초과하면 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Google Analytics 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Google Analytics을 사용하여 인증해야 합니다. 다음 단계를 사용하여 AppFabric으로 Google Analytics을 인증하는 데 필요한 정보를 찾을 수 있습니다.

OAuth 애플리케이션 생성

AppFabric은 OAuth를 사용하여 Google Analytics와 통합됩니다. 다음 단계를 완료하여에서 OAuth 애플리케이션을 생성합니다. Google Analytics

1. OAuth 동의 화면을 구성하려면 Google 웹 사이트의 Google 개발자 안내서에 있는 OAuth 동의 화면 구성의 지침을 따르세요.
2. 사용자 유형으로 외부를 선택합니다.
3. AppFabric에 대한 OAuth 자격 증명을 구성하려면 Google 개발자 안내서의 액세스 자격 증명 생성 페이지의 OAuth 클라이언트 ID 자격 증명 섹션에 있는 지침을 따르세요.
4. 다음 형식의 리디렉션 URL을 사용합니다.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

해당 주소에서 *<region>*는 AppFabric 앱 번들을 구성한 AWS 리전 의 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 us-east-1입니다. 해당 리전의 리디렉션 URL은 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2입니다.

필수 범위

Google Analytics OAuth 애플리케이션에 다음 범위를 추가해야 합니다.

```
https://www.googleapis.com/auth/analytics.edit
```

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Google Analytics 계정 ID입니다.

1. Google Analytics 홈 페이지로 이동합니다.
2. 탐색 창에서 관리를 선택합니다.
3. 계정 ID는 계정 > 계정 설정 > 계정 세부 정보 > 계정 ID에서 확인할 수 있습니다.

테넌트 이름

이 고유한 Google Analytics 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. 다음 단계에 따라에서 클라이언트 ID를 찾습니다. Google Analytics

1. 자격 증명 페이지로 이동합니다.
2. OAuth 2.0 클라이언트 IDs 섹션에서 생성한 클라이언트 ID를 선택합니다.
3. 클라이언트 ID는 페이지의 추가 정보 섹션에 나열됩니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. 다음 단계에 따라에서 클라이언트 보안 암호를 찾습니다. Google Analytics

1. 자격 증명 페이지로 이동합니다.
2. OAuth 2.0 클라이언트 IDs 섹션에서 클라이언트 이름을 선택합니다.
3. 클라이언트 보안 암호는 페이지의 클라이언트 보안 암호 섹션에 나열됩니다.

API 인증

AppFabric에서 앱 인증을 생성한 후 Google Analytics에서 인증을 승인하라는 팝업창이 뜹니다. 허용을 선택하여 AppFabric 권한 부여를 승인합니다.

AppFabricGoogle Workspace에 대한 구성

Google Workspace는 Google에서 개발하고 판매하는 클라우드 컴퓨팅, 생산성 및 협업 도구, 소프트웨어 및 제품의 모음입니다.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Google Workspace, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Google Workspace에 대한 AppFabric 지원
- AppFabric을 Google Workspace 계정에 연결

Google Workspace에 대한 AppFabric 지원

AppFabric은 Google Workspace에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Google Workspace로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Google Workspace Enterprise Standard 요금제를 구독해야 합니다. Google Workspace Enterprise Standard 요금제를 만들거나 업그레이드하는 방법에 대한 자세한 내용은 Google Workspace 요금제 웹사이트를 참조하십시오.
- Google Workspace에는 관리자 역할을 가진 사용자가 있어야 합니다.
- AppFabric이 로그를 전달하려면 Google 클라우드 프로젝트에서 Google 관리자 SDK API를 활성화해야 합니다. 자세한 내용은 Google Workspace 개발자 가이드의 Google Workspace API 활성화를 참조하십시오.

속도 제한 고려 사항

Google Workspace는 Google Workspace API에 속도 제한을 적용합니다. Google Workspace API 속도 제한에 대한 자세한 내용은 Google Workspace 웹사이트의 Google Workspace 관리자 가이드에서 한도 및 할당량을 참조하십시오. AppFabric과 기존 Google Workspace API 애플리케이션의 조합이 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

대부분의 감사 이벤트에 대해 최대 30분의 지연이 표시되고 특정 감사 이벤트가 대상으로 전달되는 데 최대 4시간의 지연이 표시될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 자세한 내용은 Google WorkSpace Admin Help 웹 사이트의 데이터 보존 및 지연 시간을 참조하세요. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면에 문의하세요지원.

AppFabric을 Google Workspace 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Google Workspace을 사용하여 인증해야 합니다. Google Workspace을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth을 사용하여 Google Workspace과 통합됩니다. Google Workspace에서 OAuth 애플리케이션을 만들려면 다음 단계를 사용하십시오.

1. OAuth 동의 화면을 구성하려면 Google Workspace 웹사이트의 Google Workspace 개발자 안내서에 있는 OAuth 동의 화면 구성의 지침을 따르십시오.

   사용자 유형으로 내부를 선택합니다.
2. AppFabric의 OAuth 보안 인증을 구성하려면 Google Workspace 개발자 안내서의 액세스 자격 증명 생성 페이지의 OAuth 클라이언트 ID 보안 인증 섹션에 있는 지침을 따르십시오.
3. 다음 형식의 리디렉션 URL을 사용합니다.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   이 URL에서 *<region>*는 AppFabric 앱 번들을 구성한 AWS 리전 의 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 us-east-1입니다. 해당 리전의 리디렉션 URL은 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2입니다.

필수 범위

Google Workspace OAuth 애플리케이션에 다음 범위를 추가해야 합니다.

- `https://www.googleapis.com/auth/admin.reports.audit.readonly`
- `https://www.googleapis.com/auth/admin.directory.user`

이러한 범위가 보이지 않으면 Google Cloud API 라이브러리에 관리자 SDK API를 추가하십시오.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Google Workspace 프로젝트 ID입니다. 프로젝트 ID를 찾으려면 Google API 콘솔 도움말 웹 사이트에서 프로젝트 ID 찾기를 참조하십시오.

테넌트 이름

이 고유 Google Workspace 이름을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. 클라이언트 ID를 찾으려면 다음 단계를 따르십시오.

1. Google Workspace 개발자 안내서의 보안 인증 관리 페이지의 보안 인증 보기 섹션에 있는 정보를 사용하여 클라이언트 ID를 찾으십시오.
2. AppFabric의 클라이언트 ID 필드에 OAuth 클라이언트의 클라이언트 ID를 입력합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. 클라이언트 암호를 찾으려면 다음 단계를 사용합니다.

1. Google Workspace 개발자 안내서의 보안 인증 관리 페이지에 있는 보안 인증 보기 섹션에 있는 정보를 사용하여 클라이언트 암호를 찾으십시오.
2. 클라이언트 암호를 재설정해야 하는 경우 Google Workspace 개발자 안내서의 보안 인증 관리 페이지에 있는 클라이언트 암호 재설정 섹션에 있는 지침을 따르십시오.
3. AppFabric의 클라이언트 암호 필드에 클라이언트 암호를 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Google Workspace에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricHubSpot에 대한 구성

HubSpot은 마케팅, 영업, 콘텐츠 관리 및 고객 서비스를 연결하는 데 필요한 모든 소프트웨어, 통합 및 리소스를 갖춘 고객 플랫폼입니다. HubSpot의 연결된 플랫폼을 사용하면 가장 중요한 대상인 고객에 집중하여 비즈니스를 더 빠르게 성장시킬 수 있습니다.

보안용 AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고HubSpot, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

HubSpot에 대한 AppFabric 지원

AppFabric은 HubSpot에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 HubSpot로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 액세스 감사 로그에 액세스하려면 HubSpot의 엔터프라이즈를 구독하는 계정이 있어야 합니다. HubSpot 구독에 대한 자세한 내용은 HubSpot 지식 기반에서 HubSpot 구독 관리를 참조하세요.
- 개발자 계정과 이 계정에 연결된 앱이 있어야 합니다.
- HubSpot 계정에 앱을 설치하려면 최고 관리자여야 합니다. 또는 App Marketplace 액세스 권한과 함께 앱이 요청하는 범위를 수락할 수 있는 사용자 권한이 있어야 합니다.

속도 제한 고려 사항

HubSpot는 HubSpot API에 속도 제한을 적용합니다. OAuth를 사용하는 앱의 제한를 비롯한 HubSpot API 속도 제한에 대한 자세한 내용은 HubSpot 웹 사이트의 속도 제한을 참조하세요. AppFabric과 기존

HubSpot API 애플리케이션의 조합이 HubSpot의 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 HubSpot 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 HubSpot을 사용하여 인증해야 합니다. HubSpot을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth을 사용하여 HubSpot과 통합됩니다. HubSpot에서 OAuth 애플리케이션을 생성하려면 다음 단계를 사용합니다.

1. HubSpot 웹 사이트에서 HubSpot 가이드의 퍼블릭 앱 생성 섹션의 지침을 따릅니다.
2. 인증 탭에서 필수 범위에 나열된 세 가지 범위를 추가합니다.
3. 리디렉션 URL에서다음 형식의 리디렉션 URL을 앱 리디렉션 URL로 사용합니다.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   이 URL에서 *<region>*은 AppFabric 앱 번들을 구성한 AWS 리전 에 대한 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 us-east-1입니다. 해당 리전의 리디렉션 URL은 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2입니다.
4. 앱 생성을 선택합니다.

필수 범위

HubSpot OAuth 애플리케이션에 다음 범위를 추가해야 합니다.

- settings.users.read
- crm.objects.owners.read
- account-info.security.read

앱 인증

테넌트 ID

이 고유한 HubSpot 조직을 식별하는 ID를 입력합니다. 예를 들어 HubSpot 계정 ID를 입력합니다.

테넌트 이름

이 고유한 HubSpot 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. HubSpot에서 클라이언트 ID를 찾으려면 다음 단계를 사용합니다.

1. HubSpot로그인 페이지로 이동한 다음 개발자 계정 보안 인증 정보를 사용하여 로그인합니다.
2. 앱 메뉴에서 앱을 선택합니다.
3. 인증 탭에서 클라이언트 ID 값을 찾습니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. HubSpot에서 클라이언트 암호를 찾으려면 다음 단계를 사용합니다.

1. HubSpot로그인 페이지로 이동한 다음 개발자 계정 보안 인증 정보를 사용하여 로그인합니다.
2. 앱 메뉴에서 앱을 선택합니다.
3. 인증 탭에서 클라이언트 암호 값을 찾습니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 HubSpot에서 인증을 승인하라는 팝업창이 뜹니다. 개발자 계정이 아닌 엔터프라이즈 계정 보안 인증 정보를 사용하여 계정에 로그인하여 AppFabric 인증을 승인합니다. 허용을 선택합니다.

AppFabricIBM Security® Verify에 대한 구성

IBM Security® Verify 패밀리는 자격 증명 거버넌스 관리, 인력 및 소비자 자격 증명 및 액세스 관리, 권한 있는 계정 제어를 위한 자동화된 클라우드 기반 및 온프레미스 기능을 제공합니다. 클라우드 솔루션

을 배포해야 하든 온프레미스 솔루션을 배포해야 하든 IBM Security® Verify를 사용하면 신뢰를 구축하고 작업 인력과 소비자 모두에 대한 내부자 위협으로부터 보호할 수 있습니다.

AWS AppFabric for security를 사용하여에서 감사 로그 및 사용자 데이터를 수신하고IBM Security® Verify, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림으로 데이터를 출력할 수 있습니다.

주제

- IBM Security® Verify에 대한 AppFabric 지원
- AppFabric을 IBM Security® Verify 계정에 연결

IBM Security® Verify에 대한 AppFabric 지원

AppFabric은 IBM Security® Verify에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 IBM Security® Verify로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 감사 로그에 액세스하려면 IBM Security® Verify SaaS 계정이 있어야 합니다.
- 감사 로그에 액세스하려면 IBM Security® Verify SaaS 계정에 관리자 역할이 있어야 합니다.

속도 제한 고려 사항

IBM Security® Verify는 IBM Security® Verify API에 속도 제한을 적용합니다. IBM Security® Verify API 속도 제한에 대한 자세한 내용은 IBM 약관을 참조하세요. AppFabric과 기존 IBM Security® Verify API 애플리케이션의 조합이 IBM Security® Verify 제한을 초과하면 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 대상으로 전달되기까지 최대 30분의 지연이 발생할 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 그러나 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 IBM Security® Verify 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 IBM Security® Verify을 사용하여 인증해야 합니다. IBM Security® Verify을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth를 사용하여 IBM Security® Verify와 통합됩니다. 에서 OAuth 애플리케이션을 생성하려면 IBM 설명서 웹 사이트의 API 클라이언트 생성을 IBM Security® Verify참조하세요.

1. 처음 로그인하는 경우 등록된 이메일 주소로 전송된 로그인 URL과 자격 증명을 사용합니다.
2. 에서 관리 콘솔에 액세스합니다`https://<hostname>.verify.ibm.com/ui/admin/`. 자세한 내용은 IBM Security® Verify에 대한 액세스 단원을 참조하십시오.
3. 관리 콘솔의 보안 < API 액세스 < API 클라이언트에서 추가를 선택합니다.
4. 다음 옵션을 선택합니다. 이는 감사 로그 및 사용자 세부 정보를 읽는 데 필요합니다.
   - 보고서 읽기
   - 사용자 및 그룹 읽기
5. 클라이언트 인증 방법에서 기본 옵션을 유지합니다.

   사용자 지정 범위 필드를 편집하지 마십시오.
6. 다음을 선택합니다.
7. IP 필터 필드를 편집하지 마십시오.
8. 다음을 선택합니다.
9. 추가 속성 필드를 편집하지 마십시오.
10. 다음을 선택합니다.
11. 이름 및 설명을 지정합니다. 설명은 선택 사항입니다.
12. API 클라이언트 생성을 선택합니다.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. 테넌트 ID는 IBM Security® Verify 표준 URL에서 찾을 수 있습니다. 예를 들어 `https://hostname.verify.ibm.com/` URL에서 테넌트 ID는 이전에(또는 이전

사용하는 ice.ibmcloud.com 경우 이전에.verify.ibm.com) 찾을 수 있는 호스트 이름입니다. 베니티 URL을 사용하는 경우 IBM Security® Verify 지원 팀에 문의하여 표준 URL을 받으세요.

테넌트 이름

이 고유한 IBM Security® Verify 테넌트를 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 권한 부여 및 앱 권한 부여에서 생성된 수집에 레이블을 지정합니다.

클라이언트 ID입니다

AppFabric은 클라이언트 ID를 요청합니다. IBM Security® Verify에서 클라이언트 ID를 찾으려면 다음 단계를 사용하십시오.

1. 처음 로그인하는 경우 등록된 이메일 주소로 전송된 로그인 URL과 자격 증명을 사용합니다.
2. 에서 관리 콘솔에 액세스합니다https://<hostname>.verify.ibm.com/ui/admin/. 자세한 내용은 IBM Security® Verify에 대한 액세스 단원을 참조하십시오.
3. 관리 콘솔의 보안 < API 액세스 < API 클라이언트에서 특정 OAuth 앱 옆에 있는 줄임표(")를 선택합니다.
4. 연결 세부 정보를 선택합니다.
5. API 자격 증명에서 클라이언트 ID를 찾습니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. IBM Security® Verify에서 클라이언트 암호를 찾으려면 다음 단계를 사용합니다.

1. 처음 로그인하는 경우 등록된 이메일 주소로 전송된 로그인 URL과 자격 증명을 사용합니다.
2. 에서 관리 콘솔에 액세스합니다https://<hostname>.verify.ibm.com/ui/admin/. 자세한 내용은 IBM Security® Verify에 대한 액세스 단원을 참조하십시오.
3. 관리 콘솔의 보안 < API 액세스 < API 클라이언트에서 특정 OAuth 앱 옆에 있는 줄임표(")를 선택합니다.
4. 연결 세부 정보를 선택합니다.
5. API 자격 증명에서 클라이언트 보안 암호를 찾습니다.

AppFabricJumpCloud에 대한 구성

JumpCloud Inc.는 자격 증명 관리를 위한 클라우드 기반 디렉터리 플랫폼을 제공하는 미국 엔터프라이즈 소프트웨어 회사입니다. ID 관리를 중앙 집중화하고 간소화하여 플랫폼, 프로토콜, 공급자 또는 위치에 관계없이 사용자가 단일 자격 증명 세트로 시스템, 앱, 네트워크 및 파일 서버에 안전하게 액세스할 수 있도록 합니다.

AWS AppFabric을 사용하여 JumpCloud에서 감사 로그 및 사용자 데이터를 수신하고, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림으로 데이터를 출력할 수 있습니다.

주제

JumpCloud에 대한 AppFabric 지원

AppFabric은 JumpCloud에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 JumpCloud로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 활성 유료 JumpCloud 구독 플랜이 있어야 합니다. 자세한 내용은 JumpCloud 웹 Select a package that's right for you 사이트의 섹션을 참조하세요.
- "청구가 있는 관리자" 역할이 있어야 합니다.

속도 제한 고려 사항

JumpCloud는 속도 제한을 게시하지 않습니다. 지원 사례를 생성하거나 JumpCloud 고객 팀에 문의해야 합니다. AppFabric과 기존 JumpCloud API 애플리케이션의 조합이 JumpCloud's 제한을 초과하면 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 사용할 수 있는 감사 이벤트의 지연과 데이터 손실을 줄이기 위한 예방 조치로 인한 것입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 JumpCloud 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 JumpCloud을 사용하여 인증해야 합니다. JumpCloud AppFabric으로 권한을 부여하는 데 필요한 정보를 찾으려면 다음 섹션의 단계를 따르세요.

JumpCloud 계정에서 조직 토큰 생성

AppFabric은 API 키를 사용하여와 통합합니다. JumpCloud에서 API 키를 생성JumpCloud하려면 다음 단계를 따릅니다.

1. 관리자로 계정에 로그인합니다JumpCloud.
2. 관리자 포털의 오른쪽 상단에 있는 계정 이니셜을 선택하고 메뉴에서 내 API 키를 선택합니다.
3. 새 API 키 생성을 선택하거나 기존 키를 선택합니다.

> **Note**
>
> JumpCloud는 하나의 활성 API 키만 허용합니다. 새 API 키를 생성하면 현재 API 키에 대한 액세스가 취소됩니다. 이렇게 하면 이전 API 키를 사용하여 모든 호출에 액세스할 수 없게 됩니다. 이전 API 키를 사용하는 기존 통합을 새 키 값으로 업데이트해야 합니다.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. 여기서 “조직 ID”는 테넌트 ID입니다. "조직 ID"를 찾으려면 다음 단계를 따릅니다.

1. JumpCloud 계정에 로그인합니다.
2. 탐색 창에서 설정을 선택한 다음 조직 프로필을 선택하고 일반을 선택합니다.
3. "눈" 아이콘을 선택하여 가려진 보기를 제거합니다.
4. "double-page" 아이콘을 선택하여 ID를 복사합니다.

테넌트 이름

이 고유한 JumpCloud 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

서비스 계정 토큰

AppFabric은 서비스 계정 토큰을 요청합니다. AppFabric에서는이 주제의 JumpCloud 계정에서 조직 토큰 생성앞부분에서에서 생성한 조직 API 토큰입니다.

AppFabric용 Microsoft 365 구성

Microsoft 365는 Microsoft가 소유한 생산성 소프트웨어, 협업 및 클라우드 기반 서비스 제품군입니다.

AWS AppFabric for security를 사용하여 Microsoft 365의 로그 및 사용자 데이터를 감사하고, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Microsoft 365를 위한 AppFabric 지원
- AppFabric을 Microsoft 365 계정에 연결

Microsoft 365를 위한 AppFabric 지원

AppFabric은 Microsoft 365에서의 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Microsoft 365로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Microsoft 365 Enterprise 요금제를 구독해야 합니다. Microsoft 365 Enterprise 요금제를 만들거나 업그레이드하는 방법에 대한 자세한 내용은 Microsoft 웹사이트의 Microsoft 365 Enterprise 요금제를 참조하십시오.
- Microsoft 365 계정에 관리자 권한이 있는 사용자가 있어야 합니다.
- 조직에 대해 감사 로깅을 켜야 합니다. 자세한 내용은 Microsoft 웹사이트에서 감사 켜기 또는 끄기를 참조하십시오.

속도 제한 고려 사항

Microsoft 365는은 Microsoft 365 API에 속도 제한을 부과합니다. Microsoft 365 API 속도 제한에 대한 자세한 내용은 Microsoft 웹사이트의 Microsoft 그래프 설명서에서 Microsoft 그래프 서비스별 제한을 참조하십시오. AppFabric과 기존 Microsoft 365 API 애플리케이션의 조합이 한도를 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Microsoft 365 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 Microsoft 365를 사용하여 AppFabric을 인증해야 합니다. AppFabric으로 Microsoft 365를 승인하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth를 사용하여 Microsoft 365와 통합됩니다. Microsoft 365에서 OAuth 애플리케이션을 생성하려면 다음 단계를 사용하십시오.

1. Microsoft 웹사이트의 Azure Active Directory 개발자 가이드에서 애플리케이션 등록 섹션에 있는 지침을 따르십시오.

   지원되는 계정 유형 구성에서만 이 조직 디렉터리의 계정을 선택하십시오.
2. Azure Active Directory 개발자 가이드의 리디렉션 URI 추가 섹션에 있는 지침을 따르십시오.

   웹 플랫폼을 선택합니다.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   이 URL에서 *<region>*는 AppFabric 앱 번들을 구성한 AWS 리전 의 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 `us-east-1`입니다. 해당 리전의 리디렉션 URL은 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`입니다.

   웹 플랫폼의 다른 입력 필드는 건너뛸 수 있습니다.
3. Azure Active Directory 개발자 가이드의 클라이언트 암호 추가 섹션에 있는 지침을 따르십시오.

필수 권한

OAuth 애플리케이션에 다음 권한을 추가해야 합니다. 권한을 추가하려면 Azure Active Directory 개발자 가이드의 웹 API 액세스를 위한 권한 추가 섹션에 있는 지침을 따르십시오.

- `Microsoft Graph API` > `User.Read` (자동 추가됨)

- `Office 365 Management APIs` > `ActivityFeed.Read` (위임 유형 선택)
- `Office 365 Management APIs` > `ActivityFeed.ReadDlp` (위임 유형 선택)
- `Office 365 Management APIs` > `ServiceHealth.Read` (위임 유형 선택)

권한을 추가한 후 권한에 대한 관리자 동의를 부여하려면 Azure Active Directory 개발자 가이드의 관리자 동의 버튼 섹션에 있는 지침을 따르십시오.

앱 인증

AppFabric은 Microsoft 365 계정으로부터 사용자 정보 및 감사 로그를 수신하는 것을 지원합니다. Microsoft 365에서 감사 로그와 사용자 데이터를 모두 받으려면 두 개의 앱 인증을 생성해야 합니다. 하나는 앱 인증 드롭다운 목록에서 Microsoft 365로 이름이 지정되고 다른 하나는 앱 인증 드롭다운 목록에서 Microsoft 365 감사 로그로 이름이 지정됩니다. 두 앱 인증 모두에 동일한 테넌트 ID, 클라이언트 ID 및 클라이언트 암호를 사용할 수 있습니다. Microsoft 365에서 감사 로그를 받으려면 Microsoft 365 및 Microsoft 365 감사 로그 앱 인증이 모두 필요합니다. 사용자 액세스 도구만 사용하려면 Microsoft 365 앱 인증만 필요합니다.

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Azure Active Directory 테넌트 ID입니다. Azure Active Directory 테넌트 ID를 찾으려면 Microsoft 웹사이트의 Azure 제품 설명서에서 Azure Active Directory 테넌트 ID를 찾는 방법 을 참조하십시오.

테넌트 이름

이 고유한 Microsoft 365 계정을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. AppFabric의 클라이언트 ID는 Microsoft 365 애플리케이션(클라이언트 ID)입니다. Microsoft 365 애플리케이션(클라이언트) ID를 찾으려면 다음 단계를 사용하십시오.

1. AppFabric과 함께 사용하는 OAuth 애플리케이션의 개요 페이지를 엽니다.
2. 애플리케이션(클라이언트) ID는 에센셜 아래에 표시됩니다.
3. AppFabric의 클라이언트 ID 필드에 OAuth 클라이언트의 애플리케이션(클라이언트) ID를 입력합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. Microsoft 365는 OAuth 애플리케이션의 클라이언트 암호를 처음 생성할 때만 이 값을 제공합니다. 클라이언트 암호가 없는 경우 새 클라이언트 암호를 생성하려면 다음 단계를 사용하십시오.

1. 클라이언트 암호를 만들려면 Azure Active Directory 개발자 가이드의 클라이언트 암호 추가 섹션에 있는 지침을 따르십시오.
2. AppFabric의 클라이언트 암호 필드에 값 필드의 내용을 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Microsoft 365에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricMiro에 대한 구성

Miro은 규모를 불문하고 분산된 팀이 차세대 솔루션을 구축할 수 있도록 지원하는 혁신을 위한 온라인 작업 공간입니다. 플랫폼의 무한한 캔버스를 통해 팀은 매력적인 워크숍과 회의를 진행하고, 제품을 디자인하고, 아이디어를 브레인스토밍하는 등의 작업을 수행할 수 있습니다. Miro는 샌프란시스코와 암스테르담에 공동 본사를 두고 있으며 Fortune 100대 기업의 99%를 포함하여 전 세계 5천만 명 이상의 사용자에게 서비스를 제공하고 있습니다. Miro는 2011년에 설립되어 현재 전 세계 12개 허브에 1,500명 이상의 직원이 근무하고 있습니다. 자세히 알아보려면 Miro를 방문하십시오.

Miro에는 다이어그램 작성, 와이어프레임 작성, 실시간 데이터 시각화, 워크숍 촉진, 신속한 변화를 위한 실무, 워크숍 및 대화형 프레젠테이션을 위한 기본 지원 등 혁신을 위해 설계된 모든 협업 기능이 포함되어 있습니다. Miro는 최근 AI 기반 매핑 및 다이어그램 작성, 클러스터링 및 요약, 콘텐츠 생성을 통해 Miro의 기능을 확장하는 Miro AI를 발표했습니다. Miro을 통해 조직은 독립 실행형 도구의 수를 줄여 정보 파편화 및 비용을 줄일 수 있습니다.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Miro, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Miro에 대한 AppFabric 지원
- AppFabric을 Miro 계정에 연결

Miro에 대한 AppFabric 지원

AppFabric은 Miro에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Miro로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Miro 엔터프라이즈 요금제가 있어야 합니다. Miro 요금제 유형에 대한 자세한 내용은 Miro 웹 사이트의 Miro가격 페이지를 참조하십시오.
- Miro 계정에 회사 관리자 역할을 가진 사용자가 있어야 합니다. 역할에 대한 자세한 내용은 Miro 도움말 센터 웹 사이트의 Miro 내 역할의 회사 수준 섹션을 참조하십시오.
- Miro 계정에 엔터프라이즈 개발자 팀이 있어야 합니다. 개발자 팀을 만드는 방법에 대한 자세한 내용은 Miro 도움말 센터 웹 사이트에서 엔터프라이즈 개발자 팀을 참조하십시오.

속도 제한 고려 사항

Miro는 Miro API에 속도 제한을 부과합니다. Miro API 속도 제한에 대한 자세한 내용은 Miro 웹 사이트의 Miro 개발자 안내서에서 속도 제한을 참조하십시오. AppFabric과 기존 Miro API 애플리케이션의 조합이 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Miro 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Miro을 사용하여 인증해야 합니다. Miro을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth을 사용하여 Miro과 통합됩니다. Miro에서 OAuth 애플리케이션을 만들려면 다음 단계를 사용하십시오.

1. OAuth 애플리케이션을 만들려면 Miro 도움말 센터 웹 사이트의 엔터프라이즈 개발자 팀 문서의 앱 생성 및 설치 섹션에 있는 지침을 따르십시오.

2. 앱 생성 대화 상자에서 엔터프라이즈 조직의 개발자 팀을 선택한 후 사용자 인증 토큰 만료 확인란을 선택합니다.

> **Note**
>
> 앱을 만든 후에는 이 옵션을 변경할 수 없으므로 앱을 만들기 전에 이 작업을 수행해야 합니다.

3. 앱 페이지의 OAuth 2.0용 리디렉션 URI 섹션에 다음 형식의 URL을 입력합니다.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

이 URL에는 *<region>*은 AppFabric 앱 번들을 구성한 AWS 리전 에 대한 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 `us-east-1`입니다. 해당 리전의 리디렉션 URL은 `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2`입니다.

4. AppFabric 앱 인증에 사용할 클라이언트 ID와 클라이언트 암호를 복사하고 저장합니다.

필수 범위

Miro OAuth 앱 페이지의 `Permissions` 섹션에 다음 범위를 추가해야 합니다.

- `auditlogs:read`
- `organizations:read`

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Miro 팀 ID입니다. Miro 팀 ID를 찾는 방법에 대한 자세한 내용은 나는 새 Miro 관리자입니다의 자주 묻는 질문 섹션을 참조하십시오. Miro 도움말 센터 웹사이트에서 어디서부터 시작해야 할까요?를 참조하십시오.

테넌트 이름

이 고유한 Miro 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. 클라이언트 ID를 찾으려면 다음 단계를 따르십시오.

1. Miro 프로필 설정으로 이동합니다.
2. 내 앱 탭을 선택합니다.
3. AppFabric과 연결하는 데 사용하는 앱을 선택합니다.
4. 앱 보안 인증 섹션의 클라이언트 ID를 AppFabric의 클라이언트 ID 필드에 입력합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. 클라이언트 암호를 찾으려면 다음 단계를 사용합니다.

1. Miro 프로필 설정으로 이동합니다.
2. 내 앱 탭을 선택합니다.
3. AppFabric과 연결하는 데 사용하는 앱을 선택합니다.
4. 앱 보안 인증 섹션의 클라이언트 암호를 AppFabric의 클라이언트 암호 필드에 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Miro에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricOkta에 대한 구성

Okta는 세계 최고의 아이덴티티 기업입니다. 선도적인 독립 아이덴티티 파트너로서, Okta는 모든 사람이 어디서나, 어떤 디바이스 또는 앱으로든 모든 기술을 안전하게 사용할 수 있도록 합니다. 가장 신뢰할 수 있는 브랜드들은 안전한 액세스, 인증 및 자동화를 가능하게 하는 Okta를 신뢰합니다. Okta Workforce Identity 및 Customer Identity Cloud의 핵심인 유연성과 중립성을 바탕으로 비즈니스 리더와 개발자는 맞춤형 솔루션과 7,000개 이상의 사전 구축된 통합 기능을 통해 혁신에 집중하고 디지털 트랜스포메이션을 가속화할 수 있습니다. Okta는 아이덴티티가 여러분의 소유가 되는 세상을 구축하고 있습니다. 자세한 내용은 okta.com을 참조하세요.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Okta, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

Okta에 대한 AppFabric 지원

AppFabric은 Okta에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Okta로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- AppFabric은 모든 Okta 요금제 유형에서 사용할 수 있습니다.
- Okta 계정에 수퍼 관리자 역할을 가진 사용자가 있어야 합니다.
- AppFabric에서 앱 인증을 승인하는 사용자는 Okta 계정에 수퍼 관리자 역할도 있어야 합니다.

속도 제한 고려 사항

Okta은 Okta API에 속도 제한을 부과합니다. Okta API 속도 제한에 대한 자세한 내용은 Okta 웹사이트의 Okta 개발자 안내서에서 속도 제한을 참조하십시오. AppFabric과 기존 Okta API 애플리케이션의 조합이 Okta의 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Okta 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Okta을 사용하여 인증해야 합니다. Okta을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth를 사용하여 Okta와 통합됩니다. AppFabric과 연결할 OAuth 애플리케이션을 생성하려면 Okta 도움말 센터 웹사이트에서 OIDC 앱 통합 생성의 지침을 따르십시오. 이 구성에는 다음 고려 사항이 적용됩니다.

1. 애플리케이션 유형에서 웹 애플리케이션을 선택합니다.
2. 권한 부여 유형에서 인증 코드 및 새로 고침 토큰을 선택합니다.
3. 다음 형식의 리디렉션 URL을 로그인 리디렉션 URI 및 로그아웃 리디렉션 URI로 사용하십시오.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

이 URL에서 *<region>*은 AppFabric 앱 번들을 구성한 AWS 리전 에 대한 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 us-east-1입니다. 해당 리전의 리디렉션 URL은 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2입니다.

4. 신뢰할 수 있는 출처 구성을 건너뛸 수 있습니다.
5. 제어된 액세스 구성에서 Okta 조직 내 모든 사람에게 액세스 권한을 부여하십시오.

> **Note**
>
> 초기 OAuth 애플리케이션 생성 시 이 단계를 건너뛰면 애플리케이션 구성 페이지의 할당 탭을 사용하여 조직의 모든 사람을 그룹으로 할당할 수 있습니다

6. 다른 모든 옵션은 기본값으로 그대로 둘 수 있습니다.

필수 범위

Okta OAuth 애플리케이션에 다음 범위를 추가해야 합니다.

- okta.logs.read
- okta.users.read

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Okta 도메인입니다. Okta 도메인을 찾는 방법에 대한 자세한 내용은 Okta 웹사이트의 Okta 개발자 안내서에서 Okta 도메인 찾기를 참조하십시오.

테넌트 이름

이 고유한 Okta 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. Okta에서 클라이언트 ID를 찾으려면 다음 단계를 사용하십시오.

1. Okta 개발자 콘솔로 이동합니다.
2. 할당 탭을 선택합니다.
3. 애플리케이션을 선택한 다음 일반 탭을 선택합니다.
4. 클라이언트 보안 인증 섹션으로 스크롤합니다.
5. AppFabric의 클라이언트 ID 필드에 OAuth 클라이언트의 클라이언트 ID를 입력합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. Okta에서 클라이언트 암호를 찾으려면 다음 단계를 사용합니다.

1. Okta 개발자 콘솔로 이동합니다.
2. 할당 탭을 선택합니다.
3. 애플리케이션을 선택한 다음 일반 탭을 선택합니다.
4. 클라이언트 보안 인증 섹션으로 스크롤합니다.
5. AppFabric의 클라이언트 암호 필드에 OAuth 애플리케이션의 클라이언트 암호를 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Okta에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다. Okta 인증을 승인하는 사용자에게는 Okta에 수퍼 관리자 권한이 있어야 합니다.

AppFabricOneLogin by One Identity에 대한 구성

OneLogin by One Identity는 고객 및 파트너의 모든 디지털 ID를 원활하게 관리하는 최신 클라우드 기반 액세스 관리 솔루션입니다. OneLogin은 Single Sign-On(SSO), 다중 인증(MFA), 적응형 인증, 데스크톱 수준 MFA, AD, LDAP, G Suite 및 기타 외부 디렉터리와의 디렉터리 통합, ID 수명 주기 관리 등을 제공합니다. 를 사용하면 가장 일반적인 공격으로부터 조직을 보호하여 보안 강화, 원활한 사용자 경험 및 규제 요구 사항 준수를 보장할 OneLogin수 있습니다.

보안용 AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고OneLogin, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

OneLogin by One Identity에 대한 AppFabric 지원

AppFabric은 OneLogin by One Identity에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 OneLogin by One Identity로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- OneLogin Advanced 또는 Professional 계정이 있어야 합니다.
- 관리자 권한, 위임된 관리자 권한이 있는 사용자가 있어야 합니다.

속도 제한 고려 사항

OneLogin by One Identity는 OneLogin API에 속도 제한을 적용합니다. OneLogin API 속도 제한에 대한 자세한 내용은 OneLogin API 참조의 속도 제한하기를 참조하세요. AppFabric과 기존 OneLogin API 애플리케이션의 조합이 OneLogin의 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다. 그러나 OneLogin 속도 제한을 높일 수 있습니다. 도움이 필요하면 OneLogin by One Identity 계정 관리자에게 문의하거나 One Identity에 문의하세요.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 OneLogin by One Identity 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 OneLogin by One Identity을 사용하여 인증해야 합니다. OneLogin을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth을 사용하여 OneLogin by One Identity과 통합됩니다. OneLogin에서 OAuth 애플리케이션을 생성하려면 다음 단계를 사용합니다.

1. OneLogin 로그인 페이지로 이동하여 로그인합니다.
2. 개발자 메뉴에서 API 보안 인증 정보를 선택합니다.
3. 새 보안 인증 정보를 선택하고 새 보안 인증 정보의 이름을 입력한 다음 모두 읽기를 선택합니다.
4. 저장을 선택합니다. OneLogin은 클라이언트 ID와 클라이언트 암호를 생성합니다.

필수 범위

OneLogin by One Identity OAuth 애플리케이션에 다음 범위를 추가해야 합니다.

- 모두 읽어보세요. 범위 및 클라이언트 보안 인증 정보에 대한 자세한 내용은 OneLogin API 참조의 API 보안 인증 정보로 작업을 참조하세요.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 인스턴스 하위 도메인입니다. 브라우저의 주소 표시줄에서 테넌트 ID를 찾을 수 있습니다. 예를 들어, `subdomain` 는 다음 URL `https://subdomain.onelogin.com`의 테넌트 ID입니다.

테넌트 이름

이 고유한 OneLogin by One Identity 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. OneLogin by One Identity에서 클라이언트 ID를 찾으려면 다음 단계를 사용합니다.

1. OneLogin 로그인 페이지로 이동하여 로그인합니다.
2. 개발자 메뉴에서 API 보안 인증 정보를 선택합니다.
3. API 보안 인증 정보를 선택하여 클라이언트 ID를 가져옵니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. OneLogin by One Identity에서 클라이언트 암호를 찾으려면 다음 단계를 사용합니다.

1. OneLogin 로그인 페이지로 이동하여 로그인합니다.
2. 개발자 메뉴에서 API 보안 인증 정보를 선택합니다.
3. API 보안 인증 정보를 선택하여 클라이언트 암호를 가져옵니다.

클라이언트 앱 인증

AppFabric에서 테넌트 ID와 이름 및 클라이언트 ID와 이름을 사용하여 앱 인증을 생성합니다. 연결을 선택하여 인증을 활성화합니다.

AppFabricPagerDuty에 대한 구성

PagerDuty는 팀이 어떤 신호든 작업으로 전환하여 고객에게 영향을 미치는 문제를 완화하고 문제를 더 빠르게 해결하여 더 효율적으로 작동할 수 있도록 지원하는 디지털 작업 관리 플랫폼입니다. CloudWatch, GuardDuty, CloudTrail, Personal Health Dashboard와 통합합니다.

보안용 AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고PagerDuty, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- PagerDuty에 대한 AppFabric 지원
- AppFabric을 PagerDuty 계정에 연결

PagerDuty에 대한 AppFabric 지원

AppFabric은 PagerDuty에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 PagerDuty로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 감사 로그에 액세스하려면 PagerDuty Business 또는 Digital Operations 요금제를 이용해야 합니다.
- PagerDuty 계정의 글로벌 관리자 또는 계정 소유자여야 합니다.

속도 제한 고려 사항

PagerDuty는 PagerDuty API에 속도 제한을 적용합니다. PagerDuty API 속도 제한에 대한 자세한 내용은 PagerDuty 개발자 플랫폼의 REST API 속도 제한을 참조하세요. AppFabric과 기존 PagerDuty API 애플리케이션의 조합이 PagerDuty의 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 PagerDuty 계정에 연결

PagerDuty 플랫폼은 API 액세스 키를 지원합니다. API 액세스 키를 생성하려면 다음 단계를 사용합니다.

API 액세스 키 생성

AppFabric은 퍼블릭 클라이언트용 API 액세스 키를 사용하여 PagerDuty와 통합됩니다. PagerDuty에서 API 액세스 키를 생성하려면 다음 단계를 사용합니다.

1. PagerDuty 로그인 페이지로 이동하여 로그인합니다.
2. 통합, API 액세스 키를 선택합니다.
3. 새 API 생성을 선택합니다.
4. 설명을 입력한 다음 읽기 전용 API 키를 선택합니다.
5. 키 생성을 선택합니다.
6. API 키를 복사하고 저장합니다. 이는 나중에 AppFabric에서 필요합니다. API 키를 저장하기 전에 페이지를 닫으면 새 API 키를 생성하여 저장해야 합니다. PagerDuty API 속도 제한을 다른 통합과 공유하지 않으려면 이 키를 AppFabric 전용으로 사용해야 합니다.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. PagerDuty 계정의 테넌트 ID는 계정의 기본 URL입니다. 이는 PagerDuty에 로그인하고 웹 브라우저의 주소 표시줄에서 복사하여 확인할 수 있습니다. 테넌트 ID는 다음 형식 중 하나에 해당해야 합니다.

- 미국 계정의 경우, *subdomain*.pagerduty.com
- EU 계정의 경우, *subdomain*.eu.pagerduty.com

테넌트 이름

이 고유한 PagerDuty 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

서비스 계정 토큰

AppFabric은 서비스 계정 토큰을 요청합니다. AppFabric의 서비스 계정 토큰은 API 액세스 키 생성에서 생성한 API 액세스 키입니다.

AppFabricPing Identity에 대한 구성

Ping Identity에서는 모든 사용자에게 성능 저하 없이 안전하고 원활한 디지털 경험을 제공해야 한다고 믿습니다. 원활한 경험을 제공하면서 사용자의 디지털 상호 작용을 보호하기 위해 Fortune 100대 기업 중 절반 이상이 Ping Identity를 선택한 이유가 바로 여기에 있습니다. 2023년 8월 23일, 고객과 파트너에게 더 많은 선택권, 심층적인 전문 지식, 더 완벽한 ID 솔루션을 제공하기 위해 Ping Identity와 ForgeRock이 함께 힘을 모았습니다.

보안용 AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고Ping Identity, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Ping Identity에 대한 AppFabric 지원
- AppFabric을 Ping Identity 계정에 연결

Ping Identity에 대한 AppFabric 지원

AppFabric은 Ping Identity에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Ping Identity로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 에센셜, 플러스 또는 프리미엄 Ping Identity 계정이 있어야 합니다. 해당 Ping Identity 요금제 유형을 만들거나 업그레이드하는 방법에 대한 자세한 내용은 Ping Identity 웹 사이트의 모든 기능에 대한 Ping Identity 요금을 참조하십시오.
- Ping Identity 계정에는 ID 데이터 읽기 전용 역할이 있어야 합니다. 애플리케이션에 역할을 부여하여 계정에 역할을 추가할 수 있습니다. 역할에 대한 자세한 내용은 Ping Identity 지원 웹 사이트의 역할을 참조하세요.

속도 제한 고려 사항

Ping Identity는 속도 제한을 게시하지 않습니다. 지원 사례를 작성하거나 Ping Identity 고객 성공 팀에 문의해야 합니다. AppFabric과 기존 Ping Identity API 애플리케이션의 조합이 Ping Identity의 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Ping Identity 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Ping Identity을 사용하여 인증해야 합니다. Ping Identity을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth을 사용하여 Ping Identity과 통합됩니다. Ping Identity에서 OAuth 애플리케이션을 생성하려면 다음 단계를 사용합니다.

1. Ping Identity 웹 사이트의 PingOne 개발자용 가이드에서 애플리케이션 연결 생성 섹션의 지침을 따릅니다.
2. 애플리케이션을 생성한 후 권한 부여 유형을 사용자 지정합니다.
    a. 애플리케이션에 로그인한 후 구성 탭을 선택하고 연필 아이콘을 클릭하여 기존 구성을 변경합니다.
    b. 권한 부여 유형에서 인증 코드를 선택합니다. PKCE 시행을 선택 사항으로 유지합니다.
    c. 새로 고침 토큰을 선택하고 새로 고침 기간을 선택합니다.
3. 리디렉션 URL, 콜백 URL에서 다음 형식의 리디렉션 URL을 앱 리디렉션 URL로 사용합니다.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

이 URL에서 *<region>*은 AppFabric 앱 번들을 구성한 AWS 리전 에 대한 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 us-east-1입니다. 해당 리전의 리디렉션 URL은 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2입니다.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Ping Identity 인스턴스 이름입니다. 브라우저의 주소 표시줄에서 테넌트 ID를 찾을 수 있습니다. 예를 들어 *API_PATH*/v1/environments/*environmentID*입니다. 여기서 *API_PATH* 는 PingOne 서버의 지역 도메인(예:api.pingone.com, *environmentID*)을 나타내며 애플리케이션 환경 속성에 표시된 환경 ID를 나타냅니다. 환경 속성에 대한 자세한 내용은 Ping Identity 웹 사이트의 환경 속성을 참조하세요.

테넌트 이름

이 고유한 Ping Identity 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. Ping Identity에서 클라이언트 ID를 찾으려면 다음 단계를 사용합니다.

1. PingOne 관리 콘솔에 로그인하고 애플리케이션을 선택합니다.
2. 목록에서 애플리케이션을 선택합니다.
3. 개요 탭을 선택한 다음 클라이언트 ID 값을 찾습니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. Ping Identity에서 클라이언트 암호를 찾으려면 다음 단계를 사용합니다.

1. PingOne 관리 콘솔에 로그인하고 애플리케이션을 선택합니다.
2. 목록에서 애플리케이션을 선택합니다.
3. 개요 탭을 선택한 다음 클라이언트 암호 값을 찾습니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Ping Identity에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricSalesforce에 대한 구성

Salesforce는 기업이 더 많은 잠재 고객을 찾고, 더 많은 거래를 체결하고, 고객에게 놀라운 서비스를 제공하는 데 도움이 되도록 설계된 클라우드 기반 소프트웨어를 제공합니다. Salesforce's Customer 360은 완벽한 제품 제품군을 제공하고, 영업, 서비스, 마케팅, 상거래 및 IT 팀을 고객 정보에 대한 단일의 공유된 관점으로 통합하여 조직이 고객 및 직원과의 관계를 성장시키는 데 도움을 줍니다.

AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고Salesforce, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, 데이터를 Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림으로 출력할 수 있습니다.

주제

- Salesforce에 대한 AppFabric 지원
- AppFabric을 Salesforce 계정에 연결

Salesforce에 대한 AppFabric 지원

AppFabric은 Salesforce에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Salesforce로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 성능, 엔터프라이즈 또는 무제한 에디션이 있어야 합니다Salesforce. 이러한 에디션 중 하나로 업그레이드Salesforce하려면에 문의하세요.
- AppFabric이의 전체 로그 이벤트 세트가 포함된 시간당 이벤트 로그 파일을 전송하도록 Salesforce 하려면의 Shield 기능의 일부로 이벤트 모니터링을 구독해야 합니다Salesforce. 그렇지 않으면 AppFabric은 Salesforce's 표준 일일 로그 파일에서 제한된 이벤트(예: 로그인, 로그아웃, InsecureExternalAssets, API 총 사용량, CORS 위반 및 HostnameRedirects ELF 이벤트)를 전송합니다. 설정 > 이벤트 관리자로 이동하여 Salesforce 계정이 이미 Shield 기능을 구독하고 있는지 확인할 수 있습니다. 19개 이상의 이벤트가 나열되면 계정이 이벤트 모니터링을 구독합니다. 이벤트 모니터링이 없는 경우에 문의하여이 추가 기능에 대한 구독을 구매할 수 있습니다Salesforce.
- Salesforce 설정에서 이벤트 로그 파일 생성을 옵트인해야 합니다.

- 시스템 관리자 프로필을 사용하여 OAuth 애플리케이션을 생성하고 AppFabric에 대해 동일한 자격 증명으로 로그인해야 합니다.

> **Note**
>
> API 총 사용량, CORS 위반 레코드, 호스트 이름 리디렉션, 안전하지 않은 외부 자산, 로그인 및 로그아웃 이벤트는 지원되는 에디션에서 추가 비용 없이 사용할 수 있습니다Salesforce. 나머지 이벤트 유형을 구매Salesforce하려면에 문의하세요. Salesforce 이벤트 유형에 대한 자세한 내용은 Salesforce 웹 사이트의 EventLogFile 지원 이벤트 유형을 참조하세요.
> AppFabric은 로그 파일 인스턴스당 이벤트 유형당 최대 100,000개의 이벤트를 지원할 수 있습니다(이벤트 모니터링 추가 기능 구독에 따라 매일 또는 시간당). 로그 파일이 임계값을 초과하면 전체 로그 파일이 수집에서 제외될 수 있습니다.

속도 제한 고려 사항

Salesforce는 Salesforce API에 속도 제한을 부과합니다. Salesforce API 속도 제한에 대한 자세한 내용은 Salesforce 웹 사이트의 API 요청 제한 및 할당을 참조하세요. AppFabric과 기존 Salesforce API 애플리케이션의 조합이 Salesforce's 제한을 초과하면 AppFabric에 나타나는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 대상으로 전달되려면 일일 로그 파일에서 최대 6시간 지연 또는 시간당 로그 파일에서 최대 29시간 지연이 표시될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Salesforce 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Salesforce을 사용하여 인증해야 합니다. Salesforce을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth를 사용하여 Salesforce와 통합됩니다. Salesforce에서 OAuth 애플리케이션을 생성하려면 다음 단계를 사용하십시오.

1. Salesforce 계정에 로그인합니다.
2. Salesforce 설명서에 설명된 대로 설정 페이지로 이동합니다.

3. 빠른 찾기에서 App Manager를 검색합니다.
4. 새 연결된 앱을 선택합니다.
5. 양식 필드에 필수 정보를 입력합니다.
6. OAuth 설정 활성화를 선택합니다.
7. 다음 옵션을 꺼야 합니다.

   - 지원되는 권한 부여 흐름을 위해 코드 교환(PKCE) 확장을 위한 증명 키 필요
   - 웹 서버 흐름에 보안 암호 필요
   - 새로 고침 토큰 흐름에 보안 암호 필요
   - 새로 고침 토큰 교체 활성화
8. 콜백 URL 텍스트 상자에 다음 형식의 URL을 입력하고 변경 사항 저장을 선택합니다.

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   이 URL에서 *<region>*은 AppFabric 앱 번들을 구성한 AWS 리전 에 대한 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 `us-east-1`입니다. 해당 리전의 리디렉션 URL은 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`입니다.
9. 필요에 따라 범위를 입력합니다(다음 필수 범위 섹션에 설명됨). 다른 모든 필드는 기본값으로 남겨둘 수 있습니다.
10. 저장을 선택합니다.
11. 다음 단계를 완료하여 새 OAuth 앱의 새로 고침 토큰 정책을 확인합니다.

    a. 설정 페이지의 빠른 찾기 텍스트 상자에 연결된 앱을 입력한 다음 연결된 앱 관리를 선택합니다.

    b. 새로 생성된 앱 옆에 있는 편집을 선택합니다.

    c. 취소된 옵션이 선택될 때까지 새로 고침 토큰이 유효한지 확인합니다.

    d. 변경 내용을 저장합니다.
12. 다음 단계를 완료하여 감사 로그가 생성되고 있는지 확인합니다.

    a. 설정 페이지의 빠른 찾기 텍스트 상자에 이벤트 로그 파일을 입력한 다음 이벤트 로그 파일 브라우저를 선택합니다.

    b. 이벤트 로그가 이벤트 로그 파일 브라우저에 나열되어 있는지 확인합니다.
13. 생성된 앱으로 이동하여 드롭다운에서 보기를 선택합니다.
14. 소비자 세부 정보 관리(Manage Consumer Details)를 선택합니다.

자격 증명을 확인해야 하는 새 탭으로 리디렉션됩니다. 이 탭에서 소비자 키 및 소비자 보안 암호 값을 기록해 둡니다. 나중에 로그인하려면이 정보가 필요합니다.

필수 범위

Salesforce OAuth 애플리케이션에 다음 범위를 추가해야 합니다.

- APIs(API)를 통해 사용자 데이터를 관리합니다.
- 언제든지 요청을 수행합니다(`refresh_token` 및 `offline_access`).

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Salesforce 내 도메인의 하위 도메인입니다. 내 도메인 하위 도메인은 `https://`와 사이의 브라우저 주소 표시줄에서 찾을 수 있습니다`.my.salesforce.com`.

Salesforce 내 도메인을 찾으려면 Salesforce 홈 화면에서 다음 지침을 사용합니다.

1. Salesforce 설명서에 설명된 대로 설정 페이지로 이동합니다.
2. 빠른 찾기에서 회사 설정을 검색하고 결과에서 내 도메인을 선택합니다.

테넌트 이름

이 고유한 Salesforce 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. Salesforce에서 클라이언트 ID를 찾으려면 다음 단계를 사용하십시오.

1. 설정 페이지로 이동합니다.
2. 설정을 선택한 다음 앱 관리자를 선택합니다.
3. 생성된 앱을 선택하고 드롭다운 메뉴에서 보기를 선택합니다.
4. 소비자 세부 정보 관리(Manage Consumer Details)를 선택합니다. 새 탭으로 리디렉션됩니다.
5. 자격 증명을 확인한 다음 소비자 키 값을 찾습니다.

6. AppFabric의 클라이언트 ID 필드에 소비자 키를 입력합니다.

클라이언트 보안 암호(client secret)

AppFabric은 클라이언트 암호를 요청합니다. AppFabric의 클라이언트 보안 암호는의 소비자 보안 암호입니다Salesforce. 에서 보안 암호를 찾으려면 다음 단계를 Salesforce사용합니다.

1. 설정 페이지로 이동합니다.
2. 설정을 선택한 다음 앱 관리자를 선택합니다.
3. 생성된 앱을 선택하고 드롭다운 메뉴에서 보기를 선택합니다.
4. 소비자 세부 정보 관리(Manage Consumer Details)를 선택합니다. 새 탭으로 리디렉션됩니다.
5. 자격 증명을 확인한 다음 소비자 보안 암호 값을 찾습니다.
6. AppFabric의 클라이언트 보안 암호 필드에 소비자 보안 암호를 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Salesforce에서 인증을 승인하라는 팝업창이 뜹니다. 승인 페이지에서 Salesforce 시스템 관리자 역할 또는 권한을 부여하는 동안 이벤트 로그 파일 보기 및 API 활성화 Salesforce 사용자 권한이 있는 사용자를 사용해야 합니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricServiceNow에 대한 구성

ServiceNow는 엔터프라이즈 IT 운영을 자동화하는 클라우드 기반 서비스를 제공하는 선두 업체입니다. ServiceNow의 ITOM을 통해 기업은 가상화 및 클라우드 인프라를 포함한 전체 IT 환경을 완벽하게 파악하고 제어할 수 있습니다. 이는 서비스 매핑, 제공 및 보장을 간소화하여 IT 서비스 및 인프라 데이터를 단일 기록 시스템으로 통합합니다. 또한 이벤트, 사고, 문제, 구성 및 변경 관리를 포함한 주요 프로세스를 자동화하고 간소화합니다.

보안용 AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고ServiceNow, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- ServiceNow에 대한 AppFabric 지원
- 데이터 지연 고려 사항
- AppFabric을 ServiceNow 계정에 연결

ServiceNow에 대한 AppFabric 지원

AppFabric은 ServiceNow에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 ServiceNow로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- AppFabric은 모든 ServiceNow 요금제 유형에서 사용할 수 있습니다.
- ServiceNow 계정에 관리자 역할을 가진 사용자가 있어야 합니다.
- ServiceNow 인스턴스가 있어야 합니다.

속도 제한 고려 사항

ServiceNow는 ServiceNow API에 속도 제한을 부과합니다. ServiceNow API 속도 제한에 대한 자세한 내용은 ServiceNow 웹사이트의 인바운드 REST API 속도 제한을 참조하십시오. AppFabric과 기존 ServiceNow API 애플리케이션의 조합이 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 ServiceNow 계정에 연결

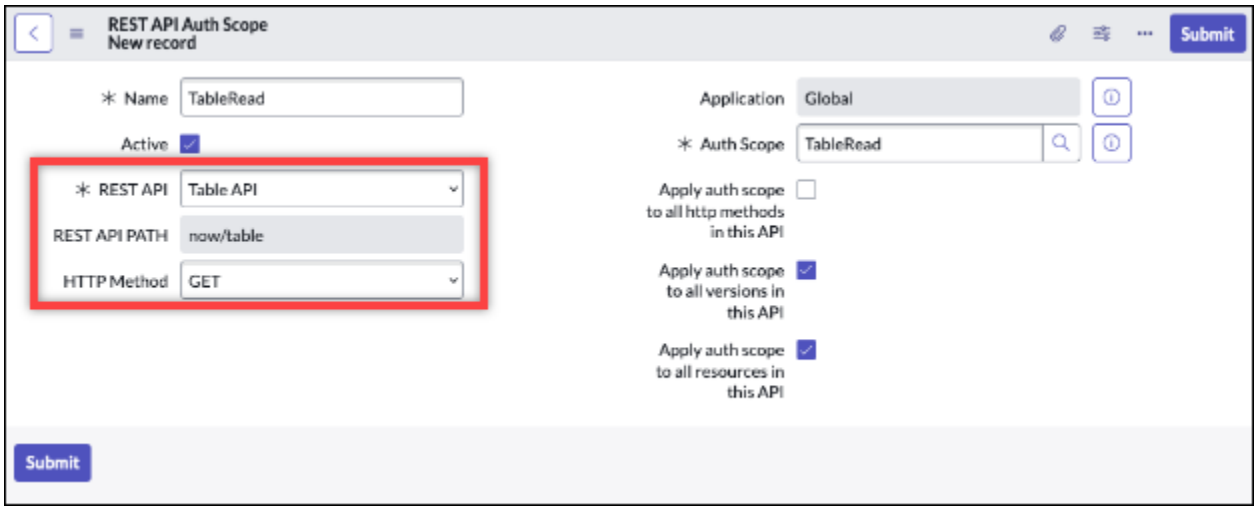
AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 ServiceNow을 사용하여 인증해야 합니다. 다음 단계를 사용하여 AppFabric으로 ServiceNow을 인증하는 데 필요한 정보를 찾을 수 있습니다.

OAuth 애플리케이션 생성

Now Platform는 퍼블릭 클라이언트가 액세스 토큰을 생성할 수 있도록 OAuth 2.0 - 권한 부여 유형을 지원합니다.

1. OAuth 애플리케이션을 등록하십시오. 이를 위해 다음 3단계를 수행해야 합니다. 이 단계를 완료하는 방법에 대한 자세한 내용은 ServiceNow 웹사이트의 ServiceNow에 애플리케이션 등록을 참조하십시오.

a. 앱을 등록하고 다음 예와 같이 인증 범위가 now/table의 REST API 경로와 GET의 HTTP 메서드를 사용하여 테이블 API에 액세스할 수 있는지 확인합니다.



b. 인증 코드를 생성합니다.

c. 인증 코드를 사용하여 베어러 토큰을 생성합니다.

2. 다음 형식의 리디렉션 URL을 사용합니다.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

이 URL에서 *<region>*은 AppFabric 앱 번들을 구성한 AWS 리전 에 대한 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 `us-east-1`입니다. 해당 리전의 리디렉션 URL은 `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2`입니다.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 인스턴스 이름입니다. 브라우저의 주소 표시줄에서 테넌트 ID를 찾을 수 있습니다. 예를 들어, *`example`* 는 다음 URL `https://`*`example`*`.service-now.com`의 테넌트 ID입니다.

테넌트 이름

이 고유한 ServiceNow 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트의 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. ServiceNow에서 클라이언트 ID를 찾으려면 다음 단계를 따르십시오.

1. ServiceNow 콘솔로 이동합니다.
2. 시스템 OAuth를 선택한 다음 애플리케이션 레지스트리 탭을 선택합니다.
3. 애플리케이션을 선택합니다.
4. AppFabric의 클라이언트 ID 필드에 OAuth 클라이언트의 클라이언트 ID를 입력합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. ServiceNow에서 클라이언트 암호를 찾으려면 다음 단계를 따르십시오.

1. ServiceNow 콘솔로 이동합니다.
2. 시스템 OAuth를 선택한 다음 애플리케이션 레지스트리 탭을 선택합니다.
3. 애플리케이션을 선택합니다.
4. AppFabric의 클라이언트 암호 필드에 OAuth 애플리케이션의 클라이언트 암호를 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 ServiceNow에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricSingularity Cloud에 대한 구성

Singularity Cloud 플랫폼은 모든 단계에서 모든 범주의 위협으로부터 기업을 보호합니다. 특허를 받은 인공 지능은 알려진 서명 및 패턴의 보안을 제로데이 및 랜섬웨어와 같은 가장 정교한 공격으로 확장합니다.

AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고Singularity Cloud, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, 데이터를 Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림으로 출력할 수 있습니다.

> **Note**
>
> Singularity Cloud 설명서는 Singularity Cloud 계정에 로그인한 후에만 액세스할 수 있습니다. 따라서이 문서의 Singularity Cloud 설명서에 직접 연결할 수 없습니다.

주제

Singularity Cloud에 대한 AppFabric 지원

AppFabric은 Singularity Cloud에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여에서 지원되는 대상으로 감사 로그Singularity Cloud를 전송하려면 Singularity Cloud 계정에 관리자 역할이 있어야 합니다. Singularity Cloud API 속도 제한에 대한 자세한 내용은 Singularity Cloud 계정에 로그인하고 설명서 섹션을 찾아 역할을 검색하세요.

속도 제한 고려 사항

Singularity Cloud는 Singularity Cloud API에 속도 제한을 적용합니다. Singularity Cloud API 속도 제한에 대한 자세한 내용은 Singularity Cloud 계정에 로그인하고, 설명서 섹션을 검색하고, API 속도 제한을 검색하세요.

데이터 지연 고려 사항

감사 이벤트가 대상으로 전달되는 데 최대 30분의 지연이 발생할 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Singularity Cloud 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Singularity Cloud을 사용하여 인증해야 합니다. Singularity Cloud을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

에 대한 API 토큰 생성 Singularity Cloud

서비스 사용자와 연결된 API 토큰을 생성하려면 다음 절차를 완료하세요. API 토큰은 특정 콘솔 사용자 또는 이메일 주소에 연결되지 않습니다.

> **Note**
>
> 서비스 사용자 API 토큰이 만료되기 전이나 후에 새 사용자를 생성하거나 서비스 사용자를 복사하여 새 API 토큰을 가져옵니다.

1. Singularity Cloud 계정에 로그인합니다.
2. 설정 도구 모음에서 사용자를 선택한 다음 서비스 사용자를 선택합니다.
3. 작업을 선택한 다음 새 서비스 사용자 생성을 선택합니다.
4. 새 서비스 사용자 생성 페이지에서 서비스 사용자의 이름, 설명 및 만료 날짜를 입력합니다.
5. 다음을 선택합니다.
6. 액세스 범위 선택 섹션에서 범위를 선택합니다.
   - 액세스 수준에 대한 계정을 선택합니다.
   - 감사 로그를 가져올 계정을 선택합니다.
7. 사용자 생성을 선택합니다.

   API 토큰이 생성됩니다. 창이 열리고 토큰을 마지막으로 볼 수 있음을 나타내는 메시지와 함께 토큰 문자열이 표시됩니다.
8. (선택 사항) API 토큰 복사를 선택하고 안전한 위치에 저장합니다.
9. 닫기를 선택하세요.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 서비스에 로그인하는 Sentinel One 웹 사이트 주소의 하위 도메인입니다. 예를 들어`example-company-1.sentinelone.net`, 주소에서 Singularity Cloud 계정에 로그인하는 경우 테넌트 ID는 입니다`example-company-1`.

테넌트 이름

이 고유한 Singularity Cloud 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

서비스 계정 토큰

이 가이드의 에 대한 API 토큰 생성 Singularity Cloud 섹션에 있는 단계를 사용하여 생성한 토큰을 사용합니다. 토큰을 분실했거나 찾을 수 없는 경우 동일한 단계를 다시 수행하여 새 토큰을 생성할 수 있습니다.

> **Note**
>
> AppFabric이 감사 로그를 수집하는 동안 Singularity Cloud 콘솔에서 새 API 토큰이 생성되면 수집이 중지됩니다. 이 경우 앱 인증을 새 API 토큰으로 업데이트하여 감사 로그 수집을 재개해야 합니다.

AppFabricSlack에 대한 구성

Slack는 사람들의 업무 생활을 더 단순하고, 더 즐겁고, 생산적으로 만드는 것을 사명으로 삼고 있습니다. 코드 없는 자동화를 통해 모든 사람에게 역량을 부여하고, 검색 및 지식 공유를 원활하게 하며, 팀이 함께 작업을 진행하면서 연결 및 참여를 유지함으로써 성과를 향상시키는 고객 기업용 생산성 플랫폼입니다. Salesforce의 일환으로 Slack는 Salesforce Customer 360에 긴밀하게 통합되어 영업, 서비스 및 마케팅 팀 전반의 생산성을 극대화합니다. 자세히 알아보고 Slack을 무료로 시작하려면 slack.com을 방문하세요.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Slack, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Slack에 대한 AppFabric 지원
- AppFabric을 Slack 계정에 연결

Slack에 대한 AppFabric 지원

AppFabric은 Slack에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Slack로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Slack을 사용하는 Enterprise Grid 요금제가 포함되어 있어야 합니다. 자세한 내용은 Slack 웹사이트의 Slack 엔터프라이즈 그리드 소개를 참조하십시오.
- Slack 계정에 조직 소유자 역할을 가진 사용자가 있어야 합니다. 역할에 대한 자세한 내용은 Slack 웹사이트의 Slack 도움말 센터에서 Slack에서의 역할 유형을 참조하십시오.

속도 제한 고려 사항

Slack은 Slack API에 속도 제한을 부과합니다. Slack API 속도 제한에 대한 자세한 내용은 Slack 웹사이트의 Slack API 사용 가이드에서 속도 제한을 참조하십시오. AppFabric과 기존 Slack API 애플리케이션의 조합이 한도를 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Slack 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Slack을 사용하여 인증해야 합니다. Slack을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth를 사용하여 Slack와 통합됩니다. OAuth 앱을 만드는 방법에는 두 가지가 있습니다. 하나는 앱 매니페스트 사용이고 다른 하나는 처음부터 새로 만들기입니다. Slack에서 OAuth 애플리케이션을 생성하려면 다음 단계를 사용하십시오.

Using an app manifest

1. 브라우저의 Slack 앱 관리 UI로 이동합니다.
2. 새 앱 생성을 선택합니다.
3. 앱 매니페스트에서를 선택합니다.
4. AppFabric을 승인하려는 워크스페이스를 선택합니다.

5. 아래 앱 매니페스트 입력 상자에서 JSON을 선택하고 기존 JSON을 다음으로 바꿉니다. *<region>*을 적절한 로 바꿉니다 AWS 리전 (예: *us-east-1*).

```
{
    "display_information": {
        "name": "AppFabric"
    },
    "oauth_config": {
        "redirect_urls": [
            "https://<region>.console.aws.amazon.com/appfabric/oauth2"
        ],
        "scopes": {
            "user": [
                "auditlogs:read",
                "users:read.email",
                "users:read"
            ]
        }
    },
    "settings": {
        "org_deploy_enabled": false,
        "socket_mode_enabled": false,
        "token_rotation_enabled": true
    }
}
```

6. 기본 정보 페이지에서 클라이언트 ID와 클라이언트 암호를 복사하여 저장합니다.
7. `auditLogs:read` 범위 내에서 앱의 공개 배포를 활성화해야 합니다. 자세한 내용은 Slack 웹 사이트의 공개 배포 활성화를 참조하십시오.

From scratch

1. 앱 생성 화면에서 처음부터 새로 만들기를 선택합니다.
2. 앱 이름을 지정하고 워크스페이스를 선택합니다.
3. 기본 정보 페이지에서 클라이언트 ID와 클라이언트 암호를 복사하여 저장합니다.
4. OAuth 및 권한 페이지에서 토큰 교체를 통한 고급 토큰 보안 옵션을 선택합니다.
5. OAuth 및 권한 페이지의 리디렉션 URL 섹션에 다음 형식의 URL을 추가합니다.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

이 URL에서 *<region>*는 AppFabric 앱 번들을 구성한 AWS 리전 의 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 `us-east-1`입니다. 해당 리전의 리디렉션 URL은 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`입니다.

6. `auditLogs:read` 범위 내에서 앱의 공개 배포를 활성화해야 합니다. 자세한 내용은 Slack 웹사이트의 공개 배포 활성화를 참조하십시오.

필수 범위

> **Note**
>
> 이 섹션은 OAuth 앱을 처음부터 만들기로 선택한 경우에만 적용됩니다. 앱 매니페스트를 사용하여 애플리케이션 인증을 생성하기로 선택한 경우 이 섹션을 건너뛰십시오.

Slack OAuth 애플리케이션의 OAuth 및 권한 페이지에 다음과 같은 사용자 토큰 범위를 추가해야 합니다.

- `auditlogs:read`
- `users:read.email`
- `users:read`

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Slack 워크스페이스 ID입니다. 테넌트 ID를 얻으려면 Slack 웹사이트의 Slack 도움말 센터에서 Slack URL 찾기의 지침을 따르십시오. Slack 워크스페이스 URL의 형식은 `examplecorp.slack.com` 또는 `examplecorp.enterprise.slack.com`와 비슷합니다. 필요한 테넌트 ID는 `.slack.com` 또는 `.enterprise.slack.com`가 없는 `examplecorp`입니다.

테넌트 이름

Slack 워크스페이스 ID를 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 Slack OAuth 애플리케이션에서 클라이언트 ID를 요청합니다. 클라이언트 ID를 찾으려면 다음 단계를 사용합니다.

1. 브라우저의 Slack 앱 관리 UI로 이동합니다.
2. AppFabric과 함께 사용하는 OAuth 애플리케이션을 선택합니다.
3. 기본 정보 페이지의 클라이언트 ID를 AppFabric의 클라이언트 ID 필드에 입력합니다.

클라이언트 암호

AppFabric은 Slack OAuth 애플리케이션에 클라이언트 암호를 요청합니다. 클라이언트 암호를 찾으려면 다음 단계를 사용합니다.

1. 브라우저의 Slack 앱 관리 UI로 이동합니다.
2. AppFabric과 함께 사용하는 OAuth 애플리케이션을 선택합니다.
3. 기본 정보 페이지의 클라이언트 암호를 AppFabric의 클라이언트 암호 필드에 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Slack에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricSmartsheet에 대한 구성

Smartsheet는 기업 전반에서 업무, 사람, 기술을 조율하는 데 도움이 되는 업무 관리 플랫폼입니다. Smartsheet는 누구나 프로젝트를 관리하고, 워크플로를 자동화하고, 규모에 맞게 솔루션을 신속하게 구축할 수 있도록 강력한 엔터프라이즈급 기능 세트를 제공하여 보안 및 규정 준수를 유지하면서 혁신을 위한 환경을 조성할 수 있습니다.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Smartsheet, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Smartsheet에 대한 AppFabric 지원
- AppFabric을 Smartsheet 계정에 연결

Smartsheet에 대한 AppFabric 지원

AppFabric은 Smartsheet에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Smartsheet로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Smartsheet 비즈니스, 엔터프라이즈 또는 어드밴스 계정이 있어야 합니다. Smartsheet 계정 생성 또는 업그레이드에 대한 자세한 내용은 Smartsheet 웹사이트의 Smartsheet 가격 책정 또는 Smartsheet 고급을 참조하십시오.
- Smartsheet 개발자 등록 절차를 완료해야 합니다.

속도 제한 고려 사항

Smartsheet은 Smartsheet API에 속도 제한을 부과합니다. Smartsheet API 속도 제한에 대한 자세한 내용은 Smartsheet 웹사이트의 Smartsheet API 참조에서 속도 제한을 참조하십시오.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Smartsheet 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Smartsheet을 사용하여 인증해야 합니다. Smartsheet을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth을 사용하여 Smartsheet과 통합됩니다. Smartsheet에서 OAuth 애플리케이션을 생성하려면 다음 단계를 사용하십시오.

1. Smartsheet 계정에서 개발자 도구를 탐색합니다.
2. 개발자 도구 화면에서 새 앱 생성을 선택합니다.
3. 새 앱 생성 화면의 모든 입력 필드를 작성합니다.

4. 앱 URL 및 앱 연락처/지원에는 임의의 고유한 값을 사용합니다.
5. 다음 형식의 리디렉션 URL을 앱 리디렉션 URL로 사용합니다.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

이 URL에서 *<region>*는 AppFabric 앱 번들을 구성한 AWS 리전 의 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 us-east-1입니다. 해당 리전의 리디렉션 URL은 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2입니다.

6. 저장을 선택합니다.
7. 앱 클라이언트 ID와 앱 암호를 복사하여 저장합니다.

필수 범위

Smartsheet에서는 OAuth 구성에 범위를 명시적으로 추가할 필요가 없습니다. AppFabric은 Smartsheet 계정에 대한 인증 요청에서 다음 범위를 요청합니다.

- READ_EVENTS
- READ_USERS

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Smartsheet 계정 ID입니다.

테넌트 이름

AppFabric은 테넌트 ID를 요청합니다. Smartsheet 계정을 고유하게 식별하는 모든 값을 입력합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. AppFabric의 클라이언트 ID는 Smartsheet 앱 클라이언트 ID입니다. Smartsheet에서 앱 클라이언트 ID를 찾으려면 다음 단계를 사용하십시오.

1. Smartsheet 계정에서 개발자 도구를 탐색합니다.
2. AppFabric과 연결하는 데 사용하는 OAuth 애플리케이션을 선택합니다.
3. 앱 프로필 화면의 앱 클라이언트 ID를 AppFabric의 클라이언트 ID 필드에 입력합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. AppFabric의 클라이언트 암호는 Smartsheet 앱 암호입니다. Smartsheet에서 앱 암호를 찾으려면 다음 단계를 사용합니다.

1. Smartsheet 계정에서 개발자 도구를 탐색합니다.
2. AppFabric과 연결하는 데 사용하는 OAuth 애플리케이션을 선택합니다.
3. 앱 프로필 화면의 앱 암호를 AppFabric의 클라이언트 암호 필드에 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Smartsheet에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricTerraform Cloud에 대한 구성

HashiCorp Terraform Cloud는 세계에서 가장 널리 사용되는 멀티 클라우드 프로비저닝 제품입니다. Terraform 에코시스템에는 3,000개 이상의 공급자, 14,000개 모듈 및 2억 5천만 개의 다운로드가 있습니다. Terraform Cloud는를 채택하는 가장 빠른 방법으로Terraform, 실무자, 팀 및 글로벌 기업이 인프라를 생성하고 협업하며 보안, 규정 준수 및 운영 제약에 대한 위험을 관리하는 데 필요한 모든 것을 제공합니다.

보안용 AWS AppFabric을 사용하여에서 감사 로그 및 사용자 데이터를 수신하고Terraform Cloud, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Terraform Cloud에 대한 AppFabric 지원
- AppFabric을 Terraform Cloud 계정에 연결

Terraform Cloud에 대한 AppFabric 지원

AppFabric은 Terraform Cloud에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Terraform Cloud로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- 감사 로그에 액세스하려면 Terraform Cloud Plus Edition 플랜이 있고 조직의 소유자여야 합니다. Terraform Cloud 플랜에 대한 자세한 내용은 HashiCorp Terraform 웹 사이트의 Terraform 요금을 참조하세요.
- TBD 감사 로그는 Terraform Cloud 계정에서 생성할 수 있는 조직에 사용할 수 있습니다.

속도 제한 고려 사항

Terraform Cloud는 Terraform Cloud API에 속도 제한을 적용합니다. Terraform Cloud API 속도 제한에 대한 자세한 내용은 Terraform Cloud 웹 사이트의 Terraform Cloud 개발자 관리 일반 설정에서 API 속도 제한을 참조하세요. AppFabric과 기존 Terraform Cloud API 애플리케이션의 조합이 Terraform Cloud의 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Terraform Cloud 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Terraform Cloud을 사용하여 인증해야 합니다. Terraform Cloud을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

조직 API 토큰 생성

AppFabric은 조직 API 토큰을 Terraform Cloud 사용하여와 통합됩니다. Terraform Cloud 조직 API 토큰에 대한 자세한 내용은 조직 API 토큰을 참조하세요. 조직을 생성하려면 조직 생성의 지침을 따릅니다. 에서 조직 API 토큰을 생성하려면 다음 단계를 Terraform Cloud사용합니다.

1. Terraform Cloud 로그인 페이지로 이동하여 로그인합니다.
2. 왼쪽 패널에서 조직, 설정을 선택한 다음 API 토큰을 선택합니다.
3. 조직 토큰에서 조직 토큰 생성을 선택한 다음 토큰 생성을 선택합니다.
4. (선택 사항) 토큰의 만료 날짜 또는 시간을 입력하거나 만료되지 않는 토큰을 생성합니다.
5. 토큰을 복사하고 저장합니다. 이는 나중에 AppFabric에서 필요합니다. 토큰을 저장하기 전에 페이지를 닫는 경우 이전 토큰을 취소하고 새 토큰을 생성해야 합니다.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. Terraform Cloud 계정의 테넌트 ID는 계정의 현재 조직 URL입니다. 조직에 로그인하고 현재 Terraform Cloud 조직 URL을 복사하여 이를 찾을 수 있습니다. 테넌트 ID는 다음 형식 중 하나에 해당해야 합니다.

```
https://app.terraform.io/app/organization_URL
```

테넌트 이름

이 고유한 Terraform Cloud 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

서비스 계정 토큰

AppFabric은 서비스 계정 토큰을 요청합니다. AppFabric의 서비스 계정 토큰은에서 생성한 조직 API 토큰입니다조직 API 토큰 생성.

AppFabricWebex by Cisco에 대한 구성

Cisco은 인터넷을 촉진하는 기술 분야의 세계적인 선두 주자입니다. Cisco 애플리케이션을 재구상하고, 데이터를 보호하고, 인프라를 혁신하고, 글로벌하고 포용적인 미래를 위해 팀의 역량을 강화함으로써 새로운 가능성에 영감을 줍니다.

정보 Webex by Cisco

Webex은 화상 회의, 통화, 메시지, 이벤트, 컨택 센터와 같은 고객 경험 솔루션과 목적에 맞게 제작된 협업 장치를 포함하는 클라우드 기반 협업 솔루션의 선도적인 공급업체입니다. Webex은 포괄적인 협업 경험을 제공하는 데 중점을 두고 AI와 기계 학습을 활용하는 혁신을 촉진하여 지리, 언어, 성격, 기술에 대한 친숙함의 장벽을 제거하는 데 도움이 됩니다. 이 솔루션은 설계상 보안 및 개인 정보 보호를 기반으로 합니다. Webex은 단일 애플리케이션 및 인터페이스를 통해 제공되는 세계 최고의 비즈니스 및 생산성 앱과 함께 작동합니다. 자세히 알아보려면 webex.com을 참조하세요.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Webex, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Webex에 대한 AppFabric 지원

- AppFabric을 Webex 계정에 연결

Webex에 대한 AppFabric 지원

AppFabric은 Webex에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Webex로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Collaboration Flex 요금제, Meet 요금제, Call 요금제 이상이 있어야 합니다. 해당 Webex 요금제 유형을 만들거나 업그레이드하는 방법에 대한 자세한 내용은 Webex 웹 사이트의 모든 기능에 대한 Webex 요금을 참조하십시오.
- Cisco AuditLog API 중 하나에서 제공하는 보안 감사 이벤트에 액세스하려면 계정에 Pro Pack 라이선스가 있어야 합니다.
- 조직 관리자 > 전체 관리자 역할을 가진 사용자가 있어야 합니다.
- 전체 관리자를 위한 관리자 역할 구성에는 규정 준수 책임자 옵션이 활성화되어 있어야 합니다.

속도 제한 고려 사항

Webex는 Webex API에 속도 제한을 부과합니다. Webex API 속도 제한에 대한 자세한 내용은 Webex 웹 사이트의 Webex 개발자 안내서에서 속도 제한을 참조하십시오. AppFabric과 기존 Webex API 애플리케이션의 조합이 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Webex 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Webex을 사용하여 인증해야 합니다. Webex을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth을 사용하여 Webex과 통합됩니다. Webex에서 OAuth 애플리케이션을 만들려면 다음 단계를 사용하십시오.

1. Webex 개발자 안내서의 통합 및 권한 부여 페이지에 있는 통합 등록 섹션의 지침을 따르십시오.
2. 다음 형식의 리디렉션 URL을 사용합니다.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

이 URL에서 *<region>*는 AppFabric 앱 번들을 구성한 AWS 리전 의 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 `us-east-1`입니다. 해당 리전의 리디렉션 URL은 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`입니다.

필수 범위

Webex OAuth 애플리케이션에 다음 범위를 추가해야 합니다.

- `spark-compliance:events_read`
- `audit:events_read`
- `spark-admin:people_read`

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Webex 조직 ID입니다. Webex 조직 ID를 찾는 방법에 대한 자세한 내용은 Webex 도움말 센터 웹 사이트의 CiscoWebex컨트롤 허브에서 조직 ID 조회를 참조하십시오.

테넌트 이름

이 고유 Webex 인스턴스를 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 Webex 클라이언트 ID를 요청합니다. Webex 클라이언트 ID를 찾으려면 다음 단계를 사용하십시오.

1. https://developer.webex.com에서 Webex 계정에 로그인합니다.
2. 오른쪽 상단에서 아바타를 선택합니다.
3. 내 Webex 앱을 선택합니다.

4. AppFabric에 사용하는 OAuth2 애플리케이션을 선택합니다.
5. 이 페이지의 클라이언트 ID를 AppFabric의 클라이언트 ID 필드에 입력합니다.

클라이언트 암호

AppFabric은 Webex 클라이언트 암호를 요청합니다. Webex은 OAuth 애플리케이션을 처음 만들 때 클라이언트 암호를 한 번만 표시합니다. 최초 클라이언트 암호를 저장하지 않은 경우 새 클라이언트 암호를 생성하려면 다음 단계를 사용하십시오.

1. https://developer.webex.com에서 Webex 계정에 로그인합니다.
2. 오른쪽 상단에서 아바타를 선택합니다.
3. 내 Webex 앱을 선택합니다.
4. AppFabric에 사용하는 OAuth2 애플리케이션을 선택합니다.
5. 이 페이지에서 새 클라이언트 암호를 생성하십시오.
6. AppFabric의 클라이언트 암호 필드에 새 클라이언트 암호를 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Webex에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 수락을 선택합니다.

AppFabricZendesk에 대한 구성

Zendesk은 2007년 전 세계 모든 기업이 온라인으로 고객 서비스를 이용할 수 있게 함으로써 고객 경험 혁명을 일으켰습니다. 오늘날, Zendesk은 전 세계 모든 사람에게 훌륭한 서비스를 제공하는 챔피언으로, 전화, 채팅, 이메일, 메시징, 소셜 채널, 커뮤니티, 리뷰 사이트, 헬프 센터를 통해 10만 개 이상의 브랜드와 수억 명의 고객을 연결하여 수십억 건의 대화를 주도하고 있습니다. Zendesk 제품은 사랑받고자 하는 사랑을 담아 만들어졌습니다. 덴마크 코펜하겐에서 창립된 이 회사는 캘리포니아에서 설립 및 성장하여 현재 전 세계에서 6,000명 이상의 직원을 고용하고 있습니다.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Zendesk, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Zendesk에 대한 AppFabric 지원
- AppFabric을 Zendesk 계정에 연결

Zendesk에 대한 AppFabric 지원

AppFabric은 Zendesk에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Zendesk로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Zendesk Suite Enterprise 또는 Enterprise Plus 계정 또는 Zendesk Support Enterprise 계정이 있어야 합니다. Zendesk Enterprise 계정을 만들거나 업그레이드하는 방법에 대한 자세한 내용은 Zendesk 웹 사이트에서 요금제 유형 Zendesk 확인하기를 참조하십시오.
- Zendesk 계정에 관리자 역할을 가진 사용자가 있어야 합니다. 역할에 대한 자세한 내용은 Zendesk 웹 사이트의 Zendesk 지원 사용자 역할 이해를 참조하십시오.

속도 제한 고려 사항

Zendesk는 Zendesk API에 속도 제한을 부과합니다. Zendesk API 속도 제한에 대한 자세한 내용은 Zendesk 웹 사이트의 Zendesk 개발자 안내서에서 속도 제한을 참조하십시오. AppFabric과 기존 Zendesk API 애플리케이션의 조합이 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 길면 30분까지 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다. 하지만 이는 계정 수준에서 사용자 지정할 수 있습니다. 도움이 필요하면 지원로 문의하십시오.

AppFabric을 Zendesk 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 AppFabric에 Zendesk을 사용하여 인증해야 합니다. Zendesk을 AppFabric으로 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

OAuth 애플리케이션 생성

AppFabric은 OAuth를 사용하여 Zendesk과 통합됩니다. Zendesk에서는 다음 설정을 사용하여 OAuth 애플리케이션을 생성해야 합니다.

1. Zendesk 지원 웹사이트의 애플리케이션에 OAuth 인증 사용하기 문서의 Zendesk에 애플리케이션 등록하기 섹션의 지침을 따르십시오.

2. 다음 형식의 리디렉션 URL을 사용합니다.

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

이 URL에서 *<region>*는 AppFabric 앱 번들을 구성한 AWS 리전 의 코드입니다. 미국 동부(버지니아 북부) 리전의 경우 이 코드는 us-east-1입니다. 해당 리전의 리디렉션 URL은 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2입니다.

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Zendesk 하위 도메인입니다. Zendesk 하위 도메인을 찾는 방법에 대한 자세한 내용은 Zendesk Support 웹 사이트에서 내 Zendesk 하위 도메인을 어디에서 찾을 수 있나요?를 참조하십시오.

테넌트 이름

이 고유한 Zendesk 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. AppFabric의 클라이언트 ID는 Zendesk API 고유 식별자입니다. Zendesk 고유 식별자를 찾으려면 다음 단계를 사용하십시오.

1. Zendesk 계정의 관리 센터로 이동합니다.
2. 앱 및 통합을 선택합니다.
3. API, Zendesk API를 선택합니다.
4. OAuth 클라이언트 탭을 선택합니다.
5. AppFabric용으로 만든 OAuth 애플리케이션을 선택합니다.
6. AppFabric의 클라이언트 ID 필드에 OAuth 클라이언트의 고유 식별자를 입력합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. AppFabric의 클라이언트 암호는 Zendesk 비밀 토큰입니다. Zendesk는 Zendesk OAuth 애플리케이션을 처음 만들 때 비밀 토큰을 한 번만 표시합니다. 초기 비밀 토큰을 저장하지 않은 경우 새 비밀 토큰을 생성하려면 다음 단계를 사용하십시오.

1. Zendesk 계정의 관리 센터로 이동합니다.
2. 앱 및 통합을 선택합니다.
3. API, Zendesk API를 선택합니다.
4. OAuth 클라이언트 탭을 선택합니다.
5. AppFabric용으로 만든 OAuth 애플리케이션을 선택합니다.
6. 비밀 토큰 필드 옆에 있는 재생성 버튼을 선택합니다.
7. AppFabric의 클라이언트 암호 필드에 새 암호 토큰을 입력합니다.

인증 승인

AppFabric에서 앱 인증을 생성한 후 Zendesk에서 인증을 승인하라는 팝업창이 뜹니다. AppFabric 인증을 승인하려면 허용을 선택합니다.

AppFabricZoom에 대한 구성

Zoom은 기업과 개인이 보다 쉽고 몰입감 있게 동적으로 연결할 수 있는 올인원 지능형 협업 플랫폼입니다. Zoom 기술은 사람을 중심에 두고 팀 채팅, 전화, 회의, 옴니채널 클라우드 컨택 센터, 스마트 레코딩, 화이트보드 등과 같은 솔루션을 하나의 제품으로 통합하여 의미 있는 연결을 가능하게 하고 현대적인 협업을 촉진하며 인간의 혁신을 주도합니다.

AWS AppFabric for security를 사용하여의 로그 및 사용자 데이터를 감사하고Zoom, 데이터를 OCSF(Open Cybersecurity Schema Framework) 형식으로 정규화하고, Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 스트림에 데이터를 출력할 수 있습니다.

주제

- Zoom에 대한 AppFabric 지원
- AppFabric을 Zoom 계정에 연결

Zoom에 대한 AppFabric 지원

AppFabric은 Zoom에서 사용자 정보 및 감사 로그 수신을 지원합니다.

사전 조건

AppFabric을 사용하여 Zoom로부터 지원되는 대상으로 감사 로그를 전송하려면 다음 요구 사항을 충족해야 합니다.

- Zoom Pro, Business, Education 또는 Enterprise 요금제가 있어야 합니다.

- Zoom 관리자 역할에는 서버 간 OAuth 애플리케이션을 만들 수 있는 권한이 있어야 합니다. 서버 간 OAuth 애플리케이션을 활성화하는 방법에 대한 자세한 내용은 Zoom 웹사이트의 Zoom 개발자 안내서에 있는 서버 간 OAuth 페이지의 권한 활성화 섹션을 참조하십시오.
- Zoom 관리자 역할에는 관리자 활동 로그를 보고 감사 활동을 로그인/로그아웃할 수 있는 권한이 있어야 합니다. 감사 활동을 볼 수 있는 권한을 설정하는 방법에 대한 자세한 내용은 Zoom 지원 웹 사이트의 역할 관리 사용 및 관리자 활동 로그 사용을 참조하십시오.

속도 제한 고려 사항

Zoom는 Zoom API에 속도 제한을 부과합니다. Zoom 속도 제한에 대한 자세한 내용은 Zoom 개발자 설명서의 속도 제한을 참조하십시오. AppFabric과 기존 Zoom 애플리케이션의 조합이 제한을 초과하는 경우 AppFabric에 표시되는 감사 로그가 지연될 수 있습니다.

데이터 지연 고려 사항

감사 이벤트가 목적지로 전달되기까지 약 24시간 정도 지연될 수 있습니다. 이는 애플리케이션에서 제공하는 감사 이벤트가 지연되고 데이터 손실을 줄이기 위한 예방 조치가 취해졌기 때문입니다.

AppFabric을 Zoom 계정에 연결

AppFabric 서비스 내에서 앱 번들을 생성한 후에는 Zoom을 사용하여 AppFabric을 인증해야 합니다. AppFabric으로 Zoom을 인증하는 데 필요한 정보를 찾으려면 다음 단계를 사용하십시오.

서버 간 OAuth 애플리케이션 만들기

AppFabric은 앱 보안 인증이 있는 서버 간 OAuth를 사용하여 Zoom와 통합합니다. Zoom에서 서버 간 OAuth 애플리케이션을 만들려면 Zoom 개발자 안내서의 서버 간 OAuth 앱 만들기의 지침을 따르십시오. AppFabric은 Zoom 웹후크를 지원하지 않으므로 웹후크 구독 추가 섹션을 건너뛰어도 됩니다.

필수 범위

Zoom는 세분화된 범위(새로 생성된 애플리케이션의 경우)와 클래식 범위(이전에 생성된 애플리케이션의 경우)라는 두 가지 유형의 범위를 제공합니다.

Zoom server-to-server OAuth 애플리케이션에 다음과 같은 세분화된 범위를 추가해야 합니다.

- `report:read:user_activities:admin`
- `report:read:operation_logs:admin`
- `user:read:email:admin`
- `user:read:user:admin`

이전에 생성한 애플리케이션을 사용하는 경우 다음과 같은 클래식 범위를 추가해야 합니다.

- `report:read:admin`
- `user:read:admin`

앱 인증

테넌트 ID

AppFabric은 테넌트 ID를 요청합니다. AppFabric의 테넌트 ID는 Zoom 계정 ID입니다. Zoom계정 ID를 찾으려면 다음 단계를 수행합니다.

1. Zoom Marketplace로 이동합니다.
2. 관리를 선택합니다.
3. AppFabric에 사용하는 서버 간 OAuth 애플리케이션을 선택합니다.
4. 앱 보안 인증 페이지의 계정 ID를 AppFabric의 테넌트 ID 필드에 입력합니다.

테넌트 이름

이 고유한 Zoom 조직을 식별하는 이름을 입력합니다. AppFabric은 테넌트 이름을 사용하여 앱 인증 및 해당 앱 인증을 통해 생성된 모든 수집에 레이블을 지정합니다.

클라이언트 ID

AppFabric은 클라이언트 ID를 요청합니다. Zoom 클라이언트 ID를 찾으려면 다음 단계를 사용하십시오.

1. Zoom Marketplace로 이동합니다.
2. 관리를 선택합니다.
3. AppFabric에 사용하는 서버 간 OAuth 애플리케이션을 선택합니다.
4. 앱 보안 인증 페이지의 클라이언트 ID를 AppFabric의 클라이언트 ID 필드에 입력합니다.

클라이언트 암호

AppFabric은 클라이언트 암호를 요청합니다. Zoom 클라이언트 암호를 찾으려면 다음 단계를 사용합니다.

1. Zoom Marketplace로 이동합니다.

2. 관리를 선택합니다.
3. AppFabric에 사용하는 서버 간 OAuth 애플리케이션을 선택합니다.
4. 앱 보안 인증 페이지의 클라이언트 암호를 AppFabric의 클라이언트 암호 필드에 입력합니다.

감사 로그 전달

Zoom는 24시간마다 API에 액세스하여 감사 로그를 사용할 수 있도록 합니다. AppFabric으로 감사 로그를 볼 때 표시되는 Zoom 데이터는 전날의 활동에 대한 데이터입니다.

AppFabric for security에서 호환되는 보안 도구 및 서비스

AWS AppFabric for security는 다음 보안 도구 및 서비스와의 통합을 지원합니다. AppFabric for security를 설정하여 연결하는 방법에 대한 자세한 내용을 보려면 서비스 이름을 선택합니다.

주제

- Barracuda XDR
- Dynatrace
- Logz.io
- Netskope
- NetWitness
- Amazon Quick
- Rapid7
- Amazon Security Lake
- Singularity Cloud
- Splunk

Barracuda XDR

Barracuda Networks는 신뢰할 수 있는 파트너이자 클라우드 우선 보안 솔루션 제공업체로서 비즈니스 여정에 따라 성장하고 적응하는 혁신적인 솔루션으로 이메일, 네트워크, 데이터 및 애플리케이션을 보호합니다. Barracuda XDR은 보안 운영 센터(SOC)의 보안 분석가 팀과 정교한 기술을 결합한 개방적이고 확장된 탐지 및 대응 솔루션입니다. 이 Barracuda XDR 플랫폼은 40개 이상의 통합 데이터 소스에서 매일 수십억 개의 원시 이벤트를 분석하고, MITRE ATT&CK® 프레임워크에 매핑되는 광범위한 위협 탐지 규칙과 함께 위협을 더 빠르게 탐지하고 대응 시간을 단축할 수 있습니다.

AWS AppFabric 감사 로그 수집 고려 사항

다음 섹션에서는 Barracuda XDR과 함께 사용할 AppFabric 출력 스키마, 출력 형식 및 출력 대상에 대해 설명합니다.

스키마 및 형식

Barracuda XDR는 다음과 같은 AppFabric 출력 스키마 및 형식을 지원합니다.

- OCSF - JSON: AppFabric은 개방형 사이버 보안 스키마 프레임워크(OCSF)를 사용하여 데이터를 정규화하고 JSON 형식으로 데이터를 출력합니다.

출력 위치

Barracuda XDR Amazon Security Lake의 감사 로그 수신을 지원합니다. AppFabric에서 Barracuda XDR로 데이터를 보내려면 아래 지침을 따릅니다.

1. Amazon Security Lake로 데이터 전송: Amazon Data Firehose를 통해 Amazon Security Lake로 데이터를 전송하도록 AppFabric을 구성합니다. 자세한 내용은 Amazon Security Lake 단원을 참조하십시오.
2. Barracuda XDR에 데이터 전송: Amazon Security Lake에서 감사 로그를 수신하도록 Barracuda XDR을 구성합니다. 자세한 내용은 Amazon Security Lake 설정 및 사용을 참조하세요.

Dynatrace

는 광범위하고 심층적인 관찰성과 지속적인 런타임 애플리케이션 보안을 고급 AIOps와 Dynatrace® Platform 결합하여 데이터에서 답변과 지능형 자동화를 제공합니다. 이를 통해 혁신가는 클라우드 운영을 현대화 및 자동화하고, 소프트웨어를 더 빠르고 안전하게 제공하고, 완벽한 디지털 경험을 보장할 수 있습니다.

AWS AppFabric 감사 로그 수집 고려 사항

다음 섹션에서는에 사용할 AppFabric 출력 스키마, 출력 형식 및 출력 대상에 대해 설명합니다 Dynatrace Platform.

스키마 및 형식

는 다음과 같은 AppFabric 출력 스키마 및 형식을 Dynatrace Platform 지원합니다.

- OCSF - JSON: AppFabric은 개방형 사이버 보안 스키마 프레임워크(OCSF)를 사용하여 데이터를 정규화하고 JSON 형식으로 데이터를 출력합니다.

출력 위치

는 다음 AppFabric 출력 위치에서 감사 로그 수신을 Dynatrace Platform 지원합니다.

- Amazon Simple Storage Service(Amazon S3)
  - 감사 로그가 포함된 Amazon S3 버킷에서 데이터를 수신Dynatrace Platform하도록를 구성하려면 의 Dynatrace S3 Log Forwarder 프로젝트의 지침을 따릅니다GitHub.

Logz.io

Logz.io은 클라우드 네이티브 기업이 Logz.io Open 360 Platform을 통해 환경을 모니터링하고 보호하도록 지원하여, 관찰 가능성과 보안을 고비용, 저가치 부담에서 벗어나 가치 있고 비용 효율적인 방식으로 전환하여 비즈니스 성과를 높일 수 있도록 지원합니다.

Logz.io Cloud SIEM은 데이터 과부하부터 광범위하게 존재하는 사이버 기술 격차에 이르기까지 오늘날의 주요 보안 과제를 신속한 쿼리, 다차원 감지 및 맞춤형 심층 보안 콘텐츠를 통해 직접 해결함으로써 데이터 볼륨에 관계없이 성능 저하 없이 클라우드 환경의 전체 확장을 모니터링하고 조사할 수 있도록 지원합니다.

이 Logz.io 솔루션은 복잡성과 비용을 줄이면서 고급 위협 분석 및 조사를 제공하도록 특별히 설계되었습니다. 고객은 전담 보안 분석가, 서비스로서의 위협 콘텐츠 및 AI 지원 기능을 통해 지원을 받게 되며, 이를 통해 잡음이 많은 데이터를 줄이고 팀이 실제 위협의 우선순위를 빠르게 결정할 수 있는 정보에 집중할 수 있습니다.

AWS AppFabric 감사 로그 수집 고려 사항

다음 섹션에서는 Logz.io과 함께 사용할 AppFabric 출력 스키마, 출력 형식 및 출력 대상에 대해 설명합니다.

스키마 및 형식

Logz.io는 다음과 같은 AppFabric 출력 스키마 및 형식을 지원합니다.

- 원시 - JSON
  - AppFabric은 소스 애플리케이션에서 사용하는 원본 스키마의 데이터를 JSON 형식으로 출력합니다.

- OCSF - JSON
  - AppFabric은 OCSF(Open Cyber Security Schema Framework)를 사용하여 데이터를 정규화하고 JSON 형식으로 데이터를 출력합니다.

출력 위치

Logz.io는 다음과 같은 AppFabric 출력 위치를 지원합니다.

- Amazon Data Firehose
  - Firehose 전송 스트림이 로 데이터를 전송하도록 구성하려면 Amazon Data Firehose 개발자 안내서의 대상 Logz.io 선택의 지침을 Logz.io따르세요.
- Amazon Simple Storage Service(Amazon S3)
  - 감사 로그가 포함된 Amazon S3 버킷에서 데이터를 수신하도록 Logz.io로 구성하려면 Logz.io 웹 사이트의 Amazon S3 버킷 구성의 지침을 따르십시오.

Netskope

글로벌 사이버 보안 리더인 Netskope는 조직이 제로 트러스트 원칙을 적용하여 데이터를 보호할 수 있도록 클라우드, 데이터 및 네트워크 보안을 재정의하고 있습니다. 빠르고 사용하기 쉬운 이 Netskope 플랫폼은 사용자, 기기 및 데이터가 어디에 있든 최적화된 액세스와 제로 트러스트 보안을 제공합니다. Netskope은 고객이 클라우드, 웹 및 프라이빗 애플리케이션 활동에 대한 위험을 줄이고 성능을 가속화하며 타의 추종을 불허하는 가시성을 갖도록 지원합니다. Fortune 100대 기업 중 25개 이상을 포함한 수천 명의 고객이 진화하는 위협, 새로운 위험, 기술 변화, 조직 및 네트워크 변경, 새로운 규제 요구 사항을 해결하기 위해 Netskope 와 강력한 NewEdge 네트워크를 신뢰하고 있습니다. Netskope이 고객이 SASE 여정에서 무엇이든 준비할 수 있도록 지원하는 방법을 알아보려면 netskope.com을 방문하십시오.

AWS AppFabric 감사 로그 수집 고려 사항

다음 섹션에서는 Netskope과 함께 사용할 AppFabric 출력 스키마, 출력 형식 및 출력 대상에 대해 설명합니다.

스키마 및 형식

Netskope는 다음과 같은 AppFabric 출력 스키마 및 형식을 지원합니다.

- 원시 - JSON

  - AppFabric은 소스 애플리케이션에서 사용하는 원본 스키마의 데이터를 JSON 형식으로 출력합니다.
- OCSF - JSON
  - AppFabric은 OCSF(Open Cyber Security Schema Framework)를 사용하여 데이터를 정규화하고 JSON 형식으로 데이터를 출력합니다.

출력 위치

Netskope는 다음과 같은 AppFabric 출력 위치를 지원합니다.

- Amazon Simple Storage Service(Amazon S3)
  - 감사 로그가 포함된 Amazon S3 버킷에서 데이터를 수신하도록 Netskope을 구성하려면 Netskope 웹 사이트의 Amazon Web Services S3에 대한 데이터 보호의 지침을 따르십시오.

NetWitness

NetWitness은 확장 탐지 및 대응(XDR) 소프트웨어의 선도적인 개발업체입니다. 보안에 매우 민감한 글로벌 고객층은 NetWitness XDR을 사용하여 정교하고 공격적인 공격으로부터 방어합니다. 디지털 공격을 탐지, 조사 및 대응할 수 있는 업계에서 가장 완벽하고 통합된 성숙한 플랫폼을 갖춘 NetWitness XDR은 현대적이고 효과적인 SOC의 통합 기반입니다.

NetWitness XDR은 고도로 모듈화된 아키텍처 덕분에 클라우드, 온프레미스, 모바일 및 원격 작업자 등 어느 곳에서나 위협을 탐지합니다. NetWitnessPlatform XDR은 적용된 위협 인텔리전스 및 사용자 행동 분석과 결합된 완벽한 가시성을 제공하여 활동의 우선 순위를 지정하고, 조사하고, 대응을 자동화합니다. 이 모든 기능을 통해 보안 분석가는 더 우수하고 빠른 효율성을 확보하여 비즈니스에 영향을 미치는 위협에 한 발 앞서 보안 운영을 유지할 수 있습니다.

AWS AppFabric 감사 로그 수집 고려 사항

다음 섹션에서는 NetWitness과 함께 사용할 AppFabric 출력 스키마, 출력 형식 및 출력 대상에 대해 설명합니다.

스키마 및 형식

NetWitness는 다음과 같은 AppFabric 출력 스키마 및 형식을 지원합니다.

- 원시 - JSON

  - AppFabric은 소스 애플리케이션에서 사용하는 원본 스키마의 데이터를 JSON 형식으로 출력합니다.
- OCSF - JSON
  - AppFabric은 OCSF(Open Cyber Security Schema Framework)를 사용하여 데이터를 정규화하고 JSON 형식으로 데이터를 출력합니다.

출력 위치

NetWitness는 다음과 같은 AppFabric 출력 위치를 지원합니다.

- Amazon Simple Storage Service(Amazon S3)
  - 감사 로그가 포함된 Amazon S3 버킷에서 데이터를 수신하도록 NetWitness을 구성하려면 NetWitness 웹 사이트의 NetWitness 플랫폼 통합 페이지에 있는 S3 Universal Connector 이벤트 소스 로그 구성 가이드의 지침을 따르십시오.

Amazon Quick

Amazon Quick은 통합 비즈니스 인텔리전스(BI)를 하이퍼스케일로 사용하여 데이터 기반 조직을 지원합니다. Quick을 사용하면 모든 사용자가 최신 대화형 대시보드, 페이지가 매겨진 보고서, 임베디드 분석 및 자연어 쿼리를 통해 동일한 정보 소스에서 다양한 분석 요구 사항을 충족할 수 있습니다. AWS AppFabric for security 로그가 소스로 저장되는 Amazon Simple Storage Service(Amazon S3) 버킷을 선택하여 Quick에서 AppFabric 감사 로그 데이터를 분석할 수 있습니다.

AppFabric 감사 로그 수집 고려 사항

다음 섹션에서는 Quick과 함께 사용할 AppFabric 출력 스키마, 출력 형식 및 출력 대상에 대해 설명합니다.

스키마 및 형식

Quick은 다음 AppFabric 출력 스키마 및 형식을 지원합니다.

- 원시 - JSON
  - AppFabric은 소스 애플리케이션에서 사용하는 원본 스키마의 데이터를 JSON 형식으로 출력합니다.
- OCSF - JSON

- AppFabric은 OCSF(Open Cyber Security Schema Framework)를 사용하여 데이터를 정규화하고 JSON 형식으로 데이터를 출력합니다.

출력 위치

Quick은 다음 AppFabric 출력 위치를 지원합니다.

- Amazon S3
  - Amazon S3 파일을 사용하여 데이터 세트를 생성하여 Amazon S3에서 Quick으로 직접 데이터를 수집할 수 있습니다. 대상 파일 세트가 빠른 데이터 소스 할당량을 초과하지 않는지 확인하려면 빠른 사용 설명서의 데이터 소스 할당량을 참조하세요.
  - 파일 세트가 Amazon S3 데이터 소스의 빠른 할당량을 초과하는 경우 Amazon Athena 및 AWS Glue 테이블을 사용하여 Amazon S3에서 데이터를 수집할 수 있습니다. 빠른 데이터 세트에서 Athena를 사용하면 추가 비용이 발생합니다. Athena 요금에 대한 자세한 내용은 Athena 요금 페이지를 참조하십시오.

    Athena 사용 방법

    1. Athena 사용 설명서의 AWS Glue 를 사용하여 Amazon S3에 있는 데이터 소스에 연결하기의 지침을 따르십시오.
    2. 빠른 사용 설명서의 Athena 데이터를 사용하여 데이터 세트 생성의 지침을 따릅니다.

Rapid7

Rapid7, Inc.는 사이버 보안을 더 단순하고 접근하기 쉽게 만들어 더 안전한 디지털 세상을 만드는 것을 사명으로 삼고 있습니다. Rapid7는 동급 최고의 기술과 최첨단 연구 및 광범위하고 전략적인 전문 지식을 통해 보안 전문가들이 최신 공격 표면을 관리할 수 있도록 지원합니다. Rapid7의 포괄적인 보안 솔루션은 1만 명 이상의 글로벌 고객들이 클라우드 위험 관리 및 위협 탐지를 통합하여 공격 표면을 줄이고 빠르고 정확하게 위협을 제거할 수 있도록 지원합니다.

AWS AppFabric 감사 로그 수집 고려 사항

다음 섹션에서는 Rapid7와 함께 사용할 AppFabric 출력 스키마, 출력 형식 및 출력 대상에 대해 설명합니다.

스키마 및 형식

Rapid7는 다음과 같은 AppFabric 출력 스키마 및 형식을 지원합니다.

- 원시 - JSON
  - AppFabric은 소스 애플리케이션에서 사용하는 원본 스키마의 데이터를 JSON 형식으로 출력합니다.
- OCSF - JSON
  - AppFabric은 OCSF(Open Cyber Security Schema Framework)를 사용하여 데이터를 정규화하고 JSON 형식으로 데이터를 출력합니다.

출력 위치

Rapid7는 다음과 같은 AppFabric 출력 위치를 지원합니다.

- Amazon Simple Storage Service(Amazon S3)
  - 감사 로그가 포함된 Amazon S3 버킷에서 데이터를 수신하도록 Rapid7을 구성하려면 Rapid7 블로그 웹사이트의 InsightIDR을 사용하여 Amazon S3 활동을 모니터링하는 방법 블로그 게시물의 지침을 따르십시오.

Amazon Security Lake

Amazon Security Lake는 AWS 환경, 서비스형 소프트웨어(SaaS) 공급자, 온프레미스 및 클라우드 소스의 보안 데이터를에 저장된 전용 데이터 레이크로 자동으로 중앙 집중화합니다 AWS 계정. Security Lake를 사용하면 조직 전체의 보안 데이터를 더 완벽하게 이해할 수 있습니다. Security Lake는 오픈 소스 보안 이벤트 스키마인 개방형 사이버 보안 스키마 프레임워크(OCSF)를 채택했습니다. OCSF 지원을 통해 서비스는 AWS 및 광범위한 엔터프라이즈 보안 데이터 소스의 보안 데이터를 정규화하고 결합합니다.

AppFabric 감사 로그 수집 고려 사항

Security Lake에 사용자 지정 소스를 추가하여의 Amazon Security Lake AWS 계정 에 SaaS 감사 로그를 가져올 수 있습니다. 다음 섹션에서는 Security Lake와 함께 사용할 AppFabric 출력 스키마, 출력 형식 및 출력 대상에 대해 설명합니다.

스키마 및 형식

Security Lake는 다음과 같은 AppFabric 출력 스키마 및 형식을 지원합니다.

- OCSF - JSON
  - AppFabric은 개방형 사이버 보안 스키마 프레임워크(OCSF)를 사용하여 데이터를 정규화하고 JSON 형식으로 데이터를 출력합니다.

출력 위치

Security Lake는 Amazon Data Firehose 전송 스트림을 AppFabric 수집 출력 위치로 사용하여 AppFabric을 사용자 지정 소스로 지원합니다. AWS Glue 테이블 및 Firehose 전송 스트림을 구성하고 Security Lake에서 사용자 지정 소스를 설정하려면 다음 절차를 사용합니다.

AWS Glue 테이블 생성

1. Amazon Simple Storage Service(S3)로 이동하여 선택한 이름으로 버킷을 생성합니다.
2. AWS Glue 콘솔로 이동합니다.
3. 데이터 카탈로그의 경우 테이블 섹션으로 이동하여 테이블 추가를 선택합니다.
4. 이 테이블에 대해 선택한 이름을 입력합니다.
5. 1단계에서 생성한 Amazon S3 버킷을 선택합니다.
6. 데이터 형식으로 JSON을 선택하고 다음을 선택합니다.
7. 스키마 선택 또는 정의 페이지에서 스키마를 JSON으로 편집을 선택합니다.
8. 다음 스키마를 입력하고 AWS Glue 테이블 생성 프로세스를 완료합니다.

```
[
    {
        "Name": "message",
        "Type": "string"
    },
    {
        "Name": "process",
        "Type":
 "struct<name:string,pid:int,user:struct<name:string,type:string,domain:string,uid:string,t
    },
    {
        "Name": "status",
        "Type": "string"
    },
    {
        "Name": "time",
        "Type": "bigint"
    },
    {
        "Name": "device",
        "Type":
 "struct<name:string,owner:struct<name:string,type:string,uid:string,type_id:int,risk_level
    },
```

```
    {
        "Name": "metadata",
        "Type":
"struct<version:string,product:struct<name:string,version:string,uid:string,data_classific
    },
    {
        "Name": "severity",
        "Type": "string"
    },
    {
        "Name": "duration",
        "Type": "int"
    },
    {
        "Name": "type_name",
        "Type": "string"
    },
    {
        "Name": "activity_id",
        "Type": "int"
    },
    {
        "Name": "type_uid",
        "Type": "int"
    },
    {
        "Name": "observables",
        "Type": "array<struct<name:string,type:string,type_id:int,value:string>>"
    },
    {
        "Name": "category_name",
        "Type": "string"
    },
    {
        "Name": "class_uid",
        "Type": "int"
    },
    {
        "Name": "category_uid",
        "Type": "int"
    },
    {
        "Name": "class_name",
        "Type": "string"
```

```
    },
    {
        "Name": "timezone_offset",
        "Type": "int"
    },
    {
        "Name": "end_time",
        "Type": "bigint"
    },
    {
        "Name": "activity_name",
        "Type": "string"
    },
    {
        "Name": "cloud",
        "Type":
"struct<account:struct<name:string,type:string,uid:string,type_id:int>,project_uid:string,
    },
    {
        "Name": "query_info",
        "Type": "struct<name:string,uid:string,query_string:string>"
    },
    {
        "Name": "query_result",
        "Type": "string"
    },
    {
        "Name": "query_result_id",
        "Type": "int"
    },
    {
        "Name": "severity_id",
        "Type": "int"
    },
    {
        "Name": "status_code",
        "Type": "string"
    },
    {
        "Name": "status_detail",
        "Type": "string"
    },
    {
        "Name": "status_id",
```

```
        "Type": "int"
    },
    {
        "Name": "network_interfaces",
        "Type":
"array<struct<name:string,type:string,hostname:string,mac:string,type_id:int,ip:string>>"
    },
    {
        "Name": "file",
        "Type":
"struct<attributes:int,name:string,type:string,path:string,type_id:int,accessor:struct<nam
    },
    {
        "Name": "actor",
        "Type":
"struct<process:struct<pid:int,file:struct<name:string,size:bigint,type:string,version:str
    },
    {
        "Name": "dst_endpoint",
        "Type":
"struct<owner:struct<name:string,type:string,uid:string,type_id:int,full_name:string,risk_
    },
    {
        "Name": "src_endpoint",
        "Type":
"struct<name:string,owner:struct<name:string,type:string,domain:string,uid:string,org:stru
    },
    {
        "Name": "user",
        "Type":
"struct<name:string,type:string,groups:array<struct<name:string,uid:string>>,type_id:int>"
    },
    {
        "Name": "resource",
        "Type":
"struct<version:string,uid:string,agent_list:array<struct<name:string,type:string,uid:stri
    },
    {
        "Name": "privileges",
        "Type": "array<string>"
    },
    {
        "Name": "action",
        "Type": "string"
```

```
    },
    {
        "Name": "action_id",
        "Type": "int"
    },
    {
        "Name": "protocol_ver",
        "Type": "string"
    },
    {
        "Name": "proxy",
        "Type":
"struct<name:string,port:int,type:string,ip:string,hostname:string,uid:string,type_id:int,
    },
    {
        "Name": "client_hassh",
        "Type":
"struct<algorithm:string,fingerprint:struct<value:string,algorithm:string,algorithm_id:int
    },
    {
        "Name": "authorizations",
        "Type": "array<string>"
    },
    {
        "Name": "proxy_tls",
        "Type":
"struct<version:string,certificate:struct<version:string,uid:string,subject:string,issuer:
    },
    {
        "Name": "load_balancer",
        "Type":
"struct<name:string,classification:string,dst_endpoint:struct<owner:struct<type:string,dom
    },
    {
        "Name": "disposition_id",
        "Type": "int"
    },
    {
        "Name": "disposition",
        "Type": "string"
    },
    {
        "Name": "proxy_traffic",
        "Type": "struct<bytes:bigint,packets:int>"
```

```
    },
    {
        "Name": "auth_type_id",
        "Type": "int"
    },
    {
        "Name": "proxy_http_response",
        "Type": "struct<code:int,message:string,status:string,length:int>"
    },
    {
        "Name": "server_hassh",
        "Type":
"struct<algorithm:string,fingerprint:struct<value:string,algorithm:string,algorithm_id:int
    },
    {
        "Name": "auth_type",
        "Type": "string"
    },
    {
        "Name": "firewall_rule",
        "Type": "struct<version:string,uid:string>"
    },
    {
        "Name": "proxy_connection_info",
        "Type":
"struct<direction:string,direction_id:int,protocol_num:int,protocol_ver:string>"
    },
    {
        "Name": "connection_info",
        "Type": "struct<direction:string,direction_id:int>"
    },
    {
        "Name": "api",
        "Type":
"struct<request:struct<data:string,uid:string>,response:struct<error:string,code:int,messa
    },
    {
        "Name": "attacks",
        "Type":
"array<struct<version:string,tactics:array<struct<name:string,uid:string>>,technique:struc
    },
    {
        "Name": "raw_data",
        "Type": "string"
```

```
    },
    {
        "Name": "email_uid",
        "Type": "string"
    },
    {
        "Name": "malware",
        "Type":
"array<struct<name:string,path:string,uid:string,classification_ids:array<int>,cves:array<
    },
    {
        "Name": "start_time_dt",
        "Type": "string"
    },
    {
        "Name": "direction",
        "Type": "string"
    },
    {
        "Name": "smtp_hello",
        "Type": "string"
    },
    {
        "Name": "unmapped",
        "Type": "string"
    },
    {
        "Name": "direction_id",
        "Type": "int"
    },
    {
        "Name": "email_auth",
        "Type":
"struct<spf:string,dkim:string,dkim_domain:string,dkim_signature:string,dmarc:string,dmarc
    },
    {
        "Name": "email",
        "Type":
"struct<uid:string,from:string,to:array<string>,data_classification:struct<category:string
    },
    {
        "Name": "impact_id",
        "Type": "int"
    },
```

```
    {
        "Name": "resources",
        "Type":
"array<struct<owner:struct<name:string,type:string,uid:string,type_id:int,full_name:string
    },
    {
        "Name": "finding_info",
        "Type":
"struct<title:string,uid:string,attacks:array<struct<version:string,tactics:array<struct<n
    },
    {
        "Name": "evidences",
        "Type":
"array<struct<process:struct<name:string,pid:int,file:struct<name:string,type:string,versi
    },
    {
        "Name": "impact",
        "Type": "string"
    },
    {
        "Name": "count",
        "Type": "int"
    },
    {
        "Name": "confidence_id",
        "Type": "int"
    },
    {
        "Name": "enrichments",
        "Type":
"array<struct<data:string,name:string,type:string,value:string,provider:string>>"
    },
    {
        "Name": "rcode",
        "Type": "string"
    },
    {
        "Name": "app_name",
        "Type": "string"
    },
    {
        "Name": "rcode_id",
        "Type": "int"
    },
```

```
    {
        "Name": "query",
        "Type":
"struct<type:string,hostname:string,class:string,opcode_id:int,packet_uid:int>"
    },
    {
        "Name": "proxy_endpoint",
        "Type":
"struct<name:string,owner:struct<name:string,type:string,domain:string,uid:string,groups:a
    },
    {
        "Name": "response_time",
        "Type": "bigint"
    },
    {
        "Name": "delay",
        "Type": "int"
    },
    {
        "Name": "start_time",
        "Type": "bigint"
    },
    {
        "Name": "proxy_http_request",
        "Type":
"struct<version:string,url:struct<port:int,scheme:string,path:string,hostname:string,query
    },
    {
        "Name": "version",
        "Type": "string"
    },
    {
        "Name": "stratum",
        "Type": "string"
    },
    {
        "Name": "stratum_id",
        "Type": "int"
    },
    {
        "Name": "dispersion",
        "Type": "int"
    },
    {
```

```
        "Name": "traffic",
        "Type":
"struct<bytes_out:int,chunks:bigint,bytes:int,packets:int,packets_in:bigint>"
    },
    {
        "Name": "precision",
        "Type": "int"
    },
    {
        "Name": "size",
        "Type": "int"
    },
    {
        "Name": "actual_permissions",
        "Type": "int"
    },
    {
        "Name": "base_address",
        "Type": "string"
    },
    {
        "Name": "requested_permissions",
        "Type": "int"
    },
    {
        "Name": "end_time_dt",
        "Type": "string"
    },
    {
        "Name": "compliance",
        "Type":
"struct<control:string,status:string,standards:array<string>,status_id:int>"
    },
    {
        "Name": "remediation",
        "Type": "struct<desc:string>"
    },
    {
        "Name": "kb_article_list",
        "Type":
"array<struct<os:struct<name:string,type:string,type_id:int,cpe_name:string,edition:string
    },
    {
        "Name": "peripheral_device",
```

```
        "Type":
"struct<name:string,class:string,uid:string,model:string,serial_number:string,vendor_name:
    },
    {
        "Name": "time_dt",
        "Type": "string"
    },
    {
        "Name": "group",
        "Type": "struct<name:string,type:string,uid:string>"
    },
    {
        "Name": "users",
        "Type":
"array<struct<name:string,type:string,uid:string,type_id:int,risk_level:string,risk_level_
    },
    {
        "Name": "confidence_score",
        "Type": "int"
    },
    {
        "Name": "state",
        "Type": "string"
    },
    {
        "Name": "state_id",
        "Type": "int"
    },
    {
        "Name": "evidence",
        "Type": "string"
    },
    {
        "Name": "confidence",
        "Type": "string"
    },
    {
        "Name": "risk_level",
        "Type": "string"
    },
    {
        "Name": "risk_score",
        "Type": "int"
    },
```

```
    {
        "Name": "impact_score",
        "Type": "int"
    },
    {
        "Name": "risk_level_id",
        "Type": "int"
    },
    {
        "Name": "finding",
        "Type":
"struct<title:string,uid:string,modified_time:bigint,modified_time_dt:string,first_seen_ti
    },
    {
        "Name": "user_result",
        "Type":
"struct<name:string,type:string,uid:string,type_id:int,account:struct<name:string,uid:stri
    },
    {
        "Name": "codes",
        "Type": "array<int>"
    },
    {
        "Name": "command",
        "Type": "string"
    },
    {
        "Name": "type",
        "Type": "string"
    },
    {
        "Name": "kernel",
        "Type": "struct<name:string,type:string,type_id:int>"
    },
    {
        "Name": "http_response",
        "Type":
"struct<code:int,status:string,http_headers:array<struct<name:string,value:string>>>"
    },
    {
        "Name": "http_request",
        "Type":
"struct<url:struct<scheme:string,path:string,hostname:string,query_string:string,category_
    },
```

```
    {
        "Name": "tls",
        "Type":
"struct<version:string,certificate:struct<subject:string,issuer:string,fingerprints:array<
    },
    {
        "Name": "web_resources",
        "Type":
"array<struct<name:string,type:string,data_classification:struct<category:string,category_
    },
    {
        "Name": "http_cookies",
        "Type":
"array<struct<name:string,value:string,is_http_only:boolean,is_secure:boolean,samesite:str
    },
    {
        "Name": "type_id",
        "Type": "int"
    },
    {
        "Name": "databucket",
        "Type":
"struct<name:string,type:string,file:struct<attributes:int,name:string,owner:struct<name:s
    },
    {
        "Name": "table",
        "Type": "struct<uid:string,created_time_dt:string>"
    },
    {
        "Name": "session",
        "Type":
"struct<count:int,uid:string,uuid:string,issuer:string,created_time:bigint,is_remote:boole
    },
    {
        "Name": "certificate",
        "Type":
"struct<version:string,uid:string,subject:string,issuer:string,fingerprints:array<struct<v
    },
    {
        "Name": "is_mfa",
        "Type": "boolean"
    },
    {
        "Name": "logon_type_id",
```

```
        "Type": "int"
    },
    {
        "Name": "auth_protocol_id",
        "Type": "int"
    },
    {
        "Name": "logon_type",
        "Type": "string"
    },
    {
        "Name": "is_remote",
        "Type": "boolean"
    },
    {
        "Name": "is_cleartext",
        "Type": "boolean"
    },
    {
        "Name": "auth_protocol",
        "Type": "string"
    },
    {
        "Name": "is_renewal",
        "Type": "boolean"
    },
    {
        "Name": "lease_dur",
        "Type": "int"
    },
    {
        "Name": "relay",
        "Type":
"struct<name:string,type:string,ip:string,mac:string,namespace:string,type_id:int>"
    },
    {
        "Name": "transaction_uid",
        "Type": "string"
    },
    {
        "Name": "file_result",
        "Type":
"struct<name:string,size:int,type:string,path:string,desc:string,product:struct<name:strin
    },
```

```
    {
        "Name": "file_diff",
        "Type": "string"
    },
    {
        "Name": "create_mask",
        "Type": "string"
    },
    {
        "Name": "web_resources_result",
        "Type":
"array<struct<type:string,data_classification:struct<category:string,category_id:int,confi
    },
    {
        "Name": "app",
        "Type":
"struct<name:string,version:string,uid:string,data_classification:struct<category:string,c
    },
    {
        "Name": "src_url",
        "Type": "string"
    },
    {
        "Name": "priority_id",
        "Type": "int"
    },
    {
        "Name": "verdict",
        "Type": "string"
    },
    {
        "Name": "desc",
        "Type": "string"
    },
    {
        "Name": "verdict_id",
        "Type": "int"
    },
    {
        "Name": "priority",
        "Type": "string"
    },
    {
        "Name": "finding_info_list",
```

```
        "Type":
"array<struct<title:string,uid:string,attacks:array<struct<version:string,tactics:array<st
    },
    {
        "Name": "expiration_time_dt",
        "Type": "string"
    },
    {
        "Name": "expiration_time",
        "Type": "bigint"
    },
    {
        "Name": "comment",
        "Type": "string"
    },
    {
        "Name": "entity",
        "Type": "struct<data:string,name:string,version:string,uid:string>"
    },
    {
        "Name": "entity_result",
        "Type":
"struct<data:string,name:string,type:string,version:string,uid:string>"
    },
    {
        "Name": "module",
        "Type":
"struct<type:string,file:struct<name:string,type:string,path:string,desc:string,type_id:in
    },
    {
        "Name": "exit_code",
        "Type": "int"
    },
    {
        "Name": "injection_type",
        "Type": "string"
    },
    {
        "Name": "injection_type_id",
        "Type": "int"
    },
    {
        "Name": "request",
        "Type": "struct<uid:string>"
```

```
    },
    {
        "Name": "response",
        "Type": "struct<error:string,code:int,message:string,error_message:string>"
    },
    {
        "Name": "driver",
        "Type":
"struct<file:struct<name:string,type:string,version:string,path:string,type_id:int,parent_
    },
    {
        "Name": "prev_security_states",
        "Type": "array<string>"
    },
    {
        "Name": "security_states",
        "Type": "array<string>"
    },
    {
        "Name": "folder",
        "Type":
"struct<name:string,type:string,path:string,desc:string,type_id:int,mime_type:string,paren
    },
    {
        "Name": "url",
        "Type":
"struct<port:int,scheme:string,path:string,hostname:string,query_string:string,resource_ty
    },
    {
        "Name": "tunnel_type_id",
        "Type": "int"
    },
    {
        "Name": "tunnel_type",
        "Type": "string"
    },
    {
        "Name": "protocol_name",
        "Type": "string"
    },
    {
        "Name": "job",
        "Type":
"struct<name:string,file:struct<name:string,type:string,path:string,signature:struct<certi
```

```
    },
    {
        "Name": "num_trusted_items",
        "Type": "int"
    },
    {
        "Name": "command_uid",
        "Type": "string"
    },
    {
        "Name": "num_registry_items",
        "Type": "int"
    },
    {
        "Name": "num_network_items",
        "Type": "int"
    },
    {
        "Name": "schedule_uid",
        "Type": "string"
    },
    {
        "Name": "num_resolutions",
        "Type": "int"
    },
    {
        "Name": "scan",
        "Type": "struct<name:string,type:string,type_id:int>"
    },
    {
        "Name": "num_detections",
        "Type": "int"
    },
    {
        "Name": "num_processes",
        "Type": "int"
    },
    {
        "Name": "num_files",
        "Type": "int"
    },
    {
        "Name": "total",
        "Type": "int"
```

```
    },
    {
        "Name": "num_folders",
        "Type": "int"
    },
    {
        "Name": "dce_rpc",
        "Type":
"struct<command:string,flags:array<string>,command_response:string,opnum:int,rpc_interface
    },
    {
        "Name": "share",
        "Type": "string"
    },
    {
        "Name": "client_dialects",
        "Type": "array<string>"
    },
    {
        "Name": "open_type",
        "Type": "string"
    },
    {
        "Name": "tree_uid",
        "Type": "string"
    },
    {
        "Name": "share_type_id",
        "Type": "int"
    },
    {
        "Name": "share_type",
        "Type": "string"
    },
    {
        "Name": "dialect",
        "Type": "string"
    },
    {
        "Name": "cis_benchmark_result",
        "Type": "struct<name:string>"
    },
    {
        "Name": "vulnerabilities",
```

```
        "Type":
 "array<struct<references:array<string>,severity:string,affected_packages:array<struct<name
    },
    {
        "Name": "service",
        "Type": "struct<name:string,uid:string>"
    },
    {
        "Name": "data_security",
        "Type":
 "struct<category:string,pattern_match:string,category_id:int,confidentiality:string,confid
    },
    {
        "Name": "database",
        "Type":
 "struct<name:string,type:string,uid:string,type_id:int,data_classification:struct<category
    }
]
```

Security Lake에서 사용자 지정 소스를 생성합니다.

1. Amazon Security Lake 콘솔로 이동합니다.
2. 탐색 창에서 사용자 지정 소스를 선택합니다.
3. 사용자 지정 소스 생성을 선택하십시오.
4. 사용자 지정 소스의 이름을 입력하고 해당하는 OCSF 이벤트 클래스를 선택합니다.

> **Note**
>
> AppFabric은 계정 변경, 인증, 사용자 액세스 관리, 그룹 관리, 웹 리소스 활동, 웹 리소스 액세스 활동 이벤트 클래스를 사용합니다.

5. AWS 계정 ID와 외부 ID 모두에 AWS 계정 ID를 입력합니다. 그다음에 생성을 선택합니다.
6. 사용자 지정 소스의 Amazon S3 위치를 저장합니다. 이를 사용하여 Amazon Data Firehose 전송 스트림을 설정합니다.

Firehose에서 전송 스트림 생성

1. Amazon Data Firehose 콘솔로 이동합니다.

2. 전송 스트림 생성을 선택합니다.
3. 소스에서 직접 PUT을 선택합니다.
4. 대상에 S3을 선택합니다.
5. 레코드 변환 및 전환 섹션에서 레코드 형식 변환 활성화를 선택하고 Apache Parquet을 출력 형식으로 선택합니다.
6. AWS Glue 테이블에서 이전 절차에서 생성한 AWS Glue 테이블을 선택하고 최신 버전을 선택합니다.
7. 대상 설정에서는 Security Lake 사용자 지정 소스로 생성한 Amazon S3 버킷을 선택합니다.
8. 동적 파티셔닝의 경우 활성화를 선택합니다.
9. JSON용 인라인 파싱의 경우 활성화를 선택합니다.
   - 키네임에 `eventDayValue`를 입력합니다.
   - JQ 표현식의 경우 `(.time/1000)|strftime("%Y%m%d")`를 입력합니다.
10. S3 버킷 접두사의 경우 다음 값을 입력합니다.

    ```
    ext/<custom source name>/region=<region>/accountId=<account_id>/eventDay=!
    {partitionKeyFromQuery:eventDayValue}/
    ```

    <custom source name>, *<region>* 및 *<account_id>*를 Security Lake 사용자 지정 소스 이름 AWS 리전 및 AWS 계정 ID로 바꿉니다.
11. S3 버킷 오류 출력 접두사에는 다음 값을 입력합니다.

    ```
    ext/AppFabric/error/
    ```

12. 재시도 기간은 300을 선택합니다.
13. 버퍼 크기로 128MiB를 선택합니다.
14. 버퍼 간격으로 60초를 선택합니다.
15. Firehose 전송 스트림의 생성 프로세스를 완료합니다.

AppFabric 수집 생성

Amazon Security Lake로 데이터를 전송하려면 AppFabric 콘솔에서 이전에 생성한 Firehose 전송 스트림을 출력 위치로 사용하는 수집을 생성해야 합니다. Firehose를 출력 위치로 사용하도록 AppFabric 수집을 구성하는 방법에 대한 자세한 내용은 출력 위치 생성을 참조하세요.

Singularity Cloud

Singularity Cloud 플랫폼은 모든 단계에서 모든 범주의 위협으로부터 기업을 보호합니다. 특허 받은 AI(인공 지능)는 알려진 서명 및 패턴의 보안을 제로데이 및 랜섬웨어와 같은 가장 정교한 공격으로 확장합니다.

AWS AppFabric 감사 로그 수집 고려 사항

다음 섹션에서는 Singularity Cloud과 함께 사용할 AppFabric 출력 스키마, 출력 형식 및 출력 대상에 대해 설명합니다.

스키마 및 형식

Singularity Cloud는 다음과 같은 AppFabric 출력 스키마 및 형식을 지원합니다.

OCSF - JSON: AppFabric은 개방형 사이버 보안 스키마 프레임워크(OCSF)를 사용하여 데이터를 정규화하고 JSON 형식으로 데이터를 출력합니다.

출력 위치

Singularity Cloud는 다음 AppFabric 출력 위치에서 감사 로그 수신을 지원합니다.

- Amazon Simple Storage Service(Amazon S3)
  - 감사 로그가 포함된 Amazon S3 버킷에서 데이터를 수신Singularity Cloud하도록를 구성하려면 Singularity Cloud’s 설명서의 지침을 따르세요.

Splunk

Splunk는 조직의 탄력성을 높이는 데 도움이 됩니다. 선도적인 조직에서는 Splunk의 통합 보안 및 관찰 플랫폼을 사용하여 디지털 시스템을 안전하고 안정적으로 유지합니다. 조직은 Splunk를 신뢰하여 보안, 인프라 및 애플리케이션 문제가 큰 문제가 되는 것을 방지하고, 디지털 중단으로 인한 충격을 흡수하며, 디지털 트랜스포메이션을 가속화합니다.

AWS AppFabric 감사 로그 수집 고려 사항

다음 섹션에서는 Splunk과 함께 사용할 AppFabric 출력 스키마, 출력 형식 및 출력 대상에 대해 설명합니다.

스키마 및 형식

Splunk는 다음 AppFabric 출력 스키마 및 형식을 지원합니다.

- 원시 - JSON
  - AppFabric은 소스 애플리케이션에서 사용하는 원본 스키마의 데이터를 JSON 형식으로 출력합니다.
- OCSF - JSON
  - AppFabric은 개방형 사이버 보안 스키마 프레임워크(OCSF)를 사용하여 데이터를 정규화하고 JSON 형식으로 데이터를 출력합니다.
- OCSF - Parquet
  - AppFabric은 개방형 사이버 보안 스키마 프레임워크(OCSF)를 사용하여 데이터를 정규화하고 데이터를 Apache Parquet 형식으로 출력합니다.

출력 위치

Splunk는 다음과 같은 AppFabric 출력 위치를 지원합니다.

- Amazon Data Firehose
  - 감사 로그가 포함된 Firehose 스트림에서 감사 로그를 수신Splunk하도록를 구성하려면 Splunk 웹 사이트의 Splunk Amazon Data Firehose용 추가 기능의 지침을 따릅니다.
- Amazon Simple Storage Service(Amazon S3)
  - 감사 로그가 포함된 Amazon S3 버킷에서 데이터를 수신하도록 Splunk를 구성하려면 Splunk 웹 사이트의 AWS용 Splunk 추가 기능에 대한 SQS 기반 S3 입력 구성 지침을 따르십시오.

Delete AWS AppFabric for 보안 리소스

AWS AppFabric for security를 계속 사용하지 않으려면 추가 요금이 발생하지 않도록 설정 중에 생성한 출력 위치 및 AppFabric for security 리소스의 데이터를 삭제해야 합니다. AppFabric 리소스를 정리하려면 각 서비스형 소프트웨어(SaaS) 애플리케이션에 대해 리소스를 생성한 역순으로 리소스를 삭제해야 합니다. 즉, 수집 대상 > 수집 > 앱 인증 > 앱 번들입니다.

최종 앱 인증을 삭제한 후 앱 번들을 삭제할 수 있습니다.

주제

- 수집 대상 삭제
- 수집 삭제
- 앱 인증 삭제
- 앱 번들 삭제

수집 대상 삭제

수집을 생성할 때 출력 위치를 선택하면 AppFabric for security가 사용자를 대신하여 수집 대상을 생성합니다. 수집 대상을 삭제하려면 다음 단계를 사용합니다.

1. https://console.aws.amazon.com/appfabric/에서 AppFabric 콘솔을 엽니다.
2. 시작하기 페이지에서 왼쪽의 메뉴를 펼칩니다.
3. 수집을 선택합니다.
4. 앱 인증을 선택합니다.
5. 삭제하려는 대상 옆에 있는 옵션 버튼을 선택하고 삭제를 선택합니다.
6. 대상 삭제 대화 상자에서 삭제를 선택하여 확인합니다.
7. 모든 대상에 대해 위 단계를 반복합니다.

수집 삭제

수집을 삭제하려면 다음 단계를 수행합니다.

1. 시작하기 페이지에서 왼쪽의 메뉴를 펼칩니다.
2. 수집을 선택합니다.
3. 앱 인증 옆에 있는 옵션 버튼을 선택합니다.
4. 작업 드롭다운 메뉴를 선택합니다.
5. 삭제를 선택합니다.
6. 수집 삭제 대화 상자에서 삭제를 선택하여 확인합니다.

앱 인증 삭제

앱 인증을 삭제하려면 다음 단계를 사용합니다.

1. 시작하기 페이지에서 왼쪽의 메뉴를 펼칩니다.
2. 앱 인증을 선택합니다.
3. 삭제할 앱 인증 옆에 있는 옵션 버튼을 선택합니다.
4. 작업 드롭다운 메뉴를 선택합니다.
5. 삭제를 선택합니다.
6. 수집 삭제 대화 상자에서 삭제를 선택하여 확인합니다.

앱 번들 삭제

앱 번들을 삭제하려면 다음 단계를 사용합니다.

1. 시작하기 페이지에서 왼쪽의 메뉴를 펼칩니다.
2. 앱 번들을 선택합니다.
3. 삭제 버튼을 선택합니다.
4. `delete`를 입력하여 확인한 후, 삭제를 선택합니다.

생산성을 위한 AWS AppFabric이란 무엇입니까?

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

> **Note**
>
> Amazon Bedrock: AWS implements 자동 침해 탐지로 구동됩니다. 생산성을 위한 AWS AppFabric은 Amazon Bedrock을 기반으로 구축되었으므로 사용자는 Amazon Bedrock에 구현된 제어를 상속하여 AI의 안전, 보안 및 책임 있는 사용을 강화합니다.

생산성을 위한AWS AppFabric(미리 보기)은 여러 애플리케이션의 컨텍스트로 인사이트와 작업을 생성하여 타사 애플리케이션의 최종 사용자 생산성을 재구상하는 데 도움이 됩니다. 앱 개발자는 다른 앱의 사용자 데이터에 액세스하는 것이 더 생산적인 앱 경험을 만드는 데 중요하다는 것을 알고 있지만 각 애플리케이션을 통합하여 구축하고 관리하기를 원하지 않습니다. 생산성을 위한 AppFabric을 사용하면 애플리케이션 개발자는 앱 간 데이터 인사이트와 작업을 생성하는 생성형 AI 기반 API에 액세스하여 신규 또는 기존 생성형 AI 어시스턴트를 통해 보다 풍부한 최종 사용자 경험을 제공할 수 있습니다. 생산성을 위한 AppFabric은 여러 애플리케이션의 데이터를 통합하므로 개발자가 지점 간 통합을 구축하거나 유지할 필요가 없습니다. 애플리케이션 개발자는 생산성을 위한 AppFabric을 애플리케이션 UI에 직접 내장하여 최종 사용자에게 일관된 경험을 제공하는 동시에 다른 애플리케이션의 관련 컨텍스트를 표시할 수 있습니다.

생산성을 위한 AppFabric은 Asana, Atlassian Jira Suite, Google Workspace, Microsoft 365, Miro, Slack, Smartsheet 등과 같이 일반적으로 사용하는 애플리케이션의 데이터를 연결합니다. 생산성을 위한 AppFabric은 앱 개발자가 사용자 채택, 만족도 및 충성도를 높이는 보다 개인화된 앱 경험을 구축할 수 있는 더 쉬운 방법을 제공합니다. 한편, 최종 사용자는 작업 흐름을 방해하지 않고 애플리케이션 전반에서 필요한 인사이트에 액세스할 수 있다는 이점을 누릴 수 있습니다.

주제

- 생산성을 위한 AppFabric APIs(미리 보기)
- AppFabric의 데이터 처리

이점

생산성을 위한 AppFabric을 사용하면 애플리케이션 개발자는 앱 간 데이터 인사이트와 작업을 생성하는 API에 액세스하여 신규 또는 기존 생성형 AI 어시스턴트를 통해 보다 풍부한 최종 사용자 경험을 제공할 수 있습니다.

- 앱 간 사용자 데이터의 단일 소스: 생산성을 위한 AppFabric은 여러 애플리케이션의 데이터를 통합하므로 개발자가 지점 간 통합을 구축하거나 유지할 필요가 없습니다. SaaS 앱 데이터는 서로 다른 데이터 유형을 모든 애플리케이션에서 이해할 수 있는 형식으로 자동 정규화하여 다른 애플리케이션에서 사용할 수 있도록 처리되므로 앱 개발자가 더 많은 데이터를 통합하여 최종 사용자의 생산성을 실제로 개선할 수 있습니다.
- 사용자 경험을 완전히 제어: 개발자는 생산성을 위한 AppFabric을 애플리케이션 UI에 직접 내장하여 사용자 경험을 완전히 제어하는 동시에 애플리케이션 전반의 컨텍스트를 통해 최종 사용자에게 개인화된 인사이트와 권장 작업을 제공합니다. 이를 통해 최종 사용자가 선호하는 SaaS 애플리케이션에서 생산성을 위한 AppFabric을 사용할 수 있고 작업을 완료하기 위해 선호하는 앱에서 액세스할 수 있습니다. 최종 사용자는 앱 간 전환에 소요되는 시간을 줄이고 작업 흐름을 유지할 수 있습니다.
- 출시 시간 단축: 앱 개발자는 단 한 번의 API 직접 호출로 모델을 미세 조정하거나, 사용자 지정 프롬프트를 작성하거나 여러 애플리케이션에 통합을 구축할 필요 없이 생성된 사용자 데이터에 대한 사용자 수준의 인사이트를 얻을 수 있습니다. AppFabric은 이러한 복잡성을 추상화하여 앱 개발자가 생성형 AI 기능을 더 빠르게 구축, 내장 또는 강화할 수 있도록 합니다. 이를 통해 앱 개발자는 가장 중요한 작업에 리소스를 집중할 수 있습니다.
- 사용자 신뢰 구축을 위한 아티팩트 참조: 결과의 일부로, 생산성을 위한 AppFabric은 인사이트를 생성하는 데 사용한 관련 아티팩트 또는 소스 파일을 표시하여 LLM 결과에 대한 최종 사용자 신뢰를 구축합니다.
- 간소화된 사용자 권한: 인사이트를 생성하는 데 사용한 사용자 아티팩트는 사용자가 액세스할 수 있는 것에 기반합니다. 생산성을 위한 AppFabric은 ISV의 권한 및 액세스 제어를 신뢰할 수 있는 소스로 사용합니다.

사용 사례

앱 개발자는 생산성을 위한 AppFabric을 사용하여 애플리케이션 내부의 생산성을 재구상할 수 있습니다. 생산성을 위한 AppFabric은 최종 사용자의 생산성 향상을 돕기 위해 다음 사용 사례에 초점을 맞춘 두 가지 API를 제공합니다.

- 하루의 우선순위 설정
  - 실행 가능한 인사이트 API는 이메일, 캘린더, 메시지, 작업 등을 포함한 애플리케이션 전반에서 시기적절한 인사이트를 표시하여 사용자가 하루를 가장 잘 관리할 수 있도록 도와줍니다. 또한 사용자는 선호하는 애플리케이션에서 이메일 작성, 회의 예약, 작업 항목 생성과 같은 앱 간 작업을 실행할 수 있습니다. 예를 들어 하룻밤 사이에 고객 에스컬레이션을 수행한 직원은 야간 대화의 요약을 볼 수 있을 뿐만 아니라 고객 계정 관리자와의 회의를 예약하기 위한 권장 작업도 확인할 수 있습니다. 작업에는 필수 필드(예: 작업 이름 및 소유자 또는 이메일 발신자/수신자)가 미리 채워져 있으며, 작업을 실행하기 전에 미리 채워진 콘텐츠를 편집할 수 있습니다.
- 예정된 회의 준비
  - 회의 준비 API는 사용자가 회의 목적을 요약하고 이메일, 메시지 등과 같은 관련 앱 간 아티팩트를 표시하여 회의를 가장 잘 준비할 수 있도록 도와줍니다. 이제 사용자는 빠르게 회의를 준비할 수 있고 콘텐츠를 찾기 위해 여러 앱을 오가며 시간을 낭비하지 않아도 됩니다.

생산성을 위한 AppFabric에 액세스

생산성을 위한 AppFabric은 현재 평가판으로 출시되었으며 미국 동부(버지니아 북부) AWS 리전에서 사용할 수 있습니다. 에 대한 자세한 내용은의 AppFabric 엔드포인트 및 할당량을 AWS 리전참조하세요AWS 일반 참조. AWS AppFabric

각 리전에서 다음 방법 중 하나를 사용하여 생산성을 위한 AppFabric에 액세스할 수 있습니다.

- 앱 개발자로서
  - 애플리케이션 개발자를 위한 생산성을 위한 AppFabric(미리 보기) 시작하기
- 최종 사용자로서
  - 최종 사용자를 위한 생산성을 위한 AppFabric(미리 보기) 시작하기

애플리케이션 개발자를 위한 생산성을 위한 AppFabric(미리 보기) 시작하기

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

이 섹션에서는 앱 개발자가 생산성을 위한 AWS AppFabric(미리 보기)을 애플리케이션에 통합하는 데 도움이 됩니다. 생산성을 위한 AWS AppFabric을 사용하면 여러 애플리케이션에서 이메일, 일정 이벤트, 작업, 메시지 등을 통해 AI 기반 인사이트와 작업을 생성하여 개발자가 사용자를 위해 더 풍부한 앱 경험을 구축할 수 있습니다. 지원되는 애플리케이션 목록은 AWS AppFabric 지원 애플리케이션을 참조하세요.

생산성을 위한 AppFabric은 앱 개발자에게 안전하고 통제된 환경에서 빌드하고 실험할 수 있는 액세스 권한을 제공합니다. 생산성을 위한 AppFabric을 처음 사용하기 시작하면 AppClient를 생성하고 테스트 사용자 한 명을 등록해야 합니다. 이 접근 방식은 애플리케이션과 AppFabric 간의 인증 및 통신 흐름을 이해하고 테스트하는 데 도움이 되도록 설계되었습니다. 단일 사용자를 대상으로 테스트한 후 추가 사용자(5단계. AppFabric을 요청하여 애플리케이션 확인 참조)에게 액세스를 확대하기 전에 AppFabric에 애플리케이션을 제출하여 확인을 받을 수 있습니다. AppFabric은 광범위하게 도입할 수 있도록 하기 전에 애플리케이션 정보를 확인하여 앱 개발자, 최종 사용자 및 데이터를 보호함으로써 책임감 있는 방식으로 사용자 도입을 확대할 수 있는 기반을 마련합니다.

주제

사전 조건

시작하기 전에를 생성해야 합니다 AWS 계정. 자세한 내용은 에 가입 AWS 계정 단원을 참조하십시오. 또한 아래 나열된 `"appfabric:CreateAppClient"` IAM 정책에 액세스할 수 있는 사용자를 최소

한 명 생성해야 합니다. 그러면 사용자가 AppFabric에 애플리케이션을 등록할 수 있습니다. 생산성을 위한 AppFabric 기능의 권한 부여에 대한 자세한 내용은 생산성을 위한 AppFabric IAM 정책 예제 섹션을 참조하세요.

생산성을 위한 AppFabric은 평가판 기간 동안 미국 동부(버지니아 북부)에서만 사용할 수 있습니다. 아래 단계를 시작하기 전에 이 리전에 있는지 확인합니다.

1단계. 생산성을 위한 AppFabric AppClient 생성

애플리케이션 내에서 AppFabric for prodectivity 인사이트를 표시하려면 먼저 AppFabric AppClient를 생성해야 합니다. AppClient는 기본적으로 생산성을 위한 AppFabric의 게이트웨이로, 애플리케이션과 AppFabric 간의 보안 통신을 지원하는 안전한 OAuth 애플리케이션 클라이언트 역할을 합니다. AppClient를 생성하면 AppClient ID가 제공됩니다. AppClient ID는 AppFabric이 애플리케이션 및 AWS 계정과 함께 작업하고 있음을 AppFabric이 인식하는 데 중요한 고유 식별자입니다.

생산성을 위한 AppFabric은 앱 개발자에게 안전하고 통제된 환경에서 빌드하고 실험할 수 있는 액세스 권한을 제공합니다. 생산성을 위한 AppFabric을 처음 사용하기 시작하면 AppClient를 생성하고 테스트 사용자 한 명을 등록해야 합니다. 이 접근 방식은 애플리케이션과 AppFabric 간의 인증 및 통신 흐름을 이해하고 테스트하는 데 도움이 되도록 설계되었습니다. 단일 사용자를 대상으로 테스트한 후 추가 사용자(5단계. AppFabric을 요청하여 애플리케이션 확인 참조)에게 액세스를 확대하기 전에 AppFabric에 애플리케이션을 제출하여 확인을 받을 수 있습니다. AppFabric은 광범위하게 도입할 수 있도록 하기 전에 애플리케이션 정보를 확인하여 앱 개발자, 최종 사용자 및 데이터를 보호함으로써 책임감 있는 방식으로 사용자 도입을 확대할 수 있는 기반을 마련합니다.

AppClient를 생성하려면 AWS AppFabric `CreateAppClient` API 작업을 사용합니다. 이후에 AppClient를 업데이트해야 하는 경우 `UpdateAppClient` API 작업을 사용하여 redirectUrls만 변경할 수 있습니다. appName 또는 설명과 같은 AppClient와 관련된 다른 파라미터를 변경해야 하는 경우 AppClient를 삭제하고 새 파라미터를 생성해야 합니다. 자세한 내용은 CreateAppClient 단원을 참조하십시오.

Python, Node.js, Java, C#, Go, Rust 등 여러 프로그래밍 언어를 사용하여 `CreateAppClient` API를 사용하여 AWS 서비스에 애플리케이션을 등록할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서명 요청 예를 참조하세요. 이 API 작업을 수행하려면 계정의 Signature Version 4 자격 증명을 사용해야 합니다. 서명 버전 4에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하세요.

요청 필드

- `appName` - AppFabric 사용자 포털의 동의 페이지에 사용자에게 표시될 애플리케이션의 이름입니다. 동의 페이지에서는 최종 사용자에게 애플리케이션 내에 AppFabric 인사이트를 표시할 수 있는

권한을 요청합니다. 동의 페이지에 대한 자세한 내용은 2단계. 앱에 인사이트가 표시되도록 동의 섹션을 참조하세요.

- `description` - 애플리케이션에 대한 설명입니다.
- `redirectUrls` - 인증 후 최종 사용자를 리디렉션할 URI입니다. redirectUrl을 최대 5개 추가할 수 있습니다. 예를 들어 `https://localhost:8080`입니다.
- `starterUserEmails` - 애플리케이션이 검증될 때까지 인사이트를 수신할 수 있는 액세스가 허용되는 사용자 이메일 주소입니다. 이메일 주소는 하나만 사용할 수 있습니다. 예: `anyuser@example.com`
- `customerManagedKeyIdentifier`(선택 사항) - 데이터를 암호화하는 데 사용할 고객 관리형 키(KMS에서 생성)의 ARN입니다. 지정하지 않으면 AWS AppFabric 관리형 키가 사용됩니다. AWS 소유 키 및 고객 관리형 키에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 키 및 AWS 키를 참조하세요.

응답 필드

- `appClientArn` - AppClient ID를 포함하는 Amazon 리소스 이름(ARN)입니다. 예를 들어 AppClient ID는 `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`입니다.
- `verificationStatus` - AppClient 확인 상태입니다.
  - `pending_verification` - AppFabric에서 AppClient 확인이 아직 진행 중입니다. AppClient가 확인되기 전까지는 한 명의 사용자(`starterUserEmails`에서 지정된 사용자)만 AppClient를 사용할 수 있습니다. 3단계. AppFabric 사용자 포털 URL을 애플리케이션에 추가에 소개된 AppFabric 사용자 포털에서 애플리케이션이 확인되지 않았음을 알리는 알림이 사용자에게 표시됩니다.
  - `verified` - AppFabric에서 확인 프로세스를 성공적으로 완료했으며 이제 AppClient가 완전히 확인되었습니다.
  - `rejected` - AppClient에 대한 확인 프로세스를 AppFabric에서 거부했습니다. 확인 프로세스를 다시 시작하고 성공적으로 완료하기 전까지는 추가 사용자가 AppClient를 사용할 수 없습니다.

```
curl --request POST \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/ \
```

```
  --data '{
    "appName": "Test App",
    "description": "This is a test app",
    "redirectUrls": ["https://localhost:8080"],
    "starterUserEmails": ["anyuser@example.com"],
    "customerManagedKeyIdentifier": "arn:aws:kms:<region>:<account>:key/<key>"
}'
```

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

```
{
    "appClientConfigSummary": {
        "appClientArn": "arn:aws:appfabric:<region>:<account>:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "verificationStatus": "pending_verification"
    }
}
```

2단계. 애플리케이션 인증 및 권한 부여

OAuth 2.0 권한 부여 흐름을 설정하여 애플리케이션이 AppFabric 인사이트를 안전하게 통합할 수 있도록 합니다. 먼저 애플리케이션 ID를 확인하는 인증 코드를 생성해야 합니다. 자세한 내용은 인증 단원을 참조하십시오. 그런 다음 이 인증 코드를 액세스 토큰으로 교환합니다. 액세스 토큰은 애플리케이션 내에서 AppFabric 인사이트를 가져오고 표시할 수 있는 권한을 애플리케이션에 권한을 부여합니다. 자세한 내용은 토큰 단원을 참조하십시오.

애플리케이션 인증에 대한 자세한 내용은 애플리케이션 승인 액세스 허용 섹션을 참조하세요.

1. 권한 부여 코드를 생성하려면 AWS AppFabric `oauth2/authorize` API 작업을 사용합니다.

   요청 필드

   - `app_client_id`(필수) - 1단계에서 생성한 AWS 계정 AppClient ID입니다. AppClient 생성 예를 들어 `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`입니다.
   - `redirect_uri`(필수) - 1단계에서 사용한 인증 후 최종 사용자를 리디렉션할 URI입니다. AppClient 생성 예를 들어 `https://localhost:8080`입니다.
   - `state`(필수) - 요청과 콜백 사이의 상태를 유지하기 위한 고유 값입니다. 예를 들어 `a8904edc-890c-1005-1996-29a757272a44`입니다.

```
GET https://productivity.appfabric.<region>.amazonaws.com/oauth2/authorize?
app_client_id=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\
redirect_uri=https://localhost:8080&state=a8904edc-890c-1005-1996-29a757272a44
```

2. 인증 후에는 쿼리 파라미터로 반환되는 인증 코드와 함께 지정된 URI로 리디렉션됩니다. 예를 들면 `code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`로 입니다.

```
https://localhost:8080/?code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-
sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-
oampc&state=a8904edc-890c-1005-1996-29a757272a44
```

3. AppFabric `oauth2/token` API 작업을 사용하여 이 인증 코드를 액세스 토큰으로 교환합니다.

   이 토큰은 API 요청에 사용되며 처음에는 AppClient가 확인될 때까지 `starterUserEmails`에 유효합니다. AppClient가 확인된 후 모든 사용자가 이 토큰을 사용할 수 있습니다. 이 API 작업을 수행하려면 계정의 Signature Version 4 자격 증명을 사용해야 합니다. 서명 버전 4에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하세요.

   요청 필드

   - `code`(필수) - 마지막 단계에서 인증한 후 받은 인증 코드입니다. 예를 들어 `mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`입니다.
   - `app_client_id`(필수) - 1단계에서 생성한 AWS 계정 AppClient ID입니다. AppClient 생성 예를 들어 `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`입니다.
   - `grant_type`(필수) - 값은 `authorization_code`와 같아야 합니다.
   - `redirect_uri`(필수) - 1단계에서 사용한 인증 후 사용자를 리디렉션할 URI입니다. AppClient 생성 인증 코드를 생성할 때 사용한 것과 동일한 리디렉션 URI여야 합니다. 예를 들어 `https://localhost:8080`입니다.

   응답 필드

   - `expires_in` - 토큰이 만료되기까지 남은 기간입니다. 기본 만료 시간은 12시간입니다.
   - `refresh_token` - 초기 요청과 토큰 요청에서 받은 새로 고침 토큰입니다.
   - `token` - 초기 요청과 토큰 요청에서 받은 토큰입니다.

- token_type - 값은 Bearer입니다.
- appfabric_user_id - AppFabric 사용자 ID입니다. authorization_code 권한 부여 유형을 사용하는 요청의 경우에만 반환됩니다.

```
curl --location \
"https://appfabric.<region>.amazonaws.com/oauth2/token" \
--header "Content-Type: application/json" \
--header "X-Amz-Content-Sha256: <sha256_payload>" \
--header "X-Amz-Security-Token: <security_token>" \
--header "X-Amz-Date: 20230922T172215Z" \
--header "Authorization: AWS4-HMAC-SHA256 ..." \
--data "{
    \"code\": \"mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-
gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc",
    \"app_client_id\": \"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\",
    \"grant_type\": \"authorization_code\",
    \"redirect_uri\": \"https://localhost:8080\"
}"
```

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

```
{
    "expires_in": 43200,
    "refresh_token": "apkaeibaerjr2example",
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "<userId>"
}
```

3단계. AppFabric 사용자 포털 URL을 애플리케이션에 추가

최종 사용자는 AppFabric이 인사이트를 생성하는 데 사용한 애플리케이션의 데이터에 액세스할 수 있도록 권한을 부여해야 합니다. AppFabric은 최종 사용자가 앱에 권한을 부여할 수 있는 전용 사용자 포털(팝업 화면)을 구축하여 앱 개발자가 이 프로세스를 소유해야 하는 복잡성을 없애줍니다. 생산성을 위한 AppFabric을 사용할 준비가 되면 사용자는 사용자 포털로 이동하여 인사이트 및 앱 간 작업을 생성하는 데 사용하는 애플리케이션을 연결하고 관리할 수 있습니다. 로그인하면 사용자는 애플리케이션을 생산성을 위한 AppFabric에 연결한 다음 애플리케이션으로 돌아가 인사이트와 작업을 탐색할 수 있습니다. 애플리케이션을 생산성을 위한 AppFabric과 통합하려면 애플리케이션에 특정 AppFabric

URL을 추가해야 합니다. 이 단계는 사용자가 애플리케이션에서 직접 AppFabric 사용자 포털에 액세스할 수 있도록 하는 데 매우 중요합니다.

1. 애플리케이션 설정으로 이동하여 리디렉션 URL을 추가하기 위한 섹션을 찾습니다.
2. 적절한 영역을 찾은 후 다음 AppFabric URL을 애플리케이션에 대한 리디렉션 URL로 추가합니다.

```
https://userportal.appfabric.<region>.amazonaws.com/eup_login
```

URL을 추가하면 애플리케이션이 사용자를 AppFabric 사용자 포털로 안내하도록 설정됩니다. 여기서 사용자는 생산성을 위한 AppFabric 인사이트를 생성하는 데 사용되는 애플리케이션에 로그인하고 연결하며 관리할 수 있습니다.

4단계. AppFabric을 사용하여 앱 간 인사이트 및 작업 표시

사용자가 애플리케이션을 연결한 후에는 앱 및 컨텍스트 전환을 줄임으로써 사용자의 인사이트를 가져와 생산성을 높일 수 있습니다. AppFabric은 사용자가 액세스 권한이 있는 것을 기반으로 사용자에게만 인사이트를 생성합니다. AppFabric은 AppFabric이 AWS 계정 소유한에 사용자 데이터를 저장합니다. AppFabric이 데이터를 사용하는 방법에 대한 자세한 내용은 AppFabric의 데이터 처리를 참조하세요.

다음과 같은 AI 기반 API를 사용하여 앱 내에서 사용자 수준의 인사이트와 작업을 생성하고 표시할 수 있습니다.

- `ListActionableInsights` - 자세한 내용은 아래의 실행 가능한 인사이트 섹션을 참조하세요.
- `ListMeetingInsights` - 자세한 내용은 이 설명서 후반부의 회의 준비 섹션을 참조하세요.

실행 가능한 인사이트(**`ListActionableInsights`**)

`ListActionableInsights` API는 사용자가 이메일, 캘린더, 메시지, 작업 등 애플리케이션 전반의 활동을 기반으로 실행 가능한 인사이트를 표시하여 하루를 가장 잘 관리할 수 있도록 도와줍니다. 반환된 인사이트에는 인사이트를 생성하는 데 사용한 아티팩트에 대한 링크도 포함되어 있어 사용자가 인사이트를 생성하는 데 사용한 데이터를 빠르게 확인할 수 있습니다. 또한 API는 인사이트를 기반으로 제안된 작업을 반환하고 사용자가 애플리케이션 내에서 앱 간 작업을 실행하도록 할 수 있습니다. 특히, API는 Asana, Google Workspace, Microsoft 365, Smartsheet와 같은 플랫폼과 통합하여 사용자가 이메일을 보내고 캘린더 이벤트를 만들며 작업을 생성할 수 있도록 합니다. 대형 언어 모델(LLM)은 권장 작업(예: 이메일 본문 또는 작업 이름)에 세부 정보를 미리 채울 수 있으며, 사용자는 실행 전에 이를 사용자 지정할 수 있으므로 의사 결정을 단순화하고 생산성을 높일 수 있습니다. 최종 사용자가 애플리

케이션에 권한을 부여하는 경험과 마찬가지로 AppFabric은 동일한 전용 포털을 사용하여 사용자가 앱 간 작업을 보고, 편집하고, 실행할 수 있습니다. 작업을 실행하기 위해 AppFabric은 ISV가 사용자를 작업 세부 정보를 보고 실행할 수 있는 AppFabric 사용자 포털로 리디렉션해야 합니다. AppFabric에서 생성한 모든 작업에는 고유 URL이 있습니다. 이 URL은 `ListActionableInsights` API 응답의 응답에서 사용할 수 있습니다.

다음은 지원하는 앱 간 작업과 앱의 요약입니다.

- 이메일(Google Workspace, Microsoft 365) 보내기
- 캘린더 이벤트(Google Workspace, Microsoft 365) 생성
- 작업(Asana, Smartsheet) 생성

요청 필드

- `nextToken`(선택 사항) - 다음 인사이트 세트를 가져오기 위한 페이지 매김 토큰입니다.
- `includeActionExecutionStatus` - 작업 실행 상태 목록을 허용하는 필터입니다. 작업은 전달된 상태 값을 기준으로 필터링됩니다. 가능한 값: `NOT_EXECUTED` | `EXECUTED`

요청 헤더

- 인증 헤더를 `Bearer Token` 값과 함께 전달해야 합니다.

응답 필드

- `insightId` - 생성된 인사이트의 고유 ID입니다.
- `insightContent` - 이렇게 하면 인사이트의 요약과 인사이트를 생성하는 데 사용된 아티팩트로 연결하는 포함된 링크가 반환됩니다. 참고: 이는 포함된 링크(<a>태그)가 포함된 HTML 콘텐츠입니다.
- `insightTitle` - 생성된 인사이트의 제목입니다.
- `createdAt` - 인사이트가 생성된 시점입니다.
- `actions` - 생성된 인사이트에 대한 권장 작업 목록입니다. 작업 객체:
  - `actionId` - 생성된 작업의 고유 ID입니다.
  - `actionIconUrl` - 작업을 실행하도록 제안한 앱의 아이콘 URL입니다.
  - `actionTitle` - 생성된 작업의 제목입니다.

  - `actionUrl` - 최종 사용자가 AppFabric의 사용자 포털에서 작업을 보고 실행할 수 있는 고유한 URL입니다. 참고: ISV 앱은 작업을 실행할 때 이 URL을 사용하여 사용자를 AppFabric 사용자 포털(팝업 화면)로 리디렉션합니다.
  - `actionExecutionStatus` - 작업 상태를 나타내는 열거형입니다. 가능한 값은 `EXECUTED | NOT_EXECUTED`입니다.
- `nextToken`(선택 사항) - 다음 인사이트 세트를 가져오기 위한 페이지 매김 토큰입니다. 이 필드는 선택 사항 필드이며, null을 반환하면 로드할 인사이트가 더 이상 없음을 의미합니다.

자세한 내용은 ActionableInsights 단원을 참조하십시오.

```
curl -v --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/actionableInsights" \
  --header "Authorization: Bearer <token>"
```

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

```
200 OK

{
    "insights": [
        {
            "insightId": "7tff3412-33b4-479a-8812-30EXAMPLE1111",
            "insightContent": "You received an email from James
            regarding providing feedback
            for upcoming performance reviews.",
            "insightTitle": "New feedback request",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "actions": [
                {
                    "actionId": "5b4f3412-33b4-479a-8812-3EXAMPLE2222",
                    "actionIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/
eup/123.svg",
                    "actionTitle": "Send feedback request email",
                    "actionUrl": "https://userportal.appfabric.us-east-1.amazonaws.com/
action/action_id_1"
                    "actionExecutionStatus": "NOT_EXECUTED"
                }
            ]
        },
```

```
        {
            "insightId": "2dff3412-33b4-479a-8812-30bEXAMPLE3333",
            "insightContent":"Steve sent you an email asking for details on project.
 Consider replying to the email.",
            "insightTitle": "New team launch discussion",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "actions": [
                {
                    "actionId": "74251e31-5962-49d2-9ca3-1EXAMPLE1111",
                    "actionIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/
eup/123.svg",
                    "actionTitle": "Reply to team launch email",
                    "actionUrl": "https://userportal.appfabric.us-east-1.amazonaws.com/
action/action_id_2"
                    "actionExecutionStatus": "NOT_EXECUTED"
                }
            ]
        }
    ],
    "nextToken": null
}
```

회의 준비(**ListMeetingInsights**)

ListMeetingInsights API는 회의 목적을 요약하고 이메일, 메시지 등과 같은 관련 앱 간 아티팩트를 표시하여 사용자가 예정된 회의를 가장 잘 준비할 수 있도록 도와줍니다. 이제 사용자는 빠르게 회의를 준비할 수 있고 콘텐츠를 찾기 위해 여러 앱을 오가며 시간을 낭비하지 않아도 됩니다.

요청 필드

- nextToken(선택 사항) - 다음 인사이트 세트를 가져오기 위한 페이지 매김 토큰입니다.

요청 헤더

- 인증 헤더를 Bearer Token 값과 함께 전달해야 합니다.

응답 필드

- insightId - 생성된 인사이트의 고유 ID입니다.
- insightContent - 세부 정보를 문자열 형식으로 강조 표시하는 인사이트에 대한 설명입니다. 즉, 이 인사이트가 왜 중요한지에 대한 것입니다.

- `insightTitle` - 생성된 인사이트의 제목입니다.
- `createdAt` - 인사이트가 생성된 시점입니다.
- `calendarEvent` - 사용자가 집중해야 하는 중요한 캘린더 이벤트 또는 회의입니다. 캘린더 이벤트 객체:
  - `startTime` - 이벤트의 시작 시간입니다.
  - `endTime` - 이벤트의 종료 시간입니다.
  - `eventUrl` - ISV 앱의 캘린더 이벤트 URL입니다.
- `resources` - 인사이트 생성과 관련된 다른 리소스가 포함된 목록입니다. 리소스 객체:
  - `appName` - 리소스가 속한 앱 이름입니다.
  - `resourceTitle` - 리소스 제목입니다.
  - `resourceType` - 리소스의 유형입니다. 가능한 값은 `EMAIL | EVENT | MESSAGE | TASK`입니다.
  - `resourceUrl` - 앱의 리소스 URL입니다.
  - `appIconUrl` - 리소스가 속한 앱의 이미지 URL입니다.
- `nextToken`(선택 사항) - 다음 인사이트 세트를 가져오기 위한 페이지 매김 토큰입니다. 이 필드는 선택 사항 필드이며, null을 반환하면 로드할 인사이트가 더 이상 없음을 의미합니다.

자세한 내용은 MeetingInsights 단원을 참조하십시오.

```
curl --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/meetingContexts" \
  --header "Authorization: Bearer <token>"
```

작업이 성공하면 서비스가 HTTP 201 응답을 다시 전송합니다.

```
200 OK

{
    "insights": [
        {
            "insightId": "74251e31-5962-49d2-9ca3-15EXAMPLE4444"
            "insightContent": "Project demo meeting coming up soon. Prepare
 accordingly",
            "insightTitle": "Demo meeting next week",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "calendarEvent": {
```

```
                    "startTime": {
                        "timeInUTC": 2023-10-08T10:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "endTime": {
                        "timeInUTC": 2023-10-08T11:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "eventUrl": "http://someapp.com/events/1234",
            }
            "resources": [
                {
                    "appName": "SOME_EMAIL_APP",
                    "resourceTitle": "Email for project demo",
                    "resourceType": "EMAIL",
                    "resourceUrl": "http://someapp.com/emails/1234",
                    "appIconUrl":"https://d3gdwnnn63ow7w.cloudfront.net/eup/123.svg"
                }
            ]
        },
        {
            "insightId": "98751e31-5962-49d2-9ca3-15EXAMPLE5555"
            "insightContent": "Important code complete task is now due. Consider
updating the status.",
            "insightTitle": "Code complete task is due",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "calendarEvent":{
                    "startTime": {
                        "timeInUTC": 2023-10-08T10:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "endTime": {
                        "timeInUTC": 2023-10-08T11:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "eventUrl": "http://someapp.com/events/1234",
            },
            "resources": [
                {
                    "appName": "SOME_TASK_APPLICATION",
                    "resourceTitle": "Code Complete task is due",
                    "resourceType": "TASK",
                    "resourceUrl": "http://someapp.com/task/1234",
                    "appIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/eup/123.svg"
```

```
                }
            ]
        }
    ],
    "nextToken": null
}
```

인사이트나 작업에 대한 피드백 제공

AppFabric PutFeedback API 작업을 사용하여 생성된 인사이트와 작업에 대한 피드백을 제공합니다. 이 기능을 앱에 내장하여 특정 InsightId 또는 ActionId에 대한 피드백 평점(1~5, 등급이 높을수록 좋음)을 제출할 수 있는 방법을 제공할 수 있습니다.

요청 필드

- `id` - 피드백을 받는 객체의 식별자입니다. 이는 InsightId 또는 ActionId일 수 있습니다.
- `feedbackFor` - 피드백을 받는 리소스 유형입니다. 가능한 값: `ACTIONABLE_INSIGHT` | `MEETING_INSIGHT` | `ACTION`
- `feedbackRating` - 피드백 평점은 1에서 5까지입니다. 평점이 높을수록 좋습니다.

응답 필드

- 응답 필드가 없습니다.

자세한 내용은 PutFeedback 단원을 참조하십시오.

```
curl --request POST \
  --url "https://productivity.appfabric.<region>.amazonaws.com"\
"/feedback" \
  --header "Authorization: Bearer <token>" \
  --header "Content-Type: application/json" \
  --data '{
    "id": "1234-5678-9012",
    "feedbackFor": "ACTIONABLE_INSIGHT"
    "feedbackRating": 3
}'
```

작업이 성공하면 서비스가 비어있는 HTTP 본문과 함께 HTTP 201 응답을 다시 전송합니다.

5단계. AppFabric을 요청하여 애플리케이션 확인

지금까지 AppFabric 앱 간 인사이트 및 작업을 포함하도록 애플리케이션 UI를 업데이트하고 단일 사용자에 대한 인사이트를 얻었습니다. 테스트에 만족하고 AppFabric이 풍부한 경험을 추가 사용자에게 확장하고 싶다면 AppFabric에 애플리케이션를 제출하여 검토 및 확인을 받을 수 있습니다. AppFabric은 광범위하게 도입할 수 있도록 하기 전에 애플리케이션 정보를 확인하여 앱 개발자, 최종 사용자 및 데이터를 보호함으로써 책임감 있는 방식으로 사용자 도입을 확대할 수 있는 기반을 마련합니다.

확인 프로세스 시작

appfabric-appverification@amazon.com으로 이메일을 보내고 앱 확인을 요청하여 확인 프로세스를 시작합니다.

사용자의 이메일에 다음 세부 정보를 포함합니다.

- AWS 계정 ID
- 확인하고자 하는 애플리케이션의 이름
- AppClient ID
- 연락처 정보

또한 우선순위와 영향을 평가하는 데 도움이 되도록 가능한 경우 다음 정보를 제공합니다.

- 액세스 권한을 부여하려는 예상 사용자 수
- 목표 출시일

> **Note**
>
> AWS 계정 관리자 또는 AWS 파트너 개발 관리자가 있는 경우 이메일에 복사하십시오. 이러한 연락처를 포함하면 확인 프로세스를 신속하게 처리할 수 있습니다.

확인 기준

확인 프로세스를 사용하기 전에 다음 기준을 충족하는지 확인합니다.

- 생산성을 AWS 계정 위해 AppFabric을 사용하려면 유효한를 사용해야 합니다.

또한 다음 기준 중 하나 이상을 충족합니다.

- 조직은 최소한 “AWS 선택” 티어가 AWS Partner Network 있는의 AWS 파트너입니다. 자세한 내용은 AWS 파트너 서비스 티어를 참조하세요.
- 조직이 지난 3년 이내에 AppFabric 서비스에 최소 1만 USD를 지출했어야 합니다.
- 애플리케이션은 AWS Marketplace에 등록되어 있어야 합니다. 자세한 내용은 AWS Marketplace를 참조하세요.

확인 상태 업데이트 대기

애플리케이션이 검토받은 후 이메일을 통해 답변을 드리며 AppClient의 상태는 `pending_verification`에서 `verified`으로 변경됩니다. 애플리케이션이 거부된 경우 확인 프로세스를 다시 시작해야 합니다.

생산성을 위한 AppFabric AppClients

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

생산성을 위한 AppFabric AppClient를 관리하여 인증 및 인증 프로세스의 원활한 운영 및 유지 관리를 보장할 수 있습니다.

AppClient의 세부 정보 가져오기

AppFabric `GetAppClient` API 작업을 사용하여 AppClient 상태 확인을 포함하여 AppClient에 대한 세부 정보를 볼 수 있습니다. 자세한 내용은 GetAppClient 단원을 참조하십시오.

AppClient의 세부 정보를 가져오려면 최소한 `"appfabric:GetAppClient"` IAM 정책 권한이 있어야 합니다. 자세한 내용은 AppClient의 세부 정보를 가져오는 액세스 허용 단원을 참조하십시오.

요청 필드

- `appClientId` - AppClient ID입니다.

응답 필드

- `appName` - AppFabric 사용자 포털의 동의 페이지에 사용자에게 표시될 애플리케이션의 이름입니다.
- `customerManagedKeyIdentifier`(선택 사항) - 데이터를 암호화하는 데 사용할 고객 관리형 키(KMS에서 생성)의 ARN입니다. 지정하지 않으면 AWS AppFabric 관리형 키가 사용됩니다.

- `description` - 애플리케이션에 대한 설명입니다.
- `redirectUrls` - 인증 후 최종 사용자를 리디렉션할 URI입니다. redirectUrl을 최대 5개 추가할 수 있습니다. 예를 들어 `https://localhost:8080`입니다.
- `starterUserEmails` - 애플리케이션이 검증될 때까지 인사이트를 수신할 수 있는 액세스가 허용되는 사용자 이메일 주소입니다. 이메일 주소는 하나만 사용할 수 있습니다. 예를 들어 `anyuser@example.com`입니다.
- `verificationStatus` - AppClient 확인 상태입니다.
  - `pending_verification` - AppFabric에서 AppClient 확인이 아직 진행 중입니다. AppClient가 확인되기 전까지는 한 명의 사용자(`starterUserEmails`에서 지정된 사용자)만 AppClient를 사용할 수 있습니다.
  - `verified` - AppFabric에서 확인 프로세스를 성공적으로 완료했으며 이제 AppClient가 완전히 확인되었습니다.
  - `rejected` - AppClient에 대한 확인 프로세스를 AppFabric에서 거부했습니다. 확인 프로세스를 다시 시작하고 성공적으로 완료하기 전까지는 추가 사용자가 AppClient를 사용할 수 없습니다.

```
curl --request GET \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111
```

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

```
200 OK

{
    "appClient": {
        "appName": "Test App",
        "arn": "arn:aws:appfabric:<region>:111122223333:appclient/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "customerManagedKeyArn": "arn:aws:kms:<region>:111122223333:key/<key>",
        "description": "This is a test app",
        "redirectUrls": [
            "https://localhost:8080"
        ],
```

```
        "starterUserEmails": [
            "anyuser@example.com"
        ],
        "verificationDetails": {
            "verificationStatus": "pending_verification"
        }
    }
}
```

AppClient 목록

AppFabric `ListAppClients` API 작업을 사용하여 AppClient 목록을 봅니다. AppFabric은 당 하나의 AppClient만 허용합니다 AWS 계정. 향후 변경될 수 있습니다. 자세한 내용은 ListAppClients 단원을 참조하십시오.

AppClients를 나열하려면 최소한 `"appfabric:ListAppClients"` IAM 정책 권한이 있어야 합니다. 자세한 내용은 AppClient 목록에 대한 액세스 허용 단원을 참조하십시오.

요청 필드

- 필수 필드가 없습니다.

응답 필드

- `appClientARN` - AppClient ID를 포함하는 Amazon 리소스 이름(ARN)입니다. 예를 들어 AppClient ID는 `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`입니다.
- `verificationStatus` - AppClient 확인 상태입니다.
  - `pending_verification` - AppFabric에서 AppClient 확인이 아직 진행 중입니다. AppClient가 확인되기 전까지는 한 명의 사용자(`starterUserEmails`에서 지정된 사용자)만 AppClient를 사용할 수 있습니다.
  - `verified` - AppFabric에서 확인 프로세스를 성공적으로 완료했으며 이제 AppClient가 완전히 확인되었습니다.
  - `rejected` - AppClient에 대한 확인 프로세스를 AppFabric에서 거부했습니다. 확인 프로세스를 다시 시작하고 성공적으로 완료하기 전까지는 추가 사용자가 AppClient를 사용할 수 없습니다.

```
curl --request GET \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
```

```
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients
```

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

```
200 OK

{
    "appClientList": [
        {
            "appClientArn": "arn:aws:appfabric:<region>:111122223333:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "verificationStatus": "pending_verification"
        }
    ]
}
```

AppClient 업데이트

AppFabric `UpdateAppClient` API 작업을 사용하여 AppClient에 매핑된 redirectUrls을 업데이트합니다. AppName, StarterUserEmail 등과 같은 다른 파라미터를 변경해야 하는 경우 AppClient를 삭제하고 새 파라미터를 생성해야 합니다. 자세한 내용은 UpdateAppClient 단원을 참조하십시오.

AppClient를 업데이트하려면 최소한 `"appfabric:UpdateAppClient"` IAM 정책 권한이 있어야 합니다. 자세한 내용은 AppClient 업데이트 액세스 허용 단원을 참조하십시오.

요청 필드

- `appClientId`(필수) - 리디렉션 URL을 업데이트하려는 AppClient ID입니다.
- `redirectUrls`(필수) - 업데이트된 리디렉션 URL 목록입니다. redirectUrl을 최대 5개 추가할 수 있습니다.

응답 필드

- `appName` - AppFabric 사용자 포털의 동의 페이지에 사용자에게 표시될 애플리케이션의 이름입니다.
- `customerManagedKeyIdentifier`(선택 사항) - 데이터를 암호화하는 데 사용할 고객 관리형 키(KMS에서 생성)의 ARN입니다. 지정하지 않으면 AWS AppFabric 관리형 키가 사용됩니다.

- `description` - 애플리케이션에 대한 설명입니다.
- `redirectUrls` - 인증 후 최종 사용자를 리디렉션할 URI입니다. 예를 들어 `https://localhost:8080`입니다.
- `starterUserEmails` - 애플리케이션이 검증될 때까지 인사이트를 수신할 수 있는 액세스가 허용되는 사용자 이메일 주소입니다. 이메일 주소는 하나만 사용할 수 있습니다. 예를 들어 `anyuser@example.com`입니다.
- `verificationStatus` - AppClient 확인 상태입니다.
  - `pending_verification` - AppFabric에서 AppClient 확인이 아직 진행 중입니다. AppClient가 확인되기 전까지는 한 명의 사용자(`starterUserEmails`에서 지정된 사용자)만 AppClient를 사용할 수 있습니다.
  - `verified` - AppFabric에서 확인 프로세스를 성공적으로 완료했으며 이제 AppClient가 완전히 확인되었습니다.
  - `rejected` - AppClient에 대한 확인 프로세스를 AppFabric에서 거부했습니다. 확인 프로세스를 다시 시작하고 성공적으로 완료하기 전까지는 추가 사용자가 AppClient를 사용할 수 없습니다.

```
curl --request PATCH \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 \
  --data '{
    "redirectUrls": ["https://localhost:8081"]
}'
```

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

```
200 OK

{
    "appClient": {
        "appName": "Test App",
        "arn": "arn:aws:appfabric:<region>:111122223333:appclient/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "customerManagedKeyArn": "arn:aws:kms:<region>:111122223333:key/<key>",
        "description": "This is a test app",
```

```
        "redirectUrls": [
            "https://localhost:8081"
        ],
        "starterUserEmails": [
            "anyuser@example.com"
        ],
        "verificationDetails": {
            "verificationStatus": "pending_verification"
        }
    }
}
```

AppClient 삭제

AppFabric `DeleteAppClient` API 작업을 사용하여 더 이상 필요하지 않은 AppClient를 삭제합니다. 자세한 내용은 DeleteAppClient 단원을 참조하십시오.

AppClient를 삭제하려면 최소한 `"appfabric:DeleteAppClient"` IAM 정책 권한이 있어야 합니다. 자세한 내용은 AppClient 삭제 액세스 허용 단원을 참조하십시오.

요청 필드

- `appClientId` - AppClient ID입니다.

응답 필드

- 응답 필드가 없습니다.

```
curl --request DELETE \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111
```

액션이 성공하면 해당 서비스는 빈 HTTP 본문과 함께 HTTP 204 응답을 되돌려줍니다.

최종 사용자를 위한 새로 고침 토큰

AppClient가 최종 사용자를 위해 획득한 토큰은 만료 시 새로 고침할 수 있습니다. 이는 grant_type `refresh_token`과 함께 토큰 API를 사용하여 수행할 수 있습니다. grant_type이 `authorization_code`면 사용할 `refresh_token`이 토큰 API 응답의 일부로 반환됩니다. 기본 만료는 12시간입니다. 새로 고침 API를 직접적으로 호출하려면 `"appfabric:Token"` IAM 정책 권한이 있어야 합니다. 자세한 내용은 토큰 및 AppClient 업데이트 액세스 허용 섹션을 참조하세요.

요청 필드

- `refresh_token`(필수) - 초기 `/token` 요청에서 받은 새로 고침 토큰입니다.
- `app_client_id`(필수) - AWS 계정를 위해 생성된 AppClient 리소스의 ID입니다.
- `grant_type`(필수) - `refresh_token`이어야 합니다.

응답 필드

- `expires_in` - 토큰이 만료되기까지 남은 기간입니다. 기본 만료 시간은 12시간입니다.
- `refresh_token` - 초기 요청과 토큰 요청에서 받은 새로 고침 토큰입니다.
- `token` - 초기 요청과 토큰 요청에서 받은 토큰입니다.
- `token_type` - 값은 `Bearer`입니다.
- `appfabric_user_id` - AppFabric 사용자 ID입니다. `authorization_code` 권한 부여 유형을 사용하는 요청의 경우에만 반환됩니다.

```
curl --location \
"https://appfabric.<region>.amazonaws.com/oauth2/token" \
--header "Content-Type: application/json" \
--header "X-Amz-Content-Sha256: <sha256_payload>" \
--header "X-Amz-Security-Token: <security_token>" \
--header "X-Amz-Date: 20230922T172215Z" \
--header "Authorization: AWS4-HMAC-SHA256 ..." \
--data "{
    \"refresh_token\": \"<refresh_token>",
    \"app_client_id\": \"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\",
    \"grant_type\": \"refresh_token\"
}"
```

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

```
200 OK

{
    "expires_in": 43200,
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "${UserID}"
}
```

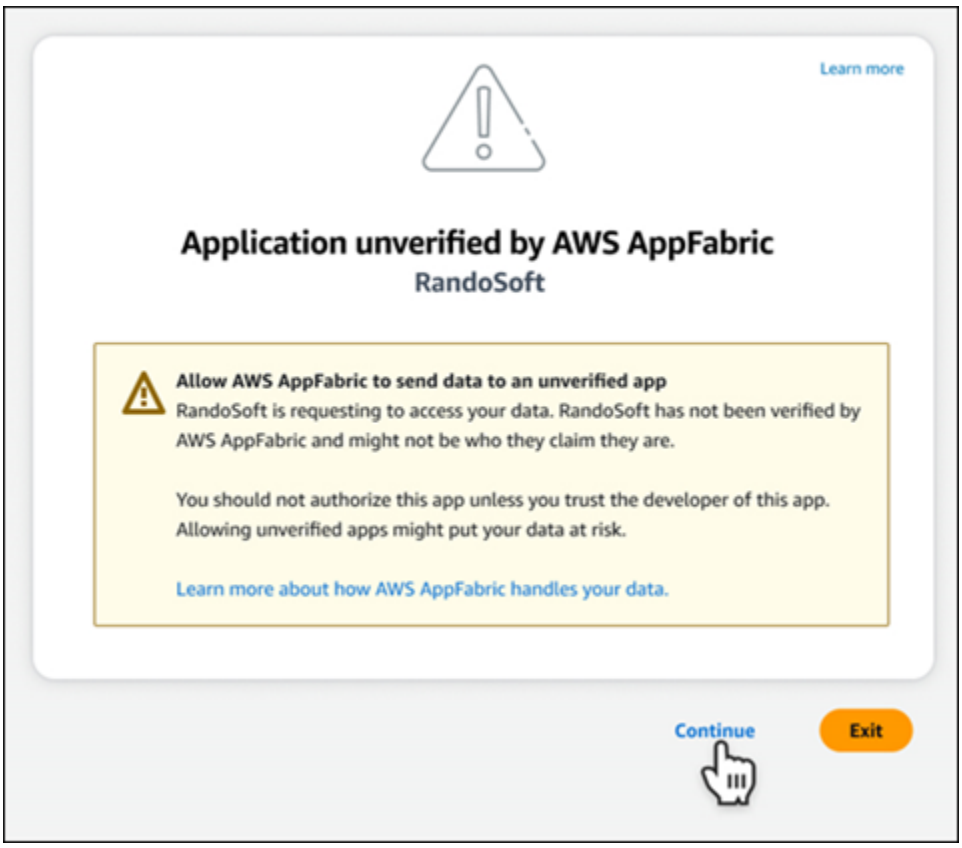
생산성을 위한 AppClients 문제 해결 AppFabric

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

이 섹션에서는 생산성을 위한 AppFabric의 일반적인 오류와 문제 해결에 대해 설명합니다.

확인되지 않은 애플리케이션

생산성을 위한 AppFabric을 사용하여 앱 경험을 강화하는 앱 개발자는 최종 사용자에게 기능을 출시하기 전에 확인 프로세스를 거칩니다. 모든 애플리케이션은 확인되지 않은 상태로 시작하다가 확인 프로세스가 완료되어야만 확인된 것으로 변경됩니다. 즉, AppClient를 생성할 때 사용한 `starterUserEmails`에 사용자에게 이 메시지가 표시됩니다.



`CreateAppClient` 오류

ServiceQuotaExceededException

AppClient를 생성할 때 다음 예외가 발생하면 AWS 계정당 생성할 수 있는 AppClient의 수를 초과한 것입니다. 한도는 1입니다. HTTP 상태 코드: 402

```
ServiceQuotaExceededException / SERVICE_QUOTA_EXCEEDED
You have exceeded the number of AppClients that can be created per AWS Account. The
 limit is 1.
HTTP Status Code: 402
```

`GetAppClient` 오류

ResourceNotFoundException

AppClient에 대한 세부 정보를 가져올 때 다음과 같은 예외가 발생하면 올바른 AppClient 식별자를 입력했는지 확인합니다. 이 오류는 지정된 AppClient를 찾을 수 없음을 나타냅니다.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
```

```
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

`DeleteAppClient` 오류

ConflictException

AppClient를 삭제할 때 다음과 같은 예외가 발생하면 다른 삭제 요청이 진행 중인 것입니다. 완료될 때까지 잠시 기다렸다가 다시 시도하세요. HTTP 상태 코드: 409

```
ConflictException
Another delete request is in progress. Wait until it completes then try again.
HTTP Status Code: 409
```

ResourceNotFoundException

AppClient를 삭제할 때 다음과 같은 예외가 발생하면 올바른 AppClient 식별자를 입력했는지 확인합니다. 이 오류는 지정된 AppClient를 찾을 수 없음을 나타냅니다.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

`UpdateAppClient` 오류

ResourceNotFoundException

AppClient를 업데이트할 때 다음과 같은 예외가 발생하면 올바른 AppClient 식별자를 입력했는지 확인합니다. 이 오류는 지정된 AppClient를 찾을 수 없음을 나타냅니다.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

`Authorize` 오류

ValidationException

API 파라미터 중 하나라도 API 사양에 정의된 제약 조건을 충족하지 않는 경우 다음과 같은 예외가 발생할 수 있습니다.

```
ValidationException
HTTP Status Code: 400
```

이유 1: AppClient ID가 지정되지 않은 경우

요청 파라미터에 `app_client_id`가 없습니다. AppClient가 아직 생성되지 않은 경우 AppClient를 생성하거나 기존 `app_client_id`를 사용하여 다시 시도하세요. AppClient ID를 찾으려면 ListAppClient API 작업을 사용합니다.

이유 2: AppFabric이 고객 관리형 키에 액세스할 수 없는 경우

```
Message: AppFabric couldn't access the customer managed key configured for AppClient.
```

AppFabric은 현재 고객 관리형 키에 액세스할 수 없습니다. 이는 최근에 권한이 변경되었기 때문일 수 있습니다. 지정된 키가 존재하는지 확인하고 AppFabric에 적절한 액세스 권한이 부여되었는지 확인합니다.

이유 3: 지정된 리디렉션 URL이 유효하지 않은 경우

```
Message: Redirect url invalid
```

요청의 리디렉션 URL이 정확한지 확인합니다. AppClient를 생성하거나 업데이트할 때 지정한 리디렉션 URL 중 하나와 일치해야 합니다. 허용된 리디렉션 URL 목록을 보려면 GetAppClient API 작업을 사용합니다.

`Token` 오류

TokenException

몇 가지 이유로 다음과 같은 예외가 발생할 수 있습니다.

```
TokenException
```

```
HTTP Status Code: 400
```

이유 1: 유효하지 않은 이메일이 지정된 경우

```
Message: Invalid Email used
```

사용 중인 이메일 주소가 AppClient를 생성할 때 `starterUserEmails` 속성에 나열한 주소와 일치하는지 확인합니다. 이메일이 일치하지 않으면 일치하는 이메일 주소로 변경한 후 다시 시도하세요. 사용된 이메일을 보려면 GetAppClient API 작업을 사용합니다.

이유 2: grant_type이 refresh_token일 때 토큰이 지정되지 않았을 경우

```
Message: refresh_token must be non-null for Refresh Token Grant-type
```

요청에 지정된 새로 고침 토큰이 null이거나 비어있습니다. 토큰 API 직접 호출 응답에서 수신한 활성 `refresh_token`을 지정합니다.

ThrottlingException

허용된 할당량을 초과하는 속도로 API를 호출하는 경우 다음과 같은 예외가 발생할 수 있습니다.

```
ThrottlingException
HTTP Status Code: 429
```

ListActionableInsights, **ListMeetingInsights**, **PutFeedback** 오류

ValidationException

API 파라미터 중 하나라도 API 사양에 정의된 제약 조건을 충족하지 않는 경우 다음과 같은 예외가 발생할 수 있습니다.

```
ValidationException
HTTP Status Code: 400
```

ThrottlingException

허용된 할당량을 초과하는 속도로 API를 호출하는 경우 다음과 같은 예외가 발생할 수 있습니다.

```
ThrottlingException
HTTP Status Code: 429
```

최종 사용자를 위한 생산성을 위한 AppFabric(미리 보기) 시작하기

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

이 섹션은 생산성을 위한 AWS AppFabric(미리 보기)을 활성화하여 작업 관리 및 워크플로 효율성을 개선하려는 SaaS 애플리케이션의 최종 사용자를 대상으로 합니다. 다음 단계에 따라 애플리케이션을 연결하고 AppFabric이 앱 간 인사이트를 표시하여 선호하는 애플리케이션에서 작업(예: 이메일 전송 또는 회의 예약)을 완료할 수 있도록 권한을 부여합니다. Asana, Atlassian Jira Suite, Google Workspace, Microsoft 365, Miro, Slack, Smartsheet 등과 같은 애플리케이션을 연결할 수 있습니다. AppFabric이 콘텐츠에 액세스할 수 있도록 권한을 부여한 후 AppFabric은 선호하는 앱 내에서 앱 간 인사이트와 작업을 직접 가져와 더 효율적으로 작업하고 현재 워크플로를 유지할 수 있도록 지원합니다.

생산성을 위한 AppFabric은 Amazon Bedrock에서 제공하는 생성형 AI를 사용합니다. AppFabric은 명시적인 허가를 받은 후에만 인사이트와 작업를 생성합니다. 각 개별 애플리케이션이 어떤 콘텐츠를 사용할지 완전히 제어할 수 있도록 권한을 부여합니다. AppFabric은 인사이트를 생성하는 데 사용되는 기본 대규모 언어 모델을 학습하거나 개선하는 데 데이터를 사용하지 않습니다. 자세한 내용은 Amazon Bedrock FAQ를 참조하세요.

주제

사전 조건

시작하기 전에 다음이 있는지 확인합니다.

- AppFabric에 로그인하기 위한 보안 인증 정보: 생산성을 위한 AppFabric을 사용하려면 Asana, Google Workspace, Microsoft 365 또는 Slack 공급업체 중 하나에 대한 페더레이션된 로그인 보안 인증 정보(사용자 이름과 암호)가 필요합니다. AppFabric에 로그인하면 생산성을 위한 AppFabric을

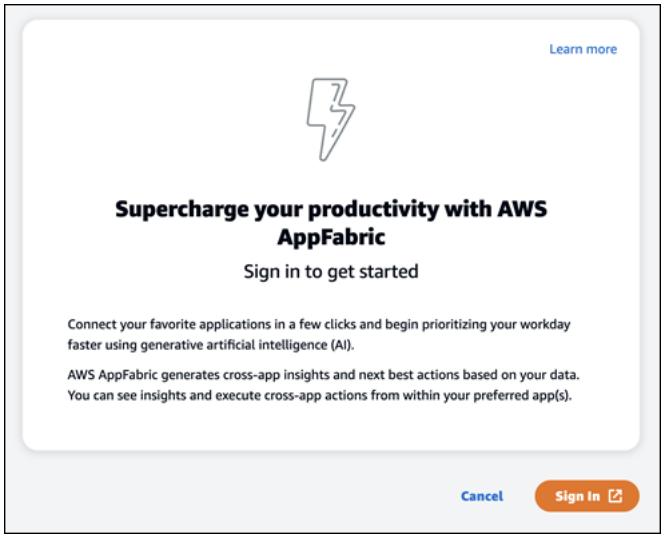
활성화하는 각 애플리케이션에서 사용자로 식별할 수 있습니다. 로그인한 후 애플리케이션을 연결하여 인사이트 생성을 시작할 수 있습니다.

- 애플리케이션 연결을 위한 보안 인증 정보: 앱 간 인사이트와 작업은 인증한 애플리케이션을 기반으로만 생성됩니다. 인증하려는 각 애플리케이션에 대한 로그인 보안 인증 정보(사용자 이름 및 암호)가 필요합니다. Asana, Atlassian Jira Suite, Google Workspace, Microsoft 365, Miro, Slack, Smartsheet와 같은 애플리케이션이 지원됩니다.

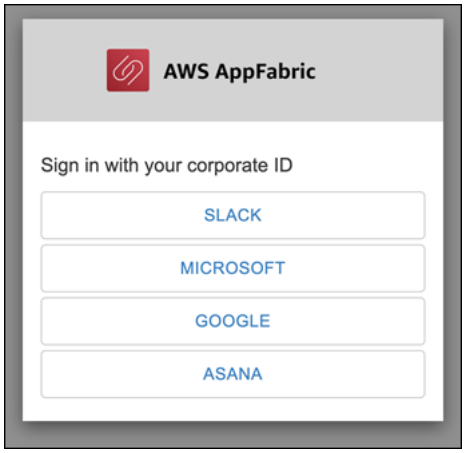
1단계. AppFabric 로그인

애플리케이션을 AppFabric에 연결하여 원하는 애플리케이션 내에서 콘텐츠와 인사이트를 직접 가져올 수 있습니다.

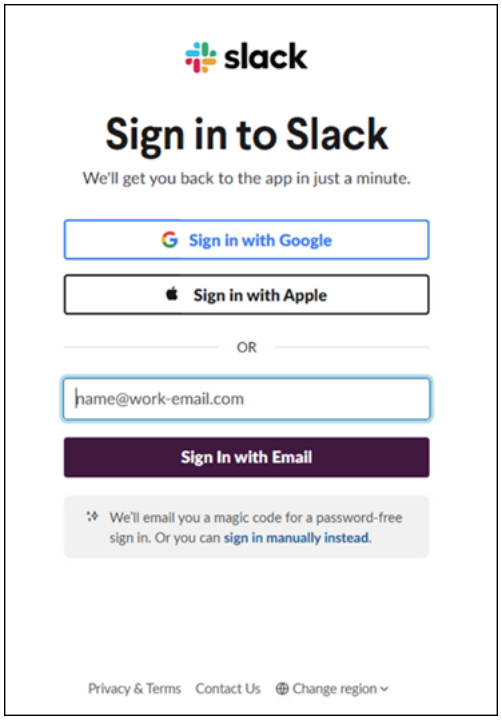
1. 모든 애플리케이션은 다양한 방식으로 생산성을 위한 AppFabric을 사용하여 더 풍부한 앱 경험을 제공합니다. 따라서 모든 애플리케이션마다 생산성을 위한 AppFabric 홈 페이지에 접속할 수 있는 진입점이 달라집니다. 홈 페이지는 AppFabric을 활성화하는 프로세스에 대한 컨텍스트를 설정하고 먼저 로그인하라는 메시지를 표시합니다. AppFabric을 활성화하려는 모든 애플리케이션이 이 화면에 표시됩니다.

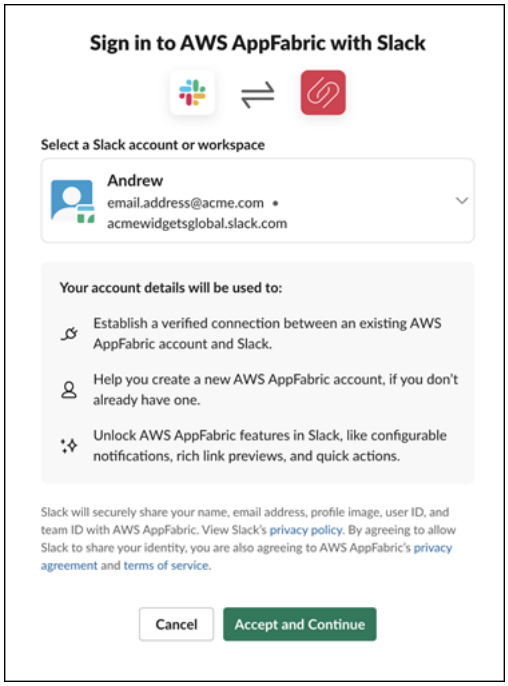


2. Asana, Google Workspace, Microsoft 365, 또는 Slack 공급업체 중 한 곳의 보안 인증 정보를 사용하여 로그인합니다. 최상의 경험을 위해 AppFabric을 활성화한 각 애플리케이션에 대해 동일한 공급업체를 사용하여 로그인하는 것이 좋습니다. 예를 들어, App1에서 Google Workspace 보안 인증 정보를 선택하면 App2에서 Google Workspace 선택을 권장하며, 이후에 다시 로그인해야 할 때도 마찬가지입니다. 다른 공급업체로 로그인하는 경우 애플리케이션 연결 프로세스를 다시 시작해야 합니다.



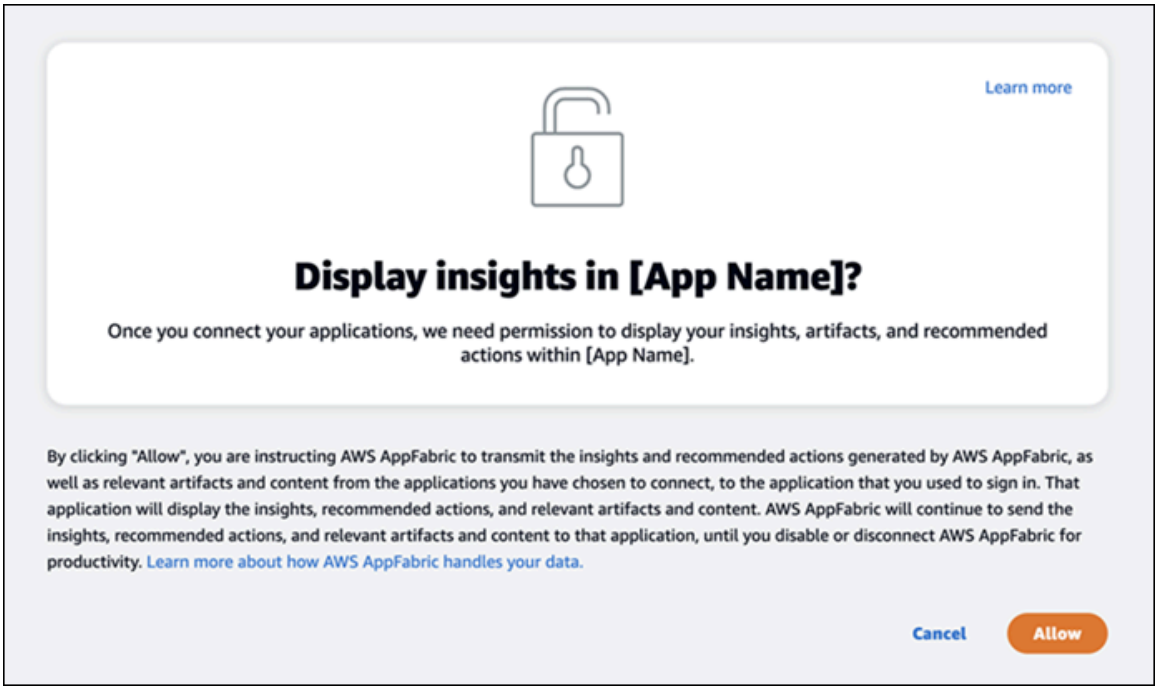
3. 메세지가 표시되면 로그인 보안 인증 정보를 입력하고 공급업체에서 AppFabric에 로그인하는 것을 수락합니다.





2단계. 앱에 인사이트가 표시되도록 동의

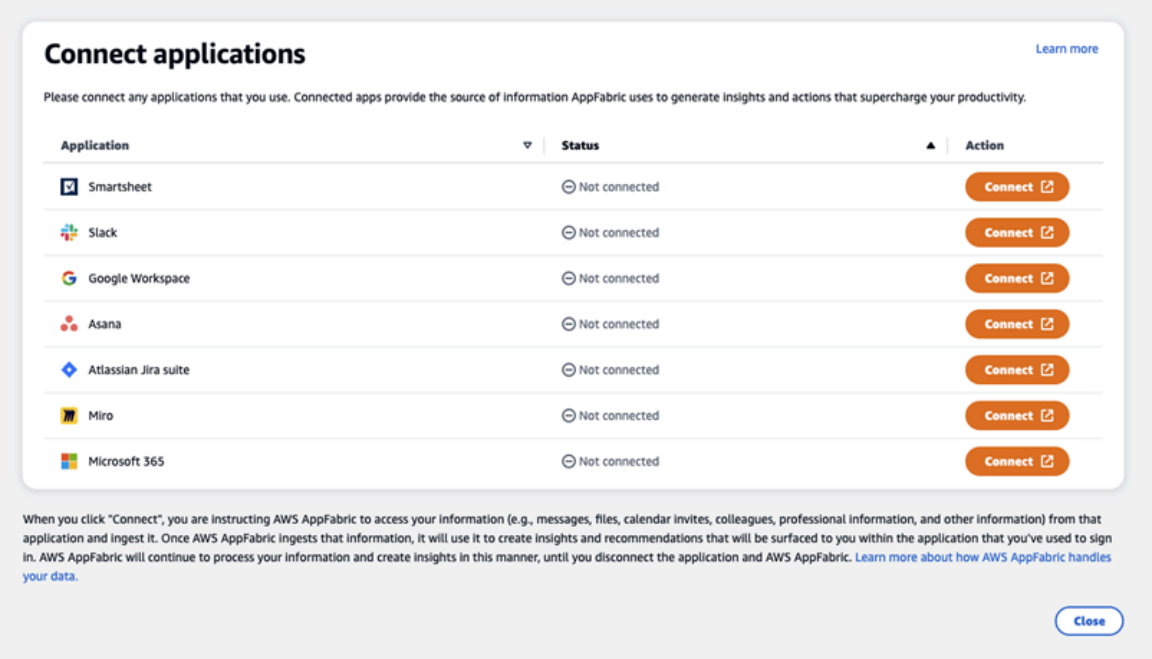
로그인한 후 AppFabric은 생산성을 위한 AppFabric을 활성화하는 애플리케이션 내에서 앱 간 인사이트 및 작업을 AppFabric이 표시할 수 있도록 허용할지 묻는 동의 페이지를 표시합니다. 예를 들면, AppFabric이 Google Workspace 이메일과 캘린더 이벤트를 가져와서 Asana에 표시하도록 허용합니까? 이 동의 단계는 AppFabric을 활성화하는 애플리케이션 당 한 번만 완료하면 됩니다.



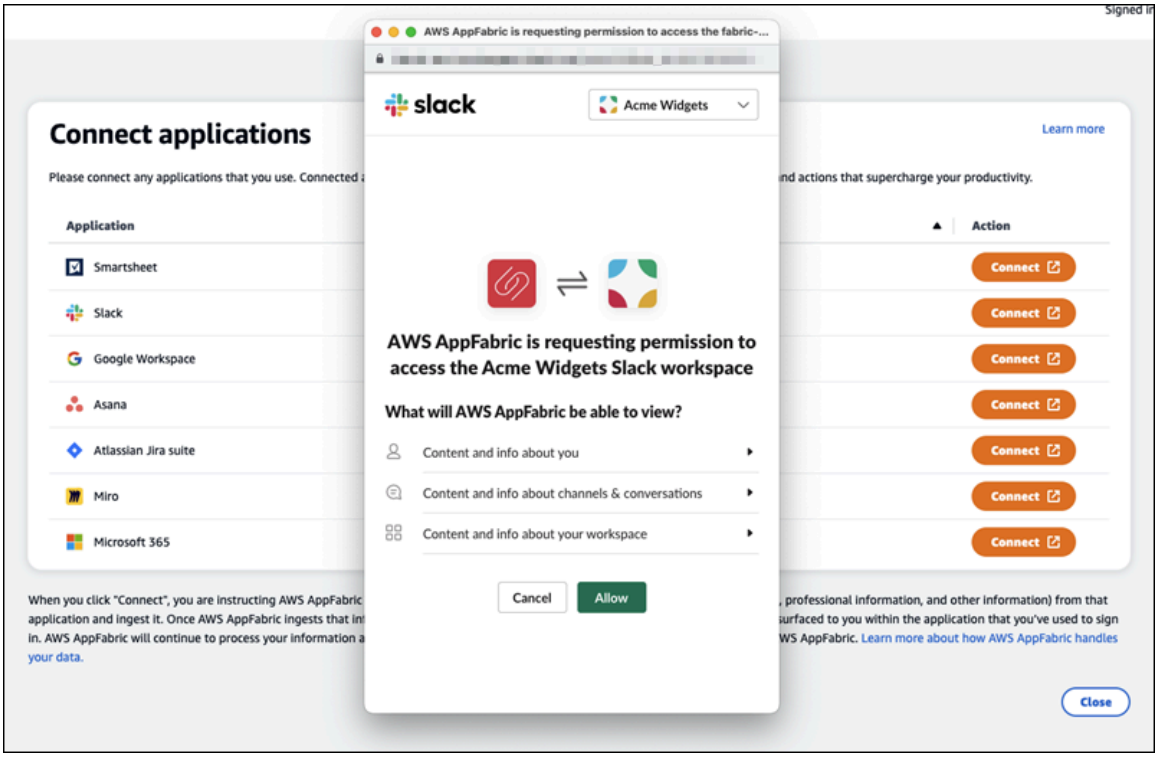
3단계. 애플리케이션을 연결하여 인사이트와 작업 생성

동의 페이지를 완료하면 애플리케이션 연결 페이지로 이동합니다. 여기서 개별 애플리케이션을 연결, 연결 해제 또는 재연결할 수 있으며 이 페이지는 궁극적으로 앱 간 인사이트 및 작업을 생성하는 데 사용됩니다. 대부분의 경우 로그인하고 동의한 후에 이 페이지를 사용하여 연결된 애플리케이션을 관리하게 됩니다.

애플리케이션을 연결하려면 사용하는 애플리케이션 옆에 있는 연결 버튼을 선택합니다.



애플리케이션에 대한 로그인 보안 인증 정보를 제공하고 AppFabric이 데이터에 액세스할 수 있는 권한을 허용하여 인사이트를 생성하고 작업을 완료해야 합니다.

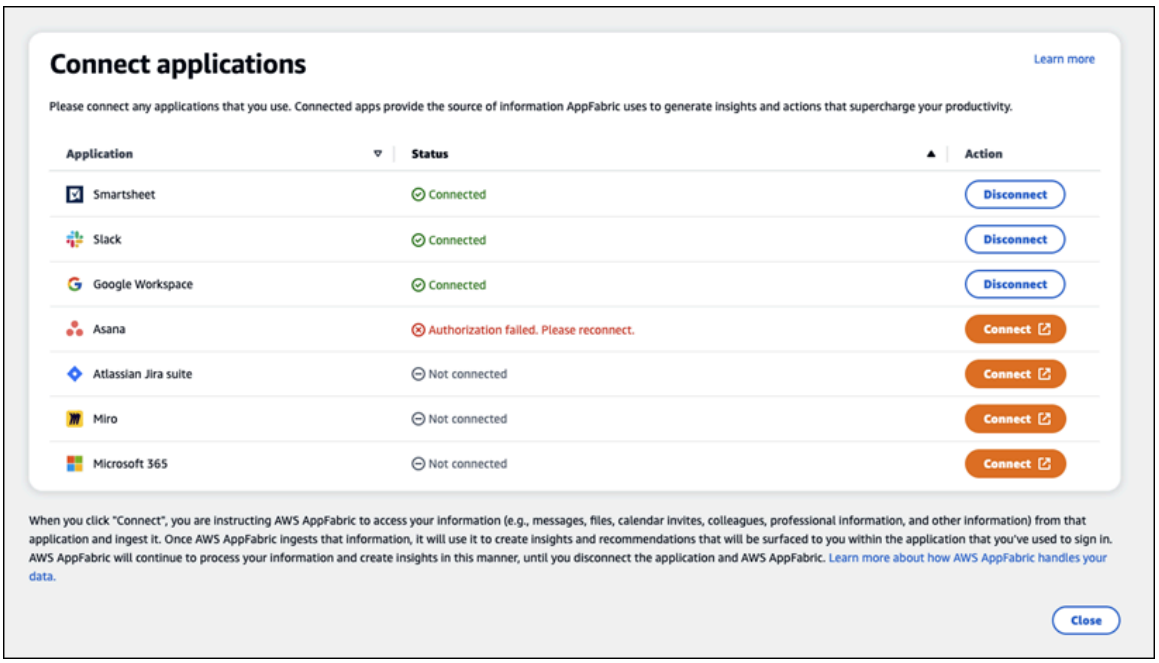


애플리케이션을 성공적으로 연결하면 해당 애플리케이션의 상태가 “연결되지 않음”에서 “연결됨”으로 변경됩니다. 알림: 인사이트와 작업을 생성하는 데 사용하려는 모든 애플리케이션에 대해 이 인증 단계를 완료해야 합니다.

애플리케이션 연결은 영구적이지 않습니다. 애플리케이션을 주기적으로 다시 연결해야 합니다. 이렇게 하는 이유는 인사이트를 생성할 수 있는 허가를 계속 받을 수 있도록 하기 위함입니다.

가능한 상태는 다음과 같습니다.

- 연결됨 - AppFabric에 권한이 부여되었으며 이 애플리케이션의 데이터를 사용하여 인사이트를 생성하고 있습니다.
- 연결되지 않음 - AppFabric이 이 애플리케이션의 데이터를 사용하여 인사이트를 생성하고 있지 않습니다. 연결하여 인사이트 생성을 시작할 수 있습니다.
- 인증에 실패했습니다. 다시 연결해 주세요. - 특정 애플리케이션에서 인증 실패가 있을 수 있습니다. 이 오류를 확인하려면 연결을 사용하여 애플리케이션 재연결을 시도합니다.



설정을 완료했으며 애플리케이션으로 돌아갈 수 있습니다. 애플리케이션에서 인사이트 확인을 시작하는 데 최소 몇 시간이 걸릴 수 있습니다.

필요한 경우 이 페이지로 이동하여 연결된 애플리케이션을 관리할 수 있습니다. 애플리케이션 연결 해제를 선택하면 AppFabric은 새로운 인사이트를 생성하기 위해 해당 애플리케이션의 데이터 사용 또는 새 데이터 수집을 중단합니다. 해당 기간 내에 애플리케이션을 다시 연결하지 않도록 선택하면 연결이 끊긴 애플리케이션의 데이터는 7일 이내에 자동으로 삭제됩니다.

4단계. 인사이트를 확인 시작 및 애플리케이션에서 앱 간 작업 실행

애플리케이션을 AppFabric과 연결한 후 중요한 인사이트에 액세스하고 선호하는 애플리케이션에서 직접 앱 간 작업을 수행할 수 있습니다. 참고: 각 앱에서 이 기능이 보장되는 것은 아니며, 애플리케이션 개발자가 어떤 생산성을 위한 AppFabric 기능을 활성화하기로 선택했는지에 따라 전적으로 달라집니다.

앱 간 인사이트

생산성을 위한 AppFabric은 다음과 같은 두 가지 유형의 인사이트를 제공합니다.

- 실행 가능한 인사이트: AppFabric은 연결된 앱 전반의 이메일, 캘린더 이벤트, 작업 및 메시지의 정보를 분석하고 우선순위를 정하는 데 중요할 수 있는 주요 인사이트를 생성합니다. 또한 AppFabric은 선호하는 애플리케이션 내에서 편집 및 실행할 수 있는 권장 작업(예: 이메일 전송, 회의 예약, 작업 생성)을 생성할 수 있습니다. 예를 들어, 처리해야 할 고객 에스컬레이션이 있다는 인사이트와 고객과의 회의 일정을 잡기 위한 다음 작업을 제안 받을 수 있습니다.

- 회의 준비 인사이트: 이 기능을 사용하면 예정된 회의를 가장 잘 준비할 수 있습니다. AppFabric은 예정된 회의를 분석하고 회의 목적에 대한 간략한 요약을 생성합니다. 또한 콘텐츠를 찾기 위해 앱을 전환하지 않고도 회의를 효율적으로 준비하는 데 도움이 되는 연결된 애플리케이션에서 관련 아티팩트(예: 이메일, 메시지, 작업)를 표시합니다.

앱 간 작업

특정 인사이트를 위해 AppFabric은 이메일 전송, 회의 예약, 작업 생성과 같은 권장 작업을 생성할 수도 있습니다. 작업을 생성할 때 AppFabric은 연결된 애플리케이션의 콘텐츠 및 컨텍스트를 기반으로 특정 필드를 미리 채울 수 있습니다. 예를 들어 AppFabric은 인사이트를 기반으로 제안된 이메일 응답 또는 작업 이름을 생성할 수 있습니다. 제안된 작업을 클릭하면 작업을 실행하기 전에 미리 채워진 콘텐츠를 편집할 수 있는 AppFabric 소유의 사용자 인터페이스로 이동합니다. 생성형 AI와 기본 대규모 언어 모델(LLM)이 때때로 착각할 수 있으므로 AppFabric은 사용자가 먼저 검토하고 입력하지 않으면 작업을 실행하지 않습니다.

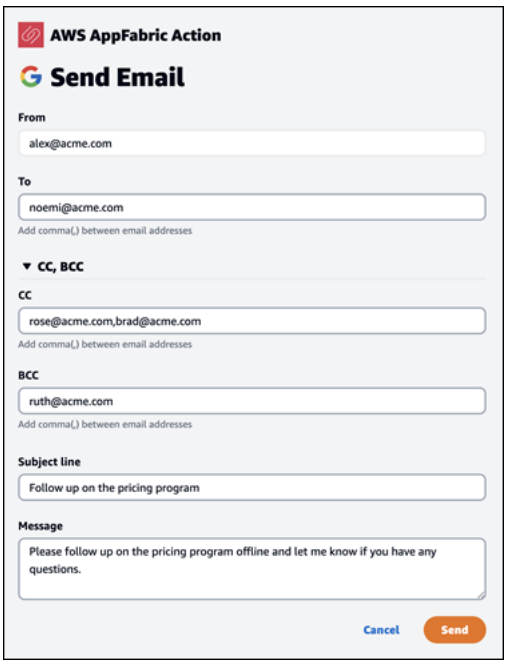
> **Note**
>
> AppFabric LLM 출력을 검증하고 확인할 책임은 귀하에게 있습니다. AppFabric은 LLM 출력의 정확성이나 품질을 보장하지 않습니다. 자세한 내용은 AWS 책임감 있는 AI 정책을 참조하세요.

이메일(Google Workspace, Microsoft 365) 생성

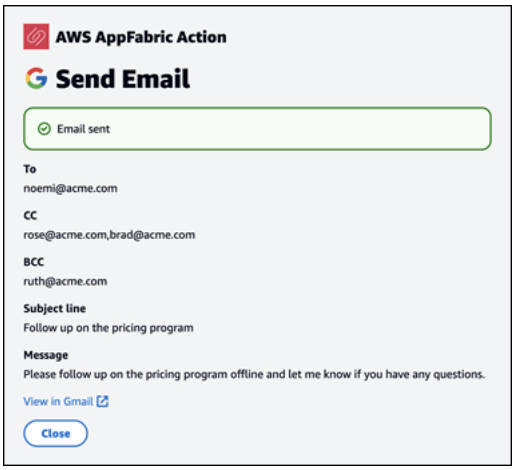
AppFabric을 사용하면 원하는 애플리케이션 내에서 이메일을 편집하고 전송할 수 있습니다. 보낸 사람, 받는 사람, 참조/숨은 참조, 이메일 제목줄 및 이메일 본문 메시지를 포함한 기본 전자 메일 필드를 지원합니다. AppFabric은 이러한 필드에 콘텐츠를 생성하여 작업 완료 시간을 단축할 수 있습니다. 이메일 편집을 완료한 후 전송을 선택하여 이메일을 보냅니다.

이메일을 보내려면 다음 필드가 필요합니다.

- 수신자 이메일(받는 사람, 참조, 숨은 참조) 중 하나 이상이 필요하며 유효한 이메일 주소여야 합니다.
- 제목줄 및 메시지 필드입니다.



이메일이 전송된 후 이메일이 전송되었다는 확인 메시지가 표시됩니다. 또한 지정된 애플리케이션에서 이메일을 볼 수 있는 링크가 표시됩니다. 이 링크를 사용하여 애플리케이션으로 빠르게 이동하여 이메일이 전송되었는지 확인할 수 있습니다.

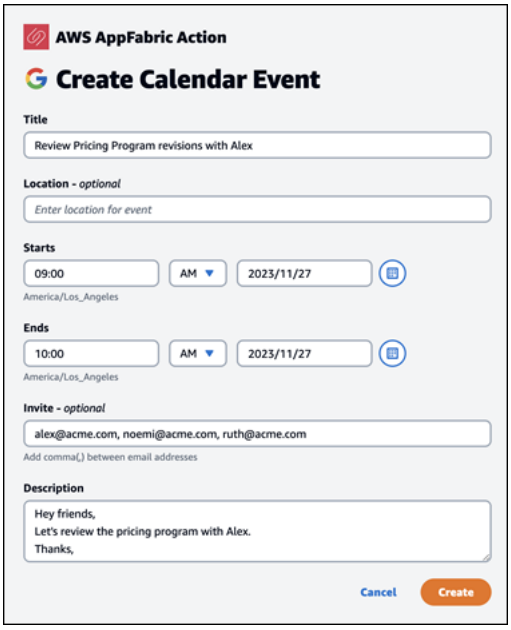


캘린더 이벤트(Google Workspace, Microsoft 365) 생성

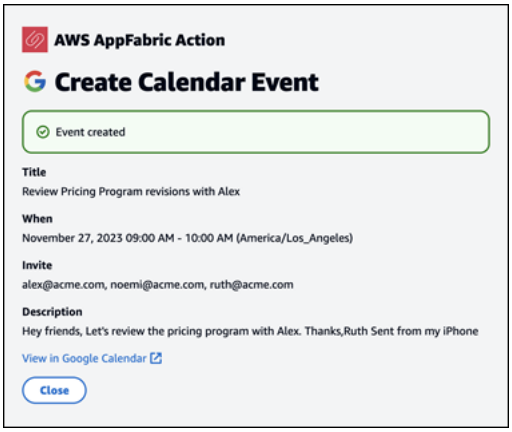
AppFabric을 사용하면 원하는 애플리케이션 내에서 캘린더 이벤트를 편집하고 생성할 수 있습니다. 이벤트 제목, 위치, 시작 시간, 종료 시간, 시작 날짜, 종료 날짜, 초대받는 사람 목록, 이벤트 세부 정보를 포함한 기본 캘린더 이벤트 필드를 지원합니다. AppFabric은 이러한 필드에 콘텐츠를 생성하여 작업 완료 시간을 단축할 수 있습니다. 캘린더 이벤트 편집을 완료한 후 생성을 선택하여 이벤트를 생성합니다.

캘린더 이벤트를 만들려면 다음 필드가 필요합니다.

- 제목, 시작, 종료 및 설명 필드입니다.
- 시작 시간 및 날짜는 종료 시간 및 날짜보다 이전이 아니어야 합니다.
- 초대 필드는 선택 사항이지만 제공된 경우 유효한 이메일 주소가 필요합니다.



캘린더 이벤트가 전송된 후 이벤트가 생성되었다는 확인 메시지가 표시됩니다. 또한 지정된 애플리케이션에서 이벤트를 볼 수 있는 링크가 표시됩니다. 이 링크를 사용하여 애플리케이션으로 빠르게 이동하여 이벤트가 생성되었는지 확인할 수 있습니다.



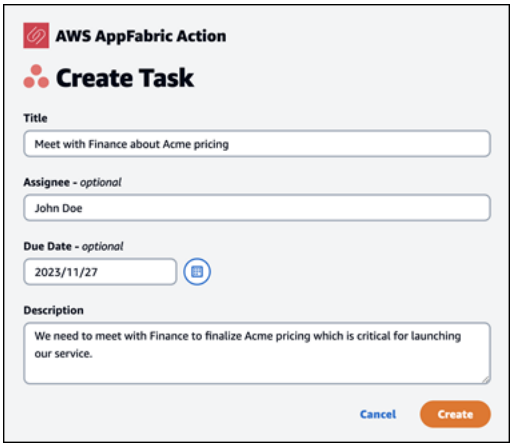
작업(Asana) 생성

AppFabric을 사용하면 원하는 애플리케이션 내에서 Asana의 작업을 편집하고 생성할 수 있습니다. 작업 이름, 작업 소유자, 기한, 작업 설명과 같은 기본 작업 필드를 지원합니다. AppFabric은 이러한 필드

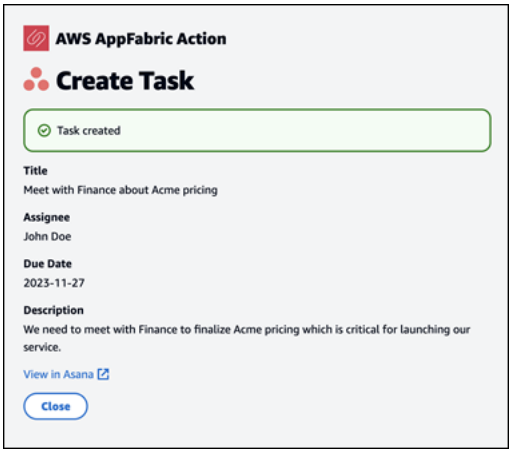
에 콘텐츠를 생성하여 작업 생성 시간을 단축할 수 있습니다. 작업 편집을 완료한 후 생성을 선택하여 작업을 생성합니다. 작업은 LLM에서 제안한 대로 해당 Asana 워크스페이스나 프로젝트 또는 작업에 생성됩니다.

Asana 작업을 생성하려면 다음 필드가 필요합니다.

- 제목 및 설명 필드입니다.
- 담당자는 유효한 이메일 주소로 수정해야 합니다.



작업이 생성되고 나면 작업이 Asana에서 생성되었다는 확인 메시지가 표시됩니다. 또한 Asana의 작업을 볼 수 있는 링크도 표시됩니다. 이 링크를 사용하면 애플리케이션으로 빠르게 이동하여 작업이 생성되었는지 확인하거나 적절한 Asana 작업 공간이나 프로젝트 또는 작업으로 이동할 수 있습니다.



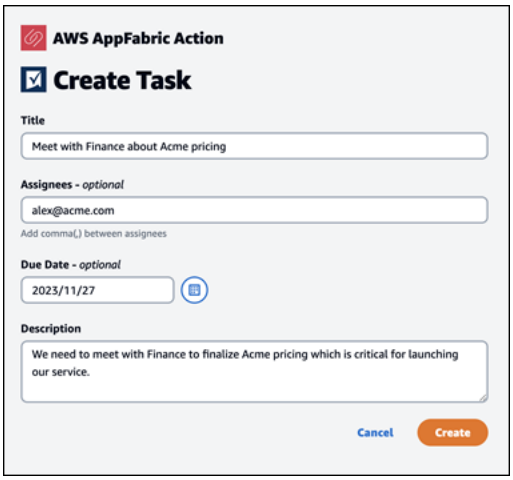
작업(Smartsheet) 생성

AppFabric을 사용하면 원하는 애플리케이션 내에서 Smartsheet의 작업을 편집하고 생성할 수 있습니다. 작업 이름, 작업 소유자, 기한, 작업 설명과 같은 기본 작업 필드를 지원합니다. AppFabric은 이러한

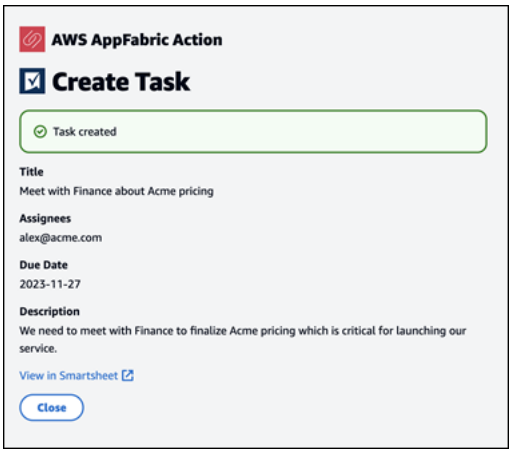
필드에 콘텐츠를 생성하여 작업 생성 시간을 단축할 수 있습니다. 작업 편집을 완료한 후 생성을 선택하여 작업을 생성합니다. Smartsheet 작업의 경우 AppFabric은 새 비공개 Smartsheet 시트를 생성하고 생성된 모든 작업을 채웁니다. 이는 AppFabric에서 생성한 작업을 구조화된 방식으로 한 곳에서 중앙 집중화하는 데 도움이 됩니다.

Smartsheet 작업을 생성하려면 다음 필드가 필요합니다.

- 제목 및 설명 필드입니다.
- 담당자는 유효한 이메일 주소를 제공해야 합니다.



작업이 생성되고 나면 작업이 Smartsheet에서 생성되었다는 확인 메시지가 표시됩니다. 또한 Smartsheet의 작업을 볼 수 있는 링크도 표시됩니다. 이 링크를 사용하면 애플리케이션으로 빠르게 이동하여 생성된 Smartsheet 시트에서 작업을 볼 수 있습니다. 향후의 모든 Smartsheet 작업이 이 시트에 입력됩니다. 시트가 삭제되면 AppFabric은 새 시트를 생성합니다.



IT 및 보안 관리자를 위한 생산성을 위한 AppFabric(미리 보기) 기능에 대한 액세스 관리

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

생산성을 위한 AppFabric 사용자 포털은 생산성을 위한 AppFabric(평가판) 기능과 통합한 모든 SaaS 애플리케이션의 사용자가 공개적으로 액세스할 수 있습니다. 조직 내에서 이러한 생성형 AI 기능에 대한 액세스를 관리하려는 IT 관리자라면 다음 옵션을 고려해 보세요.

- ID 제공업체(IdP) 로그인 제한: ID 제공업체를 통한 로그인 액세스를 차단하여 생성형 AI 기능에 대한 사용자 액세스를 제어할 수 있습니다.
- 특정 애플리케이션에 대한 OAuth 비활성화: OAuth를 비활성화하여 다운스트림 제한을 구현합니다. 이렇게 하면 사용자가 OAuth 인증이 필요한 애플리케이션을 회사의 작업 영역에 연결할 수 없습니다.

생산성을 위한 AppFabric의 최종 사용자 오류 문제 해결

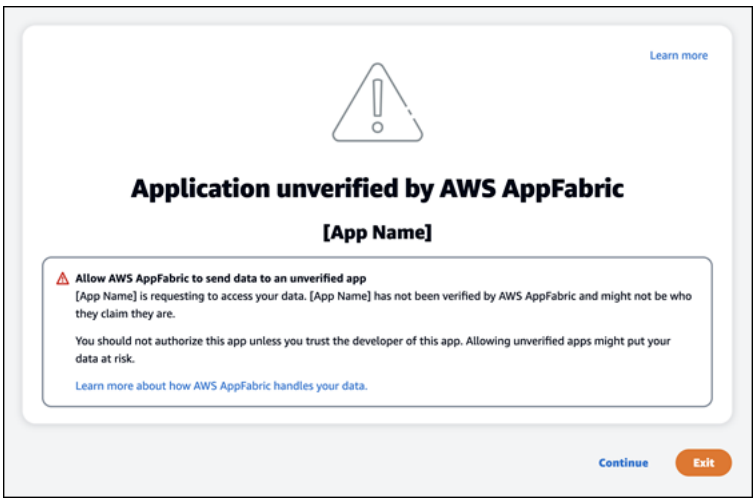
생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

이 섹션에서는 생산성을 위한 AppFabric의 일반적인 오류와 문제 해결에 대해 설명합니다.

확인되지 않은 애플리케이션

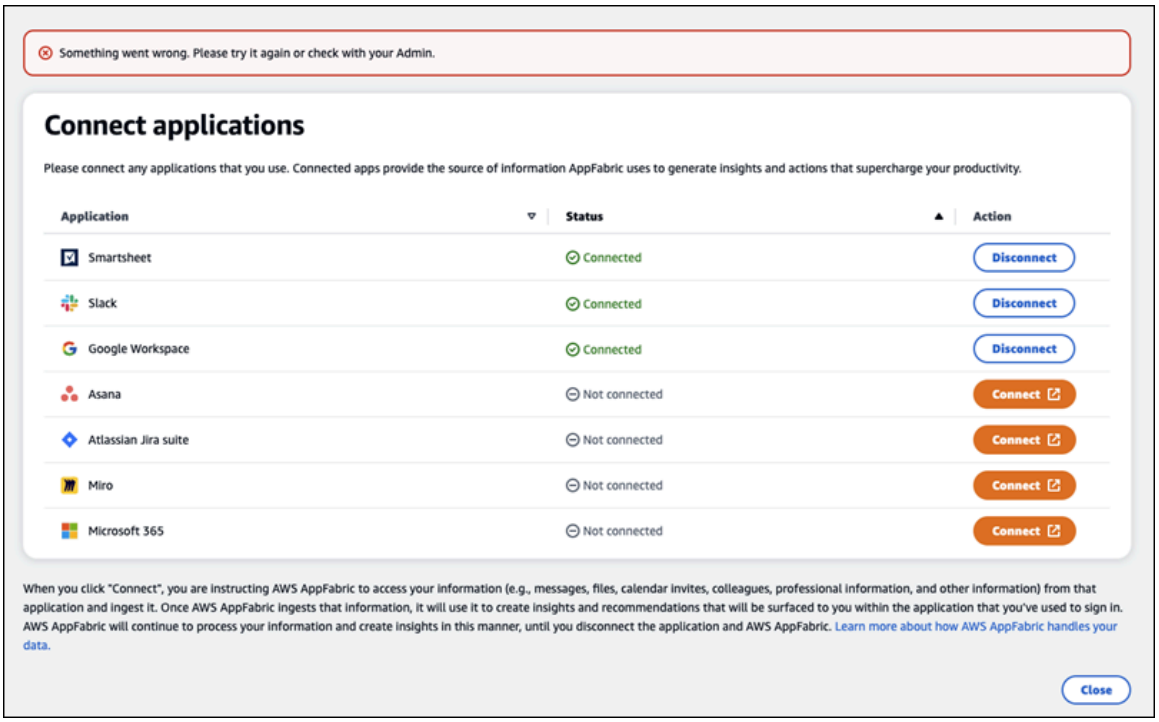
생산성을 위한 AppFabric을 사용하여 앱 경험을 강화하는 애플리케이션은 최종 사용자에게 기능을 출시하기 전에 확인 프로세스를 거칩니다. AppFabric에 로그인하려고 할 때 “확인되지 않음” 배너가 표시되는 경우 이는 애플리케이션이 앱 개발자의 ID 및 애플리케이션 등록 정보의 정확성을 확인하는 AppFabric의 확인 프로세스를 거치지 않았음을 의미합니다. 모든 애플리케이션은 확인되지 않은 상태로 시작하다가 확인 프로세스가 완료되어야만 확인된 것으로 변경됩니다.

확인되지 않은 애플리케이션을 사용할 때는 주의해야 합니다. 앱 개발자가 확실하지 않은 경우 애플리케이션이 확인 상태가 될 때까지 기다렸다가 계속 진행해도 됩니다.



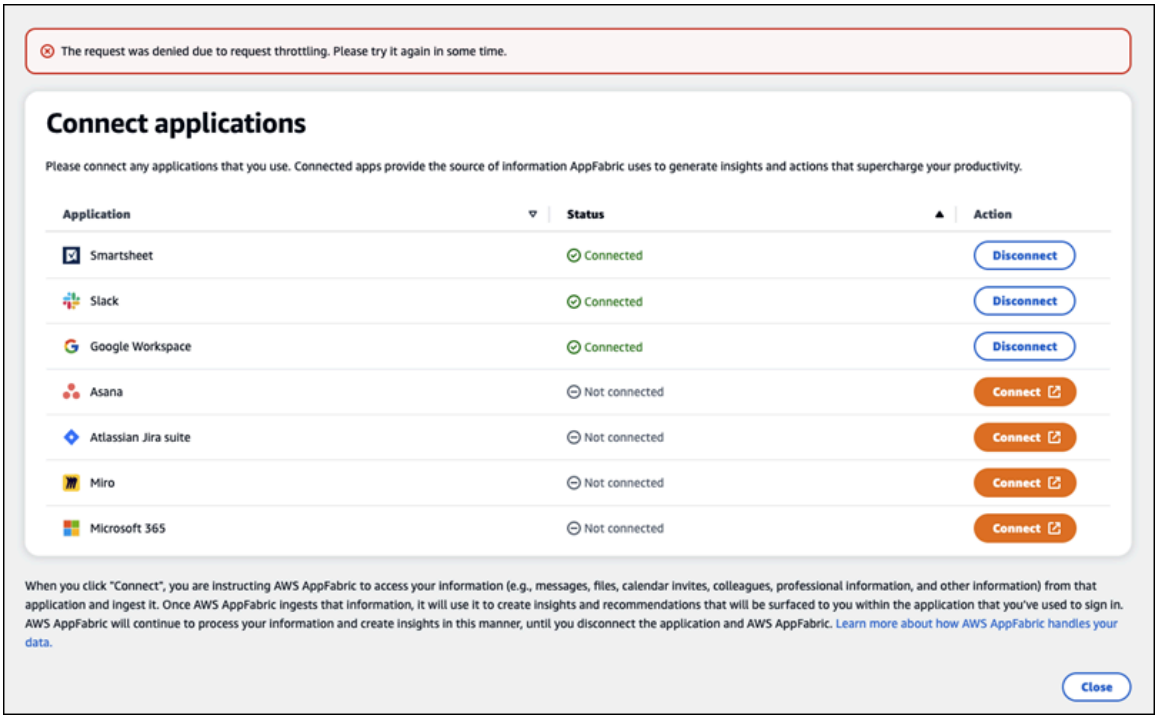
문제가 발생했습니다. 다시 시도하거나 관리자에게 확인해 주세요 (**InternalServerException**).

알 수 없는 오류, 예외 또는 실패로 인해 AppFabric 사용자 포털에서 애플리케이션을 나열하지 못하거나 애플리케이션 연결에 실패했을 때 이 메시지가 표시될 수 있습니다. 나중에 다시 시도해 주세요.



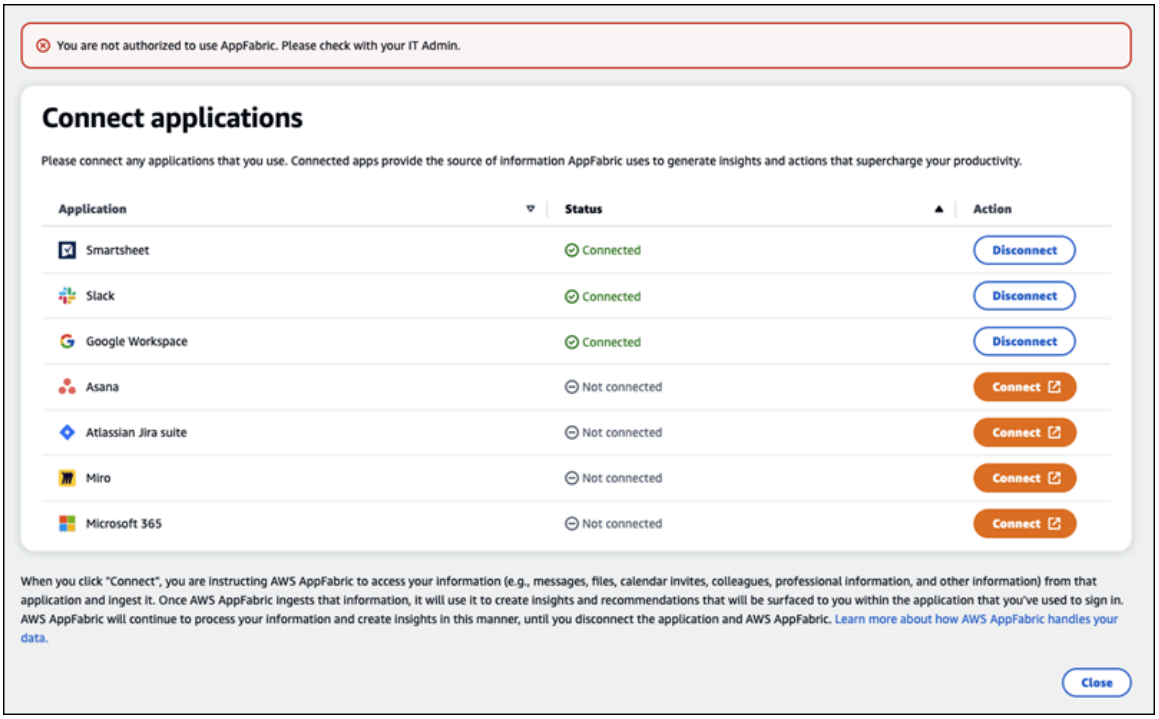
요청 스로틀링으로 인해 요청이 거부되었습니다. 잠시 후 다시 시도해 주세요 (**ThrottlingException**).

제한 문제로 인해 AppFabric 사용자 포털에서 애플리케이션을 나열하지 못하거나 애플리케이션 연결에 실패했을 때 이 메시지가 표시될 수 있습니다. 나중에 다시 시도해 주세요.



AppFabric을 사용할 권한이 없습니다. AppFabric에 다시 로그인하세요 (**`AccessDeniedException`**).

액세스 거부 예외로 인해 AppFabric 사용자 포털에서 애플리케이션을 나열하지 못하거나 애플리케이션 연결에 실패했을 때 이 메시지가 표시될 수 있습니다. AppFabric에 다시 로그인하세요.



생산성을 위한 AppFabric APIs(미리 보기)

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

이 섹션에서는 AWS AppFabric 생산성 기능에 대한 API 작업, 데이터 유형 및 일반적인 오류를 제공합니다.

> **Note**
>
> 다른 모든 AppFabric API에 대해서는 AWS AppFabric API 참조를 참조하세요.

주제

- 생산성을 위한 AppFabric API 작업(미리 보기)
- 생산성을 위한 AppFabric의 API 데이터 형식(미리 보기)
- 생산성을 위한 AppFabric의 일반적인 API 오류(미리 보기)

생산성을 위한 AppFabric API 작업(미리 보기)

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

생산성을 위한 AppFabric 기능에는 다음 작업이 지원됩니다.

다른 모든 AppFabric API 작업에 대해서는 AWS AppFabric API 작업을 참조하세요.

주제

- 인증
- CreateAppClient
- DeleteAppClient
- GetAppClient
- ListActionableInsights
- ListAppClients

- ListMeetingInsights
- PutFeedback
- 토큰
- UpdateAppClient

인증

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

AppClient를 인증합니다.

주제

- 요청 본문

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

파라미터	설명
app_client_id	인증할 AppClient의 ID입니다.
redirect_uri	인증 후 최종 사용자를 리디렉션할 URI입니다.
state	요청과 콜백 사이의 상태를 유지하기 위한 고유 값입니다.

CreateAppClient

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

AppClient를 생성합니다.

주제

- 요청 본문
- 응답 요소

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

파라미터	설명
appName	앱의 이름입니다. 유형: 문자열 길이 제약: 최소 길이는 1. 최대 길이는 255입니다. 필수 항목 여부: 예
clientToken	요청 멱등성을 보장하기 위해 제공하는 고유한 대/소문자 구분 식별자를 지정합니다. 이렇게 하면 실수로 같은 작업을 두 번 수행하지 않고 요청을 안전하게 재시도할 수 있습니다. 나중에 작업을 호출할 때 동일한 값을 전달하려면 다른 모든 파라미터에도 동일한 값을 전달해야 합니다. UUID 유형의 값을 사용하는 것이 좋습니다. 이 값을 제공하지 않으면가 임의의 값을 AWS 생성합니다. 다른 파라미터를 사용하여 `ClientToken` 과 같은 작업을 재시도하면 `IdempotentParameterMismatch` 오류가 발생하며 재시도가 실패합니다. 유형: String 패턴: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 필수 여부: 아니요
customerManagedKeyIdentifier	에서 고객 관리형 키 생성된의 ARN입니다 AWS Key Management Service. 키는 데이터 암호화에 사용합니다.

파라미터	설명
	키가 지정되지 않은 경우 AWS 관리형 키 가 사용됩니다. 리소스에 할당할 태그의 키-값 페어 맵입니다. AWS 소유 키 및 고객 관리형 키에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 고객 키 및 AWS 키를 참조하세요. 유형: 문자열 길이 제약: 최소 길이 1. 최대 길이는 1,011입니다. 패턴: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 필수 항목 여부: 아니요
description	앱에 대한 설명입니다. 유형: 문자열 필수 항목 여부: 예
iconUrl	AppClient의 아이콘 또는 로고 URL입니다. 유형: 문자열 필수 항목 여부: 아니요

파라미터	설명
redirectUrls	인증 후 최종 사용자를 리디렉션할 URI입니다. redirectUrl을 최대 5개 추가할 수 있습니다. 예를 들어 `https://localhost:8080` 입니다. 타입: 문자열 배열 배열 구성원: 최소수는 1개입니다. 최대 항목 수는 5개. 길이 제약: 최소 길이 1. 최대 길이는 2,048. 패턴: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` 필수 여부: 예
starterUserEmails	AppClient가 확인될 때까지 인사이트를 받을 수 있도록 액세스가 허용된 사용자의 스타터 이메일 주소입니다. 유형: 문자열 배열 배열 멤버: 고정된 항목 수는 1개입니다. 길이 제한: 최소 길이는 0. 최대 길이는 320입니다. 패턴: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` 필수 여부: 예
tags	리소스에 할당할 태그의 키-값 페어 맵입니다. 유형: 태그 객체 배열 배열 구성원: 최소수는 0개입니다. 최대수 50개. 필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 HTTP 201 응답을 다시 전송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

파라미터	설명
appClientSummary	AppClient의 요약을 포함합니다. 유형: AppClientSummary 객체

DeleteAppClient

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

애플리케이션 클라이언트를 삭제합니다.

주제

- 요청 본문
- 응답 요소

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

파라미터	설명
appClientIdentifier	요청에 사용할 AppClient의 Amazon 리소스 이름(ARN) 또는 범용 고유 식별자(UUID)입니다. 길이 제약: 최소 길이 1. 최대 길이는 1,011입니다. 패턴: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 필수 여부: 예

응답 요소

액션이 성공하면 해당 서비스는 빈 HTTP 본문과 함께 HTTP 204 응답을 되돌려줍니다.

GetAppClient

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

AppClient에 대한 정보를 반환합니다.

주제

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

파라미터	설명
appClientIdentifier	요청에 사용할 AppClient의 Amazon 리소스 이름(ARN) 또는 범용 고유 식별자(UUID)입니다. 길이 제약: 최소 길이 1. 최대 길이는 1,011입니다. 패턴: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 필수 여부: 예

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

파라미터	설명
appClient	AppClient에 대한 정보가 들어 있습니다. 유형: AppClient 객체

ListActionableInsights

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

가장 중요한 실행 가능 이메일 메시지, 작업 및 기타 업데이트를 나열합니다.

주제

- 요청 본문
- 응답 요소

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

파라미터	설명
nextToken	`nextToken` 이 반환되는 경우 더 많은 결과를 사용할 수 있습니다. `nextToken` 의 값은 각 페이지의 고유한 페이지 매김 토큰입니다. 반환된 토큰을 사용하여 다시 호출하여 다음 페이지를 검색합니다. 다른 모든 인수는 변경하지 않고 유지합니다. 각 페이지 매김 토큰은 24시간 후 만료됩니다. 만료된 페이지 매김 토큰을 사용하면 HTTP 400 InvalidToken 오류가 반환됩니다.

응답 요소

작업이 성공하면 서비스가 HTTP 201 응답을 다시 전송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

파라미터	설명
ActionableInsightsList	제목, 설명, 작업, 생성된 타임스탬프 등 실행 가능한 인사이트를 나열합니다. 자세한 내용은 ActionableInsights 단원을 참조하십시오.
nextToken	nextToken 이 반환되는 경우 더 많은 결과를 사용할 수 있습니다. nextToken 의 값은 각 페이지의 고유한 페이지 매김 토큰입니다. 반환된 토큰을 사용하여 다시 호출하여 다음 페이지를 검색합니다. 다른 모든 인수는 변경하지 않고 유지합니다. 각 페이지 매김 토큰은 24시간 후 만료됩니다. 만료된 페이지 매김 토큰을 사용하면 HTTP 400 InvalidToken 오류가 반환됩니다. 유형: 문자열

ListAppClients

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

모든 AppClient의 목록을 반환합니다.

주제

- 요청 본문
- 응답 요소

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

파라미터	설명
maxResults	호출 한 개당 반환되는 결과의 최대 수입니다. nextToken 을 사용하여 추가 결과 페이지를 얻을 수 있습니다. 이는 상한선일 뿐입니다. 호출당 반환되는 실제 결과 수는 지정된 최대값보다 적을 수 있습니다.

파라미터	설명
	유효 범위: 최소값 1. 최댓값은 100입니다.
nextToken	`nextToken` 이 반환되는 경우 더 많은 결과를 사용할 수 있습니다. `nextToken` 의 값은 각 페이지의 고유한 페이지 매김 토큰입니다. 반환된 토큰을 사용하여 다시 호출하여 다음 페이지를 검색합니다. 다른 모든 인수는 변경하지 않고 유지합니다. 각 페이지 매김 토큰은 24시간 후 만료됩니다. 만료된 페이지 매김 토큰을 사용하면 HTTP 400 InvalidToken 오류가 반환됩니다.

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

파라미터	설명
appClientList	AppClient 결과 목록을 포함합니다. 유형: AppClientSummary 객체의 배열
nextToken	`nextToken` 이 반환되는 경우 더 많은 결과를 사용할 수 있습니다. `nextToken` 의 값은 각 페이지의 고유한 페이지 매김 토큰입니다. 반환된 토큰을 사용하여 다시 호출하여 다음 페이지를 검색합니다. 다른 모든 인수는 변경하지 않고 유지합니다. 각 페이지 매김 토큰은 24시간 후 만료됩니다. 만료된 페이지 매김 토큰을 사용하면 HTTP 400 InvalidToken 오류가 반환됩니다. 유형: 문자열

ListMeetingInsights

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

가장 중요한 실행 가능 캘린더 이벤트를 나열합니다.

주제

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

파라미터	설명
nextToken	`nextToken` 이 반환되는 경우 더 많은 결과를 사용할 수 있습니다. `nextToken` 의 값은 각 페이지의 고유한 페이지 매김 토큰입니다. 반환된 토큰을 사용하여 다시 호출하여 다음 페이지를 검색합니다. 다른 모든 인수는 변경하지 않고 유지합니다. 각 페이지 매김 토큰은 24시간 후 만료됩니다. 만료된 페이지 매김 토큰을 사용하면 HTTP 400 InvalidToken 오류가 반환됩니다.

응답 요소

작업이 성공하면 서비스가 HTTP 201 응답을 다시 전송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

파라미터	설명
MeetingInsightList	실행 가능한 회의 인사이트를 나열합니다. 자세한 내용은 MeetingInsights 단원을 참조하십시오.
nextToken	`nextToken` 이 반환되는 경우 더 많은 결과를 사용할 수 있습니다. `nextToken` 의 값은 각 페이지의 고유한 페이지 매김 토큰입니다. 반환된 토큰을 사용하여 다시 호출하여 다음 페이지를 검색합니다. 다른 모든 인수는 변경하지 않고 유지합니다. 각 페이지 매김 토큰은 24시간 후 만료됩니다. 만료된 페이지 매김 토큰을 사용하면 HTTP 400 InvalidToken 오류가 반환됩니다. 유형: 문자열

PutFeedback

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

사용자가 주어진 인사이트나 작업에 대한 피드백을 제출할 수 있습니다.

주제

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

파라미터	설명
id	피드백을 제출받는 객체의 ID입니다. 이는 InsightId 또는 ActionId 일 수 있습니다.
feedbackFor	피드백을 받는 인사이트 유형입니다. 가능한 값: `ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION`
feedbackRating	피드백 평점: 1~5 평점이 높을수록 좋습니다.

응답 요소

작업이 성공하면 서비스가 비어있는 HTTP 본문과 함께 HTTP 201 응답을 다시 전송합니다.

토큰

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

AppClient가 인증 코드를 액세스 토큰으로 교환할 수 있도록 허용하는 정보를 포함합니다.

주제

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

파라미터	설명
code	인증 엔드포인트에서 받은 인증 코드입니다. 유형: 문자열 길이 제약: 최소 길이는 1. 최대 길이는 2,048. 필수 여부: 아니요
grant_type	토큰의 권한 부여 유형입니다. `authorization_code` 또는 `refresh_token` 여야 합니다. 유형: 문자열 필수 항목 여부: 예
app_client_id	AppClient의 ID입니다. 유형: String 패턴: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 필수 여부: 예
redirect_uri	권한 부여 엔드포인트에 전달된 리디렉션 URI입니다. 유형: 문자열 필수 항목 여부: 아니요
refresh_token	초기 토큰 요청에서 받은 새로 고침 토큰입니다.

파라미터	설명
	유형: 문자열 길이 제약: 최소 길이 1. 최대 길이 4096. 필수 여부: 아니요

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

파라미터	설명
appfabric_user_id	토큰 사용자의 ID입니다. `authorization_code` 권한 부여 유형을 사용하는 요청의 경우에만 반환됩니다. 유형: 문자열
expires_in	토큰큰이 만료될 때까지의 시간(초)입니다. 타입: Long
refresh_token	후속 요청에 사용할 새로 고침 토큰입니다. 유형: 문자열 길이 제약: 최소 길이는 1. 최대 길이는 2,048.
token	액세스 토큰 입니다. 유형: 문자열 길이 제약: 최소 길이는 1. 최대 길이는 2,048.
token_type	토큰 유형입니다. 유형: 문자열

UpdateAppClient

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

AppClient를 업데이트합니다.

주제

요청 본문

요청은 JSON 형식으로 다음 데이터를 받습니다.

파라미터	설명
appClientIdentifier	요청에 사용할 AppClient의 Amazon 리소스 이름(ARN) 또는 범용 고유 식별자(UUID)입니다. 길이 제약: 최소 길이 1. 최대 길이는 1,011입니다. 패턴: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 필수 여부: 예
redirectUrls	인증 후 최종 사용자를 리디렉션할 URI입니다. redirectUrl을 최대 5개 추가할 수 있습니다. 예를 들어 `https://localhost:8080` 입니다. 타입: 문자열 배열 배열 구성원: 최소수는 1개입니다. 최대 항목 수는 5개. 길이 제약: 최소 길이 1. 최대 길이는 2,048. 패턴: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

응답 요소

작업이 성공하면 서비스가 HTTP 200 응답을 반송합니다.

다음 데이터는 서비스에 의해 JSON 형식으로 반환됩니다.

파라미터	설명
appClient	AppClient에 대한 정보가 들어 있습니다. 유형: AppClient 객체

생산성을 위한 AppFabric의 API 데이터 형식(미리 보기)

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

AppFabric API에는 다양한 작업에 사용되는 여러 데이터 유형이 포함되어 있습니다. 이 섹션에서는 생산성을 위한 AppFabric 기능의 데이터 유형에 대해 자세히 설명합니다.

다른 모든 AppFabric API 데이터 유형에 대해서는 AWS AppFabric API 데이터 유형을 참조하세요.

> **Important**
>
> 데이터 유형 구조에서 각 요소의 순서는 보장되지 않습니다. 애플리케이션은 특정 순서를 가정해서는 안 됩니다.

주제

- ActionableInsights
- AppClient
- AppClientSummary
- MeetingInsights
- VerificationDetails

ActionableInsights

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

앱 포트폴리오의 이메일, 캘린더 초대, 메시지 및 작업을 기반으로 사용자에게 필요하고 중요하며 적합한 작업을 요약하여 제공합니다. 사용자는 애플리케이션 전반에서 하루의 방향을 가장 잘 잡을 수 있도록 돕는 사전 예방형 인사이트를 확인할 수 있습니다. 이 인사이트는 사용자가 인사이트를 생성한 개별 앱 및 아티팩트에 대한 참조(예: 포함된 링크)와 함께 인사이트 요약에 관심을 가져야 하는 이유에 대한 근거가 됩니다.

파라미터	설명
insightId	생성된 인사이트의 고유 ID입니다.
insightContent	이렇게 하면 인사이트 요약과 인사이트 생성에 사용된 아티팩트에 대한 포함된 링크가 반환됩니다. 이는 포함된 링크(<a> 태그)가 포함된 HTML 콘텐츠입니다.
insightTitle	생성된 인사이트의 제목입니다.
createdAt	인사이트가 생성된 시점입니다.
actions	생성된 인사이트에 대한 권장 작업 목록입니다. 작업 객체는 다음 파라미터를 포함합니다. • `actionId` - 생성된 작업의 고유 ID입니다. • `actionIconUrl` - 작업 실행을 제안하는 앱의 아이콘 URL입니다. • `actionTitle` - 생성된 작업의 제목입니다. • `actionUrl` - 최종 사용자가 AppFabric의 사용자 포털에서 작업을 보고 실행할 수 있는 고유 URL입니다. 작업을 실행할 때 ISV 앱은 이 URL을 사용하여 사용자를 AppFabric 사용자 포털(팝업 화면)로 리디렉션합니다.

파라미터	설명
	• `actionExecutionStatus` - 작업의 상태를 나타내는 열거형입니다. 가능한 값은 `EXECUTED | NOT_EXECUTED` 입니다.

AppClient

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

AppClient에 대한 정보가 들어 있습니다.

파라미터	설명
appName	애플리케이션의 이름입니다. 유형: 문자열 필수 항목 여부: 예
arn	AppClient의 Amazon 리소스 이름(ARN)입니다. 유형: 문자열 길이 제약: 최소 길이 1. 최대 길이는 1,011입니다. 패턴: `arn:.+` 필수 여부: 예
description	애플리케이션에 대한 설명입니다. 유형: 문자열 필수 항목 여부: 예
iconUrl	AppClient의 아이콘 또는 로고 URL입니다.

파라미터	설명
	유형: 문자열 필수 항목 여부: 아니요
redirectUrls	AppClient에 허용된 리디렉션 URL입니다. 타입: 문자열 배열 배열 구성원: 최소수는 1개입니다. 최대 항목 수는 5개. 길이 제약: 최소 길이 1. 최대 길이는 2,048. 패턴: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` 필수 여부: 예
starterUserEmails	AppClient가 확인될 때까지 인사이트를 받을 수 있도록 액세스가 허용된 사용자의 스타터 이메일 주소입니다. 유형: 문자열 배열 배열 멤버: 고정된 항목 수는 1개입니다. 길이 제한: 최소 길이는 0. 최대 길이는 320입니다. 패턴: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` 필수 여부: 예
verificationDetails	AppClient 확인의 상태 및 이유를 포함합니다. 유형: VerificationDetails 객체 필수 항목 여부: 예

파라미터	설명
customerManagedKeyArn	AppClient에 고객 관리형 키 AWS Key Management Service 대해에서 생성된의 Amazon 리소스 이름(ARN)입니다. 유형: 문자열 길이 제약: 최소 길이 1. 최대 길이는 1,011입니다. 패턴: `arn:.+` 필수 여부: 아니요
appClientId	AppClient의 ID입니다. 앱 클라이언트의 인증 흐름에 사용됩니다. 유형: String 패턴: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 필수 여부: 아니요

AppClientSummary

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

AppClient에 대한 정보가 들어 있습니다.

파라미터	설명
arn	AppClient의 Amazon 리소스 이름(ARN)입니다. 유형: 문자열 길이 제약: 최소 길이 1. 최대 길이는 1,011입니다. 패턴: `arn:.+` 필수 여부: 예

파라미터	설명
verificationStatus	AppClient 확인 상태입니다. 타입: 문자열 유효 값: `pending_verification | verified | rejected` 필수 사항 여부: 예
appClientId	AppClient의 ID입니다. 앱 클라이언트의 인증 흐름에 사용됩니다. 유형: String 패턴: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 필수 여부: 아니요

MeetingInsights

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

회의 목적, 관련 앱 간 아티팩트, 작업 활동, 이메일에서의 활동, 메시지에서의 활동, 캘린더 이벤트에서의 활동과 함께 상위 3개 미팅에 대한 요약이 포함되어 있습니다.

파라미터	설명
insightId	생성된 인사이트의 고유 ID입니다.
insightContent	세부 정보를 문자열 형식으로 강조 표시하는 인사이트에 대한 설명입니다. 즉, 이 인사이트가 왜 중요한지에 대한 것입니다.
insightTitle	생성된 인사이트의 제목입니다.
createdAt	인사이트가 생성된 시점입니다.

파라미터	설명
calendarEvent	사용자가 집중해야 하는 중요한 캘린더 이벤트 또는 회의입니다. 캘린더 이벤트 객체: • `startTime` - 이벤트의 시작 시간입니다. • `endTime` - 이벤트의 종료 시간입니다. • `eventUrl` - ISV 앱의 캘린더 이벤트 URL입니다.
resources	인사이트 생성과 관련된 다른 리소스가 포함된 목록입니다. 리소스 객체: • `appName` - 리소스가 속한 앱 이름입니다. • `resourceTitle` - 리소스 제목입니다. • `resourceType` - 리소스의 유형입니다. 가능한 값은 `EMAIL | EVENT | MESSAGE | TASK`입니다. • `resourceUrl` - 앱의 리소스 URL입니다. • `appIconUrl` - 리소스가 속한 앱의 이미지 URL입니다.
nextToken	다음 인사이트 세트를 가져오기 위한 페이지 매김 토큰입니다. 이 필드는 선택 사항 필드이며, null을 반환하면 로드할 인사이트가 더 이상 없음을 의미합니다.

VerificationDetails

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

AppClient 확인의 상태 및 이유를 포함합니다.

파라미터	설명
verificationStatus	AppClient 확인 상태입니다.

파라미터	설명
	타입: 문자열 유효 값: `pending_verification | verified | rejected` 필수 사항 여부: 예
statusReason	AppClient 확인 상태 이유입니다. 유형: 문자열 길이 제약: 최소 길이 1. 최대 길이 1024. 필수 여부: 아니요

생산성을 위한 AppFabric의 일반적인 API 오류(미리 보기)

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

이 섹션에서는 AWS AppFabric 생산성 기능의 API 작업에 공통적인 오류를 나열합니다.

다른 모든 AppFabric 일반 API 오류에 대해서는 생산성을 위한 AppClients 문제 해결 AppFabric 및 AWS AppFabric API 참조의 AWS AppFabric API 일반 오류를 참조하세요.

예외 이름	설명
TokenException	토큰 요청이 유효하지 않습니다. HTTP 상태 코드: 400

AppFabric의 데이터 처리

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

AppFabric은 사용자 콘텐츠를 AppFabric에서 관리하는 Amazon S3 버킷에 개별적으로 저장하는 단계를 거치며, 이를 통해 사용자별 인사이트를 확보할 수 있습니다. 저장 데이터 암호화 및 전송 중 암호화 등 합리적인 보호 장치를 사용하여 콘텐츠를 보호합니다. 고객 콘텐츠를 수집 후 30일 이내에 자동으로 삭제되도록 시스템을 구성했습니다. AppFabric은 사용자가 더 이상 액세스할 수 없는 데이터 아티팩트를 사용하여 인사이트를 생성하지 않습니다. 예를 들어 사용자가 데이터 소스(앱)의 연결을 끊으면 AppFabric은 해당 앱에서 데이터 수집을 중단하고 인사이트 생성에 연결이 끊긴 앱에서 남아 있는 아티팩트를 사용하지 않습니다. AppFabric의 시스템은 30일 이내에 이러한 데이터를 삭제하도록 구성되어 있습니다.

AppFabric은 인사이트를 생성하는 데 사용하는 기본 대규모 언어 모델을 교육하거나 개선하는 데 사용자 콘텐츠를 사용하지 않습니다. AppFabric의 생성형 AI 기능에 대한 자세한 내용은 Amazon Bedrock FAQ를 참조하세요.

저장 시 암호화

AWS AppFabric은 AppFabric이 디스크에 보관될 때 사용자와 관련된 모든 데이터를 투명하게 암호화하고 데이터에 액세스할 때 복호화하는 서버 측 암호화 기능인 저장 데이터 암호화를 지원합니다.

전송 중 암호화

AppFabric은 TLS 1.2를 사용하여 전송 중인 모든 콘텐츠를 보호하고 AWS 서명 버전 4가 있는 AWS 서비스에 대한 API 요청에 서명합니다.

AppFabric의 용어 및 개념

이 주제에서는 시작하는 데 도움이 되는 AWS AppFabric의 주요 용어 및 개념에 대해 설명합니다.

앱 번들

AppFabric 앱 번들은 모든 AppFabric 앱 인증 및 통합을 저장합니다(다음 수집 정의 참조). 당 하나의 앱 번들을 생성할 수 AWS 계정 있습니다 AWS 리전.

AppClient(앱 클라이언트 및 애플리케이션 클라이언트이기도 함)

데이터 수신자 앱을 위한 OAuth AppClient. AppFabric 데이터에 액세스하려면 각 데이터 수신자 앱이 AppClient를 등록해야 합니다. 개발자 사용자는 AppClient를 등록하려면 AWS 계정이 필요합니다. 각 AWS 계정은 AppClient를 하나만 등록할 수 있습니다. AppFabric은 AppClient를 기반으로 액세스 토큰을 판매합니다. AppClient는 이 AppClient를 통해 AppFabric 데이터에 액세스할 데이터 수신자 앱에 대한 정보를 포함합니다.

API 인증

앱 인증을 통해 AppFabric이 애플리케이션에 연결하고 상호 작용할 수 있는 권한을 부여합니다. 이를 통해 OAuth(개방형 인증 - 애플리케이션에 액세스 권한을 부여하는 액세스 위임을 위한 개방형 표준) 또는 PAT(개인 액세스 토큰) 보안 인증을 사용하여 애플리케이션에서 감사 로그를 수집할 수 있습니다. 앱 번들당 여러 앱 인증(최대 50개)을 설정할 수 있습니다. 이를 통해 AppFabric은 애플리케이션의 각 테넌트에 대해 필요에 따라 앱 인증 생성 단계를 반복하여 애플리케이션의 여러 테넌트로부터 감사 로그를 수집할 수 있습니다. 공유된 자격 증명은 AWS 소유 키 또는 AWS Key Management Service (AWS KMS)의 고객 관리형 키로 암호화되며 AppFabric에 저장됩니다.

수집

AppFabric 수집은 앱 인증을 사용하여 애플리케이션의 공개 API를 통해 애플리케이션에서 감사 로그를 가져옵니다. 그런 다음 감사 로그를 하나 이상(최대 5개)의 대상으로 전달합니다.

클라이언트 ID

OAuth 흐름을 사용하는 애플리케이션에 연결하기 위한 앱 인증을 생성할 때 AppFabric은 클라이언트 ID와 클라이언트 암호를 요청할 수 있습니다. 클라이언트 ID와 클라이언트 암호는 애플리케이션의 인증 앱에서 찾을 수 있습니다. 특정 인증 앱에서 클라이언트 ID를 찾을 수 있는 위치에 대한 지침은 지원되는 애플리케이션을 참조하십시오. 공유되는 클라이언트 ID 및 클라이언트 보안 암호는 AWS 소유 키 또는 고객 관리형 AWS KMS 키로 암호화되어 AppFabric에 저장됩니다.

클라이언트 보안 암호(client secret)

OAuth 흐름을 사용하는 애플리케이션에 연결하기 위한 앱 인증을 생성할 때 AppFabric은 클라이언트 ID와 클라이언트 암호를 요청할 수 있습니다. 클라이언트 ID와 클라이언트 암호는 애플리케이션의 인증 앱에서 찾을 수 있습니다. 특정 인증 앱에서 클라이언트 ID를 찾을 수 있는 위치에 대한 지침은 지원되는 애플리케이션을 참조하십시오. 공유되는 클라이언트 ID 및 클라이언트 보안 암호는 AWS 소유 키 또는 고객 관리형 AWS KMS 키로 암호화되어 AppFabric에 저장됩니다.

수집 대상

수집 대상은 수집에서 가져온 감사 로그를 저장해야 하는 위치를 정의합니다. 각 수집은 Amazon Simple Storage Service(Amazon S3) 버킷 또는의 Amazon Data Firehose인 하나 이상의 대상(최대 5개)에 감사 로그를 전송할 수 있습니다 AWS 계정. 각 대상에 대해 로그를 원시 형식으로 할지 아니면 개방형 사이버 보안 스키마 프레임워크(OCSF) 스키마로 정규화할지 정의할 수 있습니다. OCSF 스키마를 선택하면 로그 형식(JSON 또는 Apache Parquet)을 정의할 수 있습니다. Amazon S3를 대상으로 선택한 경우에만 Apache Parquet 형식을 사용할 수 있습니다.

데이터 수신자 앱

AppFabric에서 생성된 인사이트를 얻기 위해 AppFabric을 호출하는 앱입니다.

OAuth

OAuth는 웹, 모바일 및 데스크톱 애플리케이션에서 간단하고 표준적인 방법으로 보안 인증을 수행할 수 있는 개방형 프로토콜입니다. AppFabric은 OAuth를 사용하여 일부 앱 인증을 생성합니다.

개방형 사이버 보안 스키마 프레임워크(OCSF)

개방형 사이버 보안 스키마 프레임워크(OCSF) 는 공급업체에 구애받지 않는 핵심 보안 스키마와 함께 스키마 개발을 위한 확장 가능한 프레임워크를 제공하는 오픈 소스 프로젝트입니다. 공급업체 및 기타 데이터 생산자는 특정 도메인에 맞게 스키마를 채택하고 확장할 수 있습니다. 목표는 기존 보안 표준 및 프로세스를 보완하는 동시에 모든 환경, 애플리케이션 또는 솔루션에 채택되는 개방형 표준을 제공하는 것입니다. AppFabric은 이 스키마를 확장하여 AppFabric에서 지원하는 모든 SaaS 앱 감사 로그를 정규화하는 서비스형 소프트웨어(SaaS) 중심 이벤트 구조를 만들었습니다. 자세한 내용은 Open Cybersecurity Schema Framework for AWS AppFabric을 참조하십시오.

개인용 액세스 토큰(PAT)

개인 액세스 토큰(PAT)은 일반적인 암호 대신 컴퓨터 시스템에 액세스하는 데 사용할 수 있는 문자열입니다. PAT 흐름을 사용하는 애플리케이션에 연결하기 위해 앱 인증을 생성할 때 AppFabric에서 PAT를 요청할 수 있습니다. PAT는 애플리케이션의 인증 앱에서 찾을 수 있습니다. 특정 인증 앱에서

PAT를 찾을 수 있는 위치에 대한 지침은 지원되는 애플리케이션을 참조하십시오. 공유되는 서비스 계정 토큰은 AWS 소유 키 또는 고객 관리형 키 AWS KMS 키로 암호화되어 AppFabric에 저장됩니다.

서비스 계정 토큰

애플리케이션과 연결하기 위해 AppFabric 앱 인증을 생성하는 경우 일부 애플리케이션에서는 애플리케이션 인증을 위해 서비스 계정을 생성해야 합니다. AppFabric은 앱 인증 프로세스의 일부로 서비스 계정 토큰을 요청할 수 있습니다. 특정 인증 앱에서 서비스 계정 토큰을 찾을 수 있는 위치에 대한 지침은 지원되는 애플리케이션을 참조하십시오. 공유되는 서비스 계정 토큰은 AWS 소유 키 또는 고객 관리형 키 AWS KMS 키로 암호화되어 AppFabric에 저장됩니다.

테넌트 ID

앱 인증을 생성할 때 AppFabric은 앱의 테넌트 ID 및 테넌트 이름을 요청할 수 있습니다. 테넌트 ID는 애플리케이션 테넌트의 고유 식별자입니다. 애플리케이션마다 테넌트에 대한 용어가 다를 수 있습니다 (예: Slack에서는 워크스페이스 ID, Asana에서는 도메인 ID). 특정 애플리케이션에서 테넌트 ID를 찾을 수 있는 위치에 대한 지침은 지원되는 애플리케이션을 참조하십시오.

테넌트 이름

앱 인증을 생성할 때 AppFabric은 앱의 테넌트 ID 및 테넌트 이름을 요청할 수 있습니다. 테넌트 이름은 앱 번들 내에서 사용하기 위해 테넌트 ID에 부여하는 고유한 이름입니다. 이 값은 앱 인증 및 모든 관련 수집에 레이블을 지정하는 데 사용됩니다.

인 AWS AppFabric 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 AWS 서비스 에서 실행되는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. AWS AppFabric에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 .
- 클라우드의 보안 - 사용자의 책임은 AWS 서비스 사용하는에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AppFabric 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 AppFabric을 구성하는 방법을 보여줍니다. 또한 AppFabric 리소스를 모니터링하고 보호하는 데 도움이 AWS 서비스 되는 다른를 사용하는 방법을 알아봅니다.

주제

- AWS AppFabric의 데이터 보호
- AWS AppFabric의 자격 증명 및 액세스 관리
- AWS AppFabric에 대한 규정 준수 검증
- AWS AppFabric의 보안 모범 사례
- AWS AppFabric의 복원력
- 인 AWS AppFabric의 인프라 보안
- AWS AppFabric의 구성 및 취약성 분석

AWS AppFabric의 데이터 보호

AWS 공동 책임 모델 AWS AppFabric의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 이 인프라에 호스

팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 일반 데이터 보호 규정(GDPR) 센터를 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 AppFabric 또는 기타 AWS 서비스 에서 콘솔 AWS CLI, API 또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

> **Note**
>
> AppFabric for security에 적용하는 데이터 보호에 대한 자세한 내용은 AppFabric의 데이터 처리 섹션을 참조하세요.

저장 시 암호화

AWS AppFabric은 AppFabric이 디스크에 유지될 때 앱 번들과 관련된 모든 데이터를 투명하게 암호화하고 데이터에 액세스할 때 복호화하는 서버 측 암호화 기능인 저장 데이터 암호화를 지원합니다. 기본적으로 AppFabric은 AWS 소유 키 from AWS Key Management Service ()를 사용하여 데이터를 암호화합니다AWS KMS. 자체 고객 관리형 키를 사용하여 데이터를 암호화하도록 선택할 수도 있습니다AWS KMS.

앱 번들을 삭제하면 모든 메타데이터가 영구적으로 삭제됩니다.

전송 중 암호화

앱 번들을 구성할 때 AWS 소유 키 또는 고객 관리형 키를 선택할 수 있습니다. 감사 로그 수집을 위한 데이터를 수집하고 정규화할 때 AppFabric은 중간 Amazon Simple Storage Service(S3) 버킷에 데이터를 임시로 저장하고 이 키를 사용하여 암호화합니다. 이 중간 버킷은 버킷 수명 주기 정책을 사용하여 30일 후에 삭제됩니다.

AppFabric은 TLS 1.2를 사용하여 전송 중인 모든 데이터를 보호하고 AWS Signature V4를 사용하여에 대한 AWS 서비스 API 요청에 서명합니다.

키 관리

AppFabric은 AWS 소유 키 또는 고객 관리형 키를 사용한 데이터 암호화를 지원합니다. 고객 관리형 키를 사용하면 암호화된 데이터를 완전히 제어할 수 있으므로 고객 관리형 키를 사용하는 것이 좋습니다. 고객 관리형 키를 선택하면 AppFabric은 고객 관리형 키에 대한 액세스 권한을 부여하는 리소스 정책을 고객 관리형 키에 연결합니다.

고객 관리형 키

고객 관리형 키를 생성하려면 AWS KMS 개발자 안내서의 대칭 암호화 KMS 키 생성 단계를 따르십시오.

키 정책

키 정책은 고객 관리형 키에 대한 액세스를 제어합니다. 모든 고객 관리형 키에는 키를 사용할 수 있는 사람과 키를 사용하는 방법을 결정하는 문장이 포함된 정확히 하나의 키 정책이 있어야 합니다. 고객 관리형 키를 만들 때 키 정책을 지정할 수 있습니다. 키 정책을 생성하는 방법에 대한 자세한 내용은 AWS KMS 개발자 안내서의 키 정책 생성을 참조하십시오.

AppFabric에서 고객 관리형 키를 사용하려면 AppFabric 리소스를 생성하는 AWS Identity and Access Management (IAM) 사용자 또는 역할에 고객 관리형 키를 사용할 수 있는 권한이 있어야 합니다.

AppFabric에서만 사용하는 키를 만들고 AppFabric 사용자를 키 사용자로 추가하는 것이 좋습니다. 이 접근 방식은 데이터에 대한 액세스 범위를 제한합니다. 사용자에게 필요한 권한은 다음과 같습니다.

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Decrypt`

AWS KMS 콘솔은 적절한 키 정책을 사용하여 키를 생성하는 방법을 안내합니다. 키 정책에 대한 자세한 내용은 AWS KMS 개발자 안내서의 AWS KMS에서의 키 정책을 참조하십시오.

다음은 아래 내용을 허용하는 키 정책의 예입니다.

- 키의 AWS 계정 루트 사용자 전체 제어입니다.
- 사용자는 AppFabric을 사용하여 AppFabric과 함께 고객 관리형 키를 사용할 수 있습니다.
- `us-east-1`의 앱 번들 설정에 대한 키 정책입니다.

AppFabric이에서 권한 부여를 사용하는 방법 AWS KMS

AppFabric에서 고객 관리형 키를 사용하려면 권한 부여가 필요합니다. 자세한 내용은 AWS KMS 개발자 가이드에서 AWS KMS에서의 권한 부여을 참조하십시오.

앱 번들을 생성할 때 AppFabric은 `CreateGrant` 요청을 전송하여 사용자를 대신하여 권한을 생성합니다 AWS KMS. 의 권한 부여 AWS KMS 는 AppFabric에 고객 계정의 AWS KMS 키에 대한 액세스 권한을 부여하는 데 사용됩니다. AppFabric는 다음 내부 작업에 대해 고객 관리형 키를 사용할 수 있는 권한 부여가 필요합니다.

- AWS KMS 에 `GenerateDataKey` 요청을 보내 고객 관리형 키로 암호화된 데이터 키를 생성합니다.
- 데이터를 AWS KMS 암호화하고 전송 중인 애플리케이션 액세스 토큰을 복호화하는 데 사용할 수 있도록 암호화된 데이터 키를 복호화하기 위한 `Decrypt` 요청을에 보냅니다.
- AWS KMS 에 `Encrypt` 요청을 보내 전송 중인 애플리케이션 액세스 토큰을 암호화합니다.

다음은 권한 부여의 예입니다.

```
{
```

```
  "KeyId": "arn:aws:kms:us-east-1:111122223333:key/ff000af-00eb-00ce-0e00-
ea000fb0fba0SAMPLE",
  "GrantId": "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
  "Name": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "CreationDate": "2022-10-11T20:35:39+00:00",
  "GranteePrincipal": "appfabric.us-east-1.amazonaws.com",
  "RetiringPrincipal": "appfabric.us-east-1.amazonaws.com",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "Operations": [
    "Decrypt",
    "Encrypt",
    "GenerateDataKey"
  ],
  "Constraints": {
    "EncryptionContextSubset": {
      "appBundleArn": "arn:aws:fabric:us-east-1:111122223333:appbundle/
ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE"
    }
  }
},
```

앱 번들을 삭제하면 AppFabric은 고객 관리형 키에 대해 발행된 권한 부여를 사용 중지합니다.

AppFabric에 대한 암호화 키 모니터링

AppFabric에서 AWS KMS 고객 관리형 키를 사용하는 경우 AWS CloudTrail 로그를 사용하여 AppFabric이 보내는 요청을 추적할 수 있습니다 AWS KMS.

다음은 AppFabric이 고객 관리형 키에 `CreateGrant`을 사용할 때 기록되는 CloudTrail 이벤트의 예입니다.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser",
        "arn": "arn:aws:sts::111122223333:assumed-role/AssumedRole/SampleUser",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
```

```
                "arn": "arn:aws:iam::111122223333:role/AssumedRole",
                "accountId": "111122223333",
                "userName": "SampleUser"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-04-28T14:01:33Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-04-28T14:05:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "appfabric.amazonaws.com",
    "userAgent": "appfabric.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "appfabric.us-east-1.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {
                "appBundleArn": "arn:aws:appfabric:us-east-1:111122223333:appbundle/
ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE"
            }
        },
        "keyId": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLEID",
        "retiringPrincipal": "appfabric.us-east-1.amazonaws.com",
        "operations": [
            "Encrypt",
            "Decrypt",
            "GenerateDataKey"
        ]
    },
    "responseElements": {
        "grantId": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
        "keyId": "arn:aws:kms:us-east-1:111122223333:key/KEY_ID"
    },
    "additionalEventData": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
```

```
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:111122223333:key/key_ID"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_256_GCM_SHA384",
        "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
    }
}
```


AWS AppFabric의 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 AppFabric 리소스를 사용하기 위해 인증되고(로그인) 및 권한이 부여될(권한 있음) 수 있는 사람을 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조AWS AppFabric 자격 증명 및 액세스 문제 해결)
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(AWS AppFabric과 IAM의 작동 방식 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(AWS AppFabric의 자격 증명 기반 정책 예제 참조)

ID를 통한 인증

인증은 자격 증명 AWS 으로에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자가 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 What is IAM Identity Center?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여에 액세스하도록 인간 사용자에게 요구하기를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 또는 API 작업을 호출하여 역할을 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.
- 리소스 제어 정책(RCP) – 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

AWS AppFabric과 IAM의 작동 방식

IAM을 사용하여 AppFabric에 대한 액세스를 관리하기 전에 AppFabric에서 사용할 수 있는 IAM 기능에 대해 알아보십시오.

AWS AppFabric과 함께 사용할 수 있는 IAM 기능

IAM 특성	AppFabric 지원
자격 증명 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	아니요
ACL	아니요
ABAC(정책의 태그)	예
임시 보안 인증	아니요
엔터티 권한	예
서비스 역할	아니요
서비스 연결 역할	예

AppFabric 및 기타에서 대부분의 IAM 기능을 AWS 서비스 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

AppFabric에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

AppFabric의 자격 증명 기반 정책 예제

AppFabric 자격 증명 기반 정책의 예를 보려면 AWS AppFabric의 자격 증명 기반 정책 예제을 참조하십시오.

AppFabric 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM에서 교차 계정 리소스 액세스를 참조하세요.

AppFabric의 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

AppFabric 작업 목록을 보려면 서비스 승인 참조의AWS AppFabric에서 정의한 작업을 참조하세요.

AppFabric의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
appfabric
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

```
"Action": [
      "appfabric:action1",
      "appfabric:action2"
```

```
        ]
```

와일드카드 문자(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `List`라는 단어로 시작하는 모든 작업을 지정하려면 다음 작업을 포함합니다.

```
"Action": "appfabric:List*"
```

AppFabric 자격 증명 기반 정책의 예를 보려면 AWS AppFabric의 자격 증명 기반 정책 예제을 참조하십시오.

AppFabric의 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

AppFabric 리소스 유형 및 해당 ARNs 목록을 보려면 서비스 승인 참조의 AWS AppFabric에서 정의한 리소스 유형을 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면AWS AppFabric에서 정의한 작업을 참조하세요.

AppFabric 자격 증명 기반 정책의 예를 보려면 AWS AppFabric의 자격 증명 기반 정책 예제을 참조하십시오.

AppFabric의 정책 조건 키

서비스별 정책 조건 키 지원: 아니요

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수

있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

AppFabric 조건 키 목록을 보려면 서비스 승인 참조의 AWS AppFabric에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면AWS AppFabric에서 정의한 작업을 참조하세요.

AppFabric 자격 증명 기반 정책의 예를 보려면 AWS AppFabric의 자격 증명 기반 정책 예제을 참조하십시오.

AppFabric의 ACL

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

AppFabric에서의 ABAC

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*또는 `aws:TagKeys`조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

AppFabric에서 임시 보안 인증 사용

임시 자격 증명 지원: 아니요

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션 또는 전환 역할을 사용할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이

AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 임시 보안 자격 증명 및 IAM으로 작업하는 AWS 서비스 섹션을 참조하세요.

AppFabric의 서비스 간 보안 주체 권한

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은를 호출하는 보안 주체의 권한을 다운스트림 서비스에 대한 요청 AWS 서비스 과 AWS 서비스함께 사용합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AppFabric의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스 AWS에 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 AppFabric 기능이 중단될 수 있습니다. AppFabric에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집하십시오.

AppFabric의 서비스 연결 역할

서비스 연결 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 태스크를 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

AppFabric 서비스 연결 역할을 생성 또는 관리하는 방법에 대한 자세한 내용은 AppFabric에 서비스 연결 역할 사용을 참조하십시오.요.

AWS AppFabric의 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 AppFabric 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARNs 형식을 포함하여 AppFabric에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 AWS AppFabric에 사용되는 작업, 리소스 및 조건 키를 참조하세요.

목차

정책 모범 사례

ID 기반 정책은 사용자 계정에서 AppFabric 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수

있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.

- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

AppFabric 콘솔 사용

`AWSAppFabricReadOnlyAccess` AWS 관리형 정책을 IAM 자격 증명에 연결하여의 AppFabric 콘솔을 포함하여 AppFabric 서비스에 대한 읽기 전용 권한을 부여합니다 AWS Management Console. 또는 `AWSAppFabricFullAccess` AWS 관리형 정책을 IAM 자격 증명에 연결하여 AppFabric 서비스에 대한 전체 관리 권한을 부여할 수 있습니다. 자세한 내용은 AWS AWS AppFabric에 대한 관리형 정책 단원을 참조하십시오.

AppFabric for security IAM 정책 예제

다음 정책 예제는 AppFabric for security 기능에 적용됩니다.

앱 번들에 대한 액세스 허용

다음 정책 예제는 AppFabric 서비스의 앱 번들에 대한 액세스 권한을 부여합니다.

JSON

```
{
    "Version":"2012-10-17",

    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ]
}
```

앱 번들 액세스 제한

다음 정책 예제는 AppFabric 서비스의 앱 번들에 대한 액세스를 제한합니다.

JSON

```
{
    "Version":"2012-10-17",

    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ]
```

```
}
```

수집 삭제 또는 중지를 제한합니다.

다음 정책 예제는 AppFabric 서비스에서의 수집 삭제 또는 중지를 제한합니다.

JSON

```
{
    "Version":"2012-10-17",

    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StopIngestion",
                "appfabric:DeleteIngestion",
                "appfabric:DeleteIngestionDestination"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ]
}
```

생산성을 위한 AppFabric IAM 정책 예제

생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

다음 정책 예제는 생산성을 위한 AppFabric 기능에 적용됩니다.

productivity 기능에 대한 읽기 전용 액세스 허용

다음 정책 예제는 생산성을 위한 AppFabric 기능에 대한 읽기 전용 액세스 권한을 부여합니다.

> **Important**
>
> IAM 콘솔의 JSON 정책 편집기에서 이 정책을 추가할 때 잘못된 작업 오류가 표시될 수 있습니다. 이는 생산성을 위한 AppFabric 기능이 현재 평가판이기 때문입니다. 오류를 무시하고 정책 생성을 진행해야 합니다.

생산성 기능에 대한 전체 액세스 허용

다음 정책 예제는 생산성을 위한 AppFabric 기능에 대한 전체 액세스 권한을 부여합니다.

> **Important**
>
> IAM 콘솔의 JSON 정책 편집기에서 이 정책을 추가할 때 잘못된 작업 오류가 표시될 수 있습니다. 이는 생산성을 위한 AppFabric 기능이 현재 평가판이기 때문입니다. 오류를 무시하고 정책 생성을 진행해야 합니다.

AppClient 생성 액세스 허용

다음 정책 예제는 AppClient를 생성할 수 있는 액세스 권한을 부여합니다. 자세한 내용은 생산성을 위한 AppFabric AppClient 생성을 참조하세요.

> **Important**
>
> IAM 콘솔의 JSON 정책 편집기에서 이 정책을 추가할 때 잘못된 작업 오류가 표시될 수 있습니다. 이는 생산성을 위한 AppFabric 기능이 현재 평가판이기 때문입니다. 오류를 무시하고 정책 생성을 진행해야 합니다.

AppClient의 세부 정보를 가져오는 액세스 허용

다음 정책 예제는 AppClients의 세부 정보를 가져올 수 있는 액세스 권한을 부여합니다. 자세한 내용은 AppClient의 세부 정보 가져오기를 참조하세요.

> **Important**
>
> IAM 콘솔의 JSON 정책 편집기에서 이 정책을 추가할 때 잘못된 작업 오류가 표시될 수 있습니다. 이는 생산성을 위한 AppFabric 기능이 현재 평가판이기 때문입니다. 오류를 무시하고 정책 생성을 진행해야 합니다.

AppClient 목록에 대한 액세스 허용

다음 정책 예제는 AppClient를 나열할 수 있는 액세스 권한을 부여합니다. 자세한 내용은 AppClient의 세부 정보 가져오기를 참조하세요.

> **Important**
>
> IAM 콘솔의 JSON 정책 편집기에서 이 정책을 추가할 때 잘못된 작업 오류가 표시될 수 있습니다. 이는 생산성을 위한 AppFabric 기능이 현재 평가판이기 때문입니다. 오류를 무시하고 정책 생성을 진행해야 합니다.

AppClient 업데이트 액세스 허용

다음 정책 예제는 AppClient를 업데이트할 수 있는 액세스 권한을 부여합니다. 자세한 내용은 AppClient 업데이트를 참조하세요.

> **Important**
>
> IAM 콘솔의 JSON 정책 편집기에서 이 정책을 추가할 때 잘못된 작업 오류가 표시될 수 있습니다. 이는 생산성을 위한 AppFabric 기능이 현재 평가판이기 때문입니다. 오류를 무시하고 정책 생성을 진행해야 합니다.

AppClient 삭제 액세스 허용

다음 정책 예제는 AppClient를 삭제할 수 있는 액세스 권한을 부여합니다. 자세한 내용은 AppClient 업데이트를 참조하세요.

> **Important**
>
> IAM 콘솔의 JSON 정책 편집기에서 이 정책을 추가할 때 잘못된 작업 오류가 표시될 수 있습니다. 이는 생산성을 위한 AppFabric 기능이 현재 평가판이기 때문입니다. 오류를 무시하고 정책 생성을 진행해야 합니다.

애플리케이션 승인 액세스 허용

다음 정책 예제는 토큰 API를 사용하여 애플리케이션에 권한을 부여할 수 있는 액세스 권한을 부여합니다. 자세한 내용은 애플리케이션 인증 및 권한 부여를 참조하세요.

> **Important**
>
> IAM 콘솔의 JSON 정책 편집기에서 이 정책을 추가할 때 잘못된 작업 오류가 표시될 수 있습니다. 이는 생산성을 위한 AppFabric 기능이 현재 평가판이기 때문입니다. 오류를 무시하고 정책 생성을 진행해야 합니다.

기타 IAM 정책 예시

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
```

```
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AppFabric에 서비스 연결 역할 사용

AWS AppFabric은 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 AppFabric에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 AppFabric에서 사전 정의하며 사용자를 대신하여 서비스에서 다른 AWS 서비스 을 호출하기 위해 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할은 AppFabric을 더 쉽게 설정할 수 있습니다. AppFabric에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, AppFabric만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 AppFabric 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 AWS IAM으로 작업하는 서비스를 참조하고 서비스 연결 역할 열에서 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

AppFabric에 대한 서비스 연결 역할 권한

AppFabric은 라는 서비스 연결 역할을 사용합니다. AWSServiceRoleForAppFabric AppFabric은 Amazon S3 버킷 또는 Amazon Data Firehose 전송 스트림과 같은 수집 대상 리소스에 데이터를 넣을 수 있습니다. 또한 AppFabric이 CloudWatch 지표 데이터를 AWS/AppFabric 네임스페이스에 넣을 수 있습니다.

AWSServiceRoleForAppFabric 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- appfabric.amazonaws.com

AWSAppFabricServiceRolePolicy라는 역할 권한 정책은 AppFabric이 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- 작업: AWS/AppFabric 네임스페이스에서 cloudwatch:PutMetricData. 이 작업은 AppFabric이 지표 데이터를 Amazon CloudWatch AWS/AppFabric 네임스페이스에 넣을 수 있는 권한을 부여합니다. CloudWatch에 저장된 AppFabric 지표에 대한 자세한 내용은 Amazon CloudWatch를 사용한 모니터링 AWS AppFabric을 참조하십시오.
- 작업: Amazon S3 버킷의 s3:PutObject. 이 작업은 AppFabric이 사용자가 지정한 Amazon S3 버킷에 수집된 데이터를 넣을 수 있는 권한을 부여합니다.
- 작업: Amazon Data Firehose 전송 스트림firehose:PutRecordBatch에서. 이 작업은 AppFabric이 수집한 데이터를 지정한 Amazon Data Firehose 전송 스트림에 넣을 수 있는 권한을 부여합니다.

자세한 내용은 AppFabric에 대한AWS 관리형 정책을 참조하십시오.

사용자, 그룹 또는 역할이 서비스 연결 역할을 생성, 편집 또는 삭제할 수 있도록 사용 권한을 구성해야 합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하십시오.

AppFabric에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. AWS CLI, 또는 AWS API에서 AppFabric 앱 번들 AWS Management Console을 생성하면 AppFabric이 서비스 연결 역할을 생성합니다.

AppFabric에 대한 서비스 연결 역할 편집

AppFabric에서는 AWSServiceRoleForAppFabric 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을

변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하십시오.

AppFabric에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 그러나 서비스 연결 역할을 삭제하려면 먼저 모든 AppFabric 앱 번들을 삭제해야 합니다.

서비스 연결 역할을 정리

IAM을 사용하여 서비스 연결 역할을 삭제하기 전에 먼저 역할에서 사용되는 리소스를 삭제해야 합니다. AppFabric에서 생성한 앱 번들은 역할에 사용됩니다. 자세한 내용은 Delete AWS AppFabric for 보안 리소스을 참조하십시오.

> **Note**
>
> 리소스를 삭제하려 할 때 AppFabric 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하십시오.

수동으로 서비스 연결 역할 삭제

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 `AWSServiceRoleForAppFabric` 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

AppFabric 서비스 연결 역할에 대해 지원되는 리전

AppFabric은 서비스를 사용할 수 있는 모든 AWS 리전 에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS 일반 참조의 AppFabric 엔드포인트 및 할당량을 참조하십시오.

AWS AWS AppFabric에 대한 관리형 정책

사용자, 그룹 및 역할에 권한을 추가하려면 직접 정책을 작성하는 것보다 AWS 관리형 정책을 사용하는 것이 더 쉽습니다. 팀에 필요한 권한만 제공하는 IAM 고객 관리형 정책을 생성하기 위해서는 시간과 전문 지식이 필요합니다. 빠르게 시작하려면 AWS 관리형 정책을 사용할 수 있습니다. 이 정책은 일반적인 사용 사례를 다루며 사용자의 AWS 계정에서 사용할 수 있습니다. AWS 관리형 정책에 대한 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 서비스 AWS 관리형 정책을 유지 관리하고 업데이트합니다. AWS 관리형 정책에서는 권한을 변경할 수 없습니다. 서비스에서 때때로 추가 권한을 AWS 관리형 정책에 추가하여 새로운 기능을 지원

합니다. 이 유형의 업데이트는 정책이 연결된 모든 ID(사용자, 그룹 및 역할)에 적용됩니다. 서비스는 새로운 기능이 시작되거나 새 작업을 사용할 수 있을 때 AWS 관리형 정책에 업데이트됩니다. 서비스는 AWS 관리형 정책에서 권한을 제거하지 않으므로 정책 업데이트로 인해 기존 권한이 손상되지 않습니다.

또한는 여러 서비스에 걸쳐 있는 직무에 대한 관리형 정책을 AWS 지원합니다. 예를 들어 ReadOnlyAccess AWS 관리형 정책은 모든 AWS 서비스 및 리소스에 대한 읽기 전용 액세스를 제공합니다. 서비스가 새 기능을 시작하면는 새 작업 및 리소스에 대한 읽기 전용 권한을 AWS 추가합니다. 직무 정책의 목록과 설명은 IAM 사용 설명서의 직무에 관한AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AWSAppFabricReadOnlyAccess

`AWSAppFabricReadOnlyAccess` 정책을 IAM ID에 연결할 수 있습니다. 이 정책은 AppFabric 서비스에 읽기 전용 권한을 부여합니다.

> **Note**
>
> `AWSAppFabricReadOnlyAccess` 정책에서는 생산성을 위한 AppFabric 기능에 대한 읽기 전용 액세스 권한을 부여하지 않습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `appfabric`- 앱 번들 가져오기, 앱 번들 목록 표시, 앱 인증 받기, 앱 인증 목록 표시, 수집 가져오기, 수집 목록 표시, 수집 대상 가져오기, 수집 대상 목록 표시, 리소스 태그 목록 표시 권한을 부여합니다.

JSON

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

```
                "appfabric:GetIngestion",
                "appfabric:GetIngestionDestination",
                "appfabric:ListAppAuthorizations",
                "appfabric:ListAppBundles",
                "appfabric:ListIngestionDestinations",
                "appfabric:ListIngestions",
                "appfabric:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 관리형 정책: AWSAppFabricFullAccess

AWSAppFabricFullAccess 정책을 IAM ID에 연결할 수 있습니다. 이 정책은 AppFabric 서비스에 관리 권한을 부여합니다.

> **Important**
>
> 생산성을 위한 AppFabric은 현재 평가판이므로 AWSAppFabricFullAccess 정책에서는 생산성을 위한 AppFabric 기능에 대한 액세스 권한을 부여하지 않습니다. 생산성을 위한 AppFabric 기능의 액세스 권한 부여에 대한 자세한 내용은 생산성을 위한 AppFabric IAM 정책 예제 섹션을 참조하세요.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- appfabric – AppFabric에 전체 관리 권한을 부여합니다.
- kms – 별칭을 나열할 수 있는 권한을 부여합니다.
- s3 – 모든 Amazon S3 버킷을 나열하고 버킷 위치를 가져올 수 있는 권한을 부여합니다.
- firehose - Amazon Data Firehose 전송 스트림을 나열하고 전송 스트림을 설명할 수 있는 권한을 부여합니다.
- iam – AppFabric의 AWSServiceRoleForAppFabric 서비스 연결 역할을 생성할 권한을 부여합니다. 자세한 내용은 AppFabric에 서비스 연결 역할 사용 단원을 참조하십시오.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["appfabric:*"],
            "Resource": "*"
        },
        {
            "Sid": "KMSListAccess",
            "Effect": "Allow",
            "Action": ["kms:ListAliases"],
            "Resource": "*"
        },
        {
            "Sid": "S3ReadAccess",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "FirehoseReadAccess",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:ListDeliveryStreams"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUseOfServiceLinkedRole",
            "Effect": "Allow",
            "Action": ["iam:CreateServiceLinkedRole"],
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "appfabric.amazonaws.com"}
            },
            "Resource": "arn:aws:iam::*:role/aws-service-role/
appfabric.amazonaws.com/AWSServiceRoleForAppFabric"
```

```
        }
    ]
}
```

AWS 관리형 정책: AWSAppFabricServiceRolePolicy

`AWSAppFabricServiceRolePolicy` 정책을 IAM 엔터티에 연결할 수 없습니다. 이 정책은 AppFabric이 사용자를 대신하여 작업을 수행할 수 있는 서비스 연결 역할에 연결되어 있습니다. 자세한 내용은 AppFabric에 서비스 연결 역할 사용을 참조하십시오.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `cloudwatch` – AppFabric이 지표 데이터를 Amazon CloudWatch `AWS/AppFabric` 네임스페이스에 넣을 수 있는 권한을 부여합니다. CloudWatch에 저장된 AppFabric 지표에 대한 자세한 내용은 Amazon CloudWatch를 사용한 모니터링 AWS AppFabric을 참조하십시오.
- `s3` – AppFabric이 수집된 데이터를 지정한 Amazon S3 버킷에 넣을 수 있는 권한을 부여합니다.
- `firehose` - AppFabric이 수집한 데이터를 지정한 Amazon Data Firehose 전송 스트림에 넣을 수 있는 권한을 부여합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CloudWatchEmitMetric",
            "Effect": "Allow",
            "Action": ["cloudwatch:PutMetricData"],
            "Resource": "*",
            "Condition": {
                "StringEquals": {"cloudwatch:namespace": "AWS/AppFabric"}
            }
        },
        {
            "Sid": "S3PutObject",
            "Effect": "Allow",
            "Action": ["s3:PutObject"],
```

```
            "Resource": "arn:aws:s3:::*/AWSAppFabric/*",
            "Condition": {
                "StringEquals": {"s3:ResourceAccount": "${aws:PrincipalAccount}"}
            }
        },
        {
            "Sid": "FirehosePutRecord",
            "Effect": "Allow",
            "Action": ["firehose:PutRecordBatch"],
            "Resource": "arn:aws:firehose:*:*:deliverystream/*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/AWSAppFabricManaged":
 "true"}
            }
        }
    ]
}
```

AWS 관리형 정책에 대한 AppFabric 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 AppFabric의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 AppFabric 문서 기록 페이지에서 RSS 피드를 구독하십시오.

변경	설명	Date
AWSAppFabricReadOnlyAccess - 새 정책	AppFabric은 AppFabric 서비스에 읽기 전용 권한을 부여하는 새로운 정책을 추가했습니다.	2023년 6월 27일
AWSAppFabricFullAccess - 새 정책	AppFabric은 AppFabric 서비스에 관리자 권한을 부여하는 새 정책을 추가했습니다.	2023년 6월 27일
AWSAppFabricServiceRolePolicy - 새 정책	AppFabric은 `AWSServiceRoleForAppFabric` 서비스 연결 역할에 대한 새 정책을 추가했습니다.	2023년 6월 27일

변경	설명	Date
AppFabric에서 변경 내용 추적 시작	AppFabric이 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2023년 6월 27일

AWS AppFabric 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 AppFabric 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- AppFabric에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행할 권한이 없음
- 내 외부의 사람이 내 AppFabric 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

AppFabric에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 표시되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `appfabric:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 appfabric:GetWidget on resource: my-example-widget
```

이 경우, `appfabric:`*`GetWidget`* 작업을 사용하여 *`my-example-widget`* 리소스에 액세스할 수 있도록 `mateojackson` 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행할 권한이 없음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 AppFabric에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예제 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 AppFabric에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 AppFabric 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하십시오.

- AppFabric에서 이러한 기능을 지원하는지 여부를 알아보려면 AWS AppFabric과 IAM의 작동 방식을 참조하십시오
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 리소스에 대한 액세스 권한을 타사에 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 소유에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

AWS AppFabric에 대한 규정 준수 검증

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 AWS 서비스 규정 준수 프로그램 범위 내 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 에서 보고서 다운로드 AWS Artifact에서 .

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다. 사용 시 규정 준수 책임에 대한 자세한 내용은 AWS 보안 설명서를 AWS 서비스참조하세요.

AWS AppFabric의 보안 모범 사례

AWS AppFabric은 자체 보안 정책을 개발하고 구현할 때 고려해야 할 몇 가지 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용하십시오.

관리자 액세스 없이 애플리케이션 모니터링

읽기 전용 AWS Identity and Access Management (IAM) 권한을 사용하면 누구나 AppFabric을 Amazon Quick 및와 같은 기타 보안 정보 및 이벤트 관리(SIEM) 도구와 통합할 수 있습니다Splunk. 애플리케이션 보안을 모니터링하기 위해 데이터는 Amazon Simple Storage Service(Amazon S3) 버킷 또는 Amazon Data Firehose 전송 스트림으로 전송됩니다.

AppFabric 이벤트 모니터링

Amazon CloudWatch 지표를 사용하여 AppFabric을 모니터링할 수 있습니다. CloudWatch는 1분마다 AppFabric에서 데이터를 수집하여 지표로 처리합니다. 지표가 지정된 임계값과 일치할 경우 알림을 시작하도록 경보를 설정할 수 있습니다. 자세한 내용은 Amazon CloudWatch를 사용한 모니터링 AWS AppFabric 단원을 참조하십시오.

AWS AppFabric의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공하며,이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

인 AWS AppFabric의 인프라 보안

관리형 서비스인 AWS AppFabric은 Amazon Web Services: 보안 프로세스 개요 백서에 설명된 AWS 글로벌 네트워크 보안 절차로 보호됩니다. https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 AppFabric에 액세스합니다. 클라이언트는 TLS 1.0 이상을 지원해야 합니다. TLS 1.2 이상을 권장합니다. 클라이언트는 DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 요청에 서명할 임시 보안 인증 정보를 생성하려면 AWS Security Token Service(AWS STS)를 사용할 수 있습니다.

AWS AppFabric의 구성 및 취약성 분석

구성 및 IT 제어는 AWS 와 고객 간의 공동 책임입니다. 자세한 내용은 AWS 공동 책임 모델을 참조하세요.

모니터링 AWS AppFabric

모니터링은 AWS AppFabric 및 기타 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다.는 AppFabric을 모니터링하고, 이상이 있을 때 이를 보고하고, 필요한 경우 자동 조치를 취할 수 있도록 다음과 같은 모니터링 도구를 AWS 제공합니다.

- Amazon CloudWatch는 AWS 리소스와 AWS 에서 실행하는 애플리케이션을 실시간으로 모니터링합니다. 지표를 수집 및 추적하고, 사용자 지정 대시보드를 생성할 수 있으며, 지정된 지표가 지정한 임곗값에 도달하면 사용자에게 알리거나 조치를 취하도록 경보를 설정할 수 있습니다. 예를 들어 CloudWatch에서 Amazon EC2 인스턴스의 CPU 사용량 또는 기타 지표를 추적하고 필요할 때 자동으로 새 인스턴스를 시작할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용자 안내서를 참조하세요.
- Amazon CloudWatch Logs를 사용하면 Amazon EC2 인스턴스 및 기타 소스에서 로그 파일을 모니터링 AWS CloudTrail, 저장 및 액세스할 수 있습니다. CloudWatch Logs는 로그 파일의 정보를 모니터링하고 특정 임계값에 도달하면 사용자에게 알릴 수 있습니다. 또한 매우 내구성이 뛰어난 스토리지에 로그 데이터를 저장할 수 있습니다. 자세한 내용은 Amazon CloudWatch Logs 사용자 안내서를 참조하세요.
- AWS CloudTrail는에 의해 또는를 대신하여 수행된 API 호출 및 관련 이벤트를 캡처 AWS 계정 하고 사용자가 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 호출한 사용자 및 계정 AWS, 호출이 수행된 소스 IP 주소, 호출이 발생한 시기를 식별할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

Amazon CloudWatch를 사용한 모니터링 AWS AppFabric

원시 데이터를 수집하여 읽기 가능하며 실시간에 가까운 지표로 처리하는 CloudWatch를 사용하여 AWS AppFabric을 모니터링할 수 있습니다. 이러한 통계는 15개월간 보관되므로 기록 정보에 액세스하고 웹 애플리케이션 또는 서비스가 어떻게 실행되고 있는지 전체적으로 더 잘 파악할 수 있습니다. 특정 임곗값을 주시하다가 해당 임곗값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

AppFabric 서비스는 `AWS/AppFabric` 네임스페이스에서 다음 지표를 보고합니다.

지표	설명
AppFabric 앱 권한 부여 상태	앱 권한 부여의 상태입니다(1연결된 경우 , 다른 0 경우).

지표	설명
AppFabric 데이터 전송 지연 시간	AppFabric이 SaaS 애플리케이션에서 감사 로그를 수집하여 구성된 대상(Amazon S3 또는 Amazon Data Firehose)으로 전송하는 데 걸린 시간(초)입니다.
수집 대상 상태	수집 대상의 상태 (1은 활성, 0는 기타).
전체 데이터 지연	SaaS 애플리케이션에서 이벤트가 발생한 시점과 AppFabric이 해당 감사 로그를 구성된 대상(Amazon S3 또는 Amazon Data Firehose)으로 전송한 시점 간의 시간 차이(초).
수집된 데이터의 양	Amazon Simple Storage Service(Amazon S3) 또는 Amazon Data Firehose로 전송되는 데이터의 크기입니다.

AppFabric 지표에는 다음 차원이 지원됩니다.

차원	설명
수집 대상 ARN	수집 대상의 Amazon 리소스 이름(ARN)입니다.

를 사용하여 AWS AppFabric API 호출 로깅 AWS CloudTrail

AWS AppFabric은 AppFabric AWS 서비스 에서 사용자 AWS CloudTrail, 역할 또는가 수행한 작업에 대한 레코드를 제공하는 서비스와 통합됩니다. CloudTrail은 AppFabric에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 AppFabric 콘솔로부터의 호출과 AppFabric API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 AppFabric 이벤트를 포함하여 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 전달할 수 있습니다. 추적을 구성하지 않은 경우에도 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 AppFabric에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

CloudTrail의 AppFabric 정보

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. AppFabric에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 이벤트와 함께 CloudTrail AWS 서비스 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은AWS CloudTrail 사용 설명서에서 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

AppFabric에 대한 이벤트를 AWS 계정포함하여에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 트레일을 생성하면 기본적으로 모든 AWS 리전에 트레일이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스 를 구성할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서에서 다음 주제를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 수신 및 여러 계정에서 CloudTrail 로그 파일 수신

모든 작업은 CloudTrail에서 로깅되고 AWS AppFabric API 참조에 기록됩니다. 예를 들어 `CreateAppBundle`, `UpdateAppBundle` 및 `GetAppBundle` 작업을 직접적으로 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자의 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부

자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail userIdentity 요소를 참조하십시오.

AppFabric 로그 파일 항목의 이해

트레일이란 지정한 S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타

내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음은 `CreateAppBundle` 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예시입니다.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser",
        "arn": "arn:aws:sts::111122223333:assumed-role/AssumedRole/SampleUser",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAXUFER33B4FVC2GCYR",
                "arn": "arn:aws:iam::111122223333:role/AssumedRole",
                "accountId": "111122223333",
                "userName": "SampleUser"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-31T21:11:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-31T21:22:16Z",
    "eventSource": "appfabric.amazonaws.com",
    "eventName": "CreateAppBundle",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.90.81.91",
    "userAgent": "Coral/Apache-HttpClient5",
    "requestParameters": {
        "clientToken": "64d9069f-e565-49a4-9374-6dc8631142e2"
    },
    "responseElements": {
        "appBundle": {
            "arn": "arn:aws:appfabric:us-
east-1:111122223333:appbundle/6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1",
            "idpClientConfiguration": {
                "samlAudience": "urn:amazon:cognito:sp:us-east-1_GEdGiavzr",
```

```
                "samlRedirect": "https://6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1.auth.us-
east-1.amazoncognito.com/saml2/idpresponse",
                "oidcRedirect": "https://6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1.auth.us-
east-1.amazoncognito.com/oauth2/idpresponse"
            }
        }
    },
    "requestID": "17e15a5d-8c66-46c7-ad5b-f521004fa9c2",
    "eventID": "ba1dd847-86f6-4386-85be-0398e844a358",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "frontend.fabric.us-east-1.amazonaws.com"
    }
}
```

AppFabric 할당량

AWS 계정 에는 각에 대해 이전에 제한이라고 하는 기본 할당량이 있습니다 AWS 서비스. 다르게 표시되지 않는 한 리전별로 각 할당량이 적용됩니다. 일부 할당량에 대한 증가를 요청할 수 있으며 다른 할당량은 늘릴 수 없습니다.

AppFabric에 대한 할당량을 보려면Service Quotas 콘솔을 엽니다. 탐색 창에서 AWS 서비스 를 선택하고 AppFabric을 선택합니다.

할당량 증가을 요청하려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하십시오. Service Quotas에서 아직 할당량을 사용할 수 없는 경우 한도 증가 양식을 사용합니다.

에 있는 AppFabric과 관련된 할당량은 다음 표에 AWS 계정 나와 있습니다.

이름	기본값	조정 가능	설명
애플리케이션 번들	지원되는 각 리전: 1	아니요	현재 AWS 리전의 계정에서 생성할 수 있는 최대 애플리케이션 번들 수입니다.
애플리케이션 인증	지원되는 각 리전: 50	아니요	현재 AWS 리전의 계정에서 생성할 수 있는 최대 애플리케이션 권한 부여 수입니다.
수집	지원되는 각 리전: 50	아니요	현재 AWS 리전의 계정에서 생성할 수 있는 최대 수집 수입니다.
수집 대상	지원되는 각 리전: 5	아니요	현재 AWS 리전의 계정에서 수집당 생성할 수 있는 최대 수집 대상 수입니다.

이름	기본값	조정 가능	설명
AppClient	지원되는 각 리전: 1	아니요	현재 AWS 리전의 계정에서 생성할 수 있는 AppClients의 최대 수입니다. 생산성을 위한 AWS AppFabric 기능은 미리 보기 중이며 변경될 수 있습니다.

AppFabric 관리 설명서의 문서 기록

다음 표에서는 AWS AppFabric의 설명서 릴리스를 설명합니다.

변경 사항	설명	날짜
새로 지원되는 애플리케이션	를 지원되는 애플리케이션JumpCloud으로 추가했습니다. 자세한 내용은 AWS AppFabric에서 지원되는 애플리케이션을 참조하세요.	2024년 6월 5일
새로 지원되는 애플리케이션 및 보안 도구	지원되는 애플리케이션Google Analytics으로 Azure Monitor 및를 추가했습니다. 자세한 내용은 AWS AppFabric에서 지원되는 애플리케이션을 참조하세요. 지원되는 보안 도구Singularity Cloud로를 추가했습니다. 자세한 내용은 호환 가능한 보안 도구를 참조하세요.	2024년 4월 30일
새로 지원되는 애플리케이션	를 지원되는 애플리케이션SentinelOne으로 추가했습니다. 자세한 내용은 AWS AppFabric에서 지원되는 애플리케이션을 참조하세요.	2024년 4월 25일
새로 지원되는 애플리케이션	를 지원되는 애플리케이션1Password으로 추가했습니다. 자세한 내용은 AWS AppFabric에서 지원되는 애플리케이션을 참조하세요.	2024년 4월 23일
새로 지원되는 보안 도구	호환되는 보안 도구Dynatrace로를 추가했습니다. 자세한 내	2024년 3월 26일

	용은 호환되는 보안 도구를 참조하세요.	
새 지표	AppFabric 앱 권한 부여 상태 지표가 추가되었습니다. 자세한 내용은 Amazon CloudWatch Logs를 사용한 Monitoring AWS AppFabric을 참조하세요.	2024년 3월 8일
새로 지원되는 애플리케이션	를 지원되는 애플리케이션IBM Security® Verify으로 추가했습니다. 자세한 내용은 AWS AppFabric에서 지원되는 애플리케이션을 참조하세요.	2024년 3월 6일
새로 지원되는 애플리케이션	지원되는 애플리케이션Box으로를 추가했습니다. 자세한 내용은 AWS AppFabric에서 지원되는 애플리케이션을 참조하세요.	2024년 2월 28일
새로 지원되는 애플리케이션 및 지표	Cisco Duo, 및 Salesforce를 지원되는 애플리케이션Terraform Cloud으로 추가했습니다. 이에 대한 자세한 내용은 AWS AppFabric에서 지원되는 애플리케이션을 참조하세요. AppFabric 데이터 전송 지연 시간 및 전체 데이터 지연 지표가 추가되었습니다. 자세한 내용은 Amazon CloudWatch Logs를 사용한 Monitoring AWS AppFabric을 참조하세요.	2024년 2월 1일

Atlassian Confluence, Genesys Cloud, HubSpot, OneLogin by One Identity, PagerDuty, 및 Ping Identity 등 지원되는 애플리케이션 추가 및 호환 가능한 보안 도구 Barracuda XDR 추가	지원되는 새 애플리케이션에 대한 자세한 내용은 지원되는 애플리케이션 in AWS AppFabric 및 호환되는 보안 도구를 참조하세요.	2023년 12월 15일
Atlassian Confluence, Genesys Cloud, HubSpot, OneLogin by One Identity, PagerDuty, 및 Ping Identity 등 지원되는 애플리케이션 추가 및 호환 가능한 보안 도구 Barracuda XDR 추가	지원되는 새 애플리케이션에 대한 자세한 내용은 지원되는 애플리케이션 in AWS AppFabric 및 호환되는 보안 도구를 참조하세요.	2023년 12월 15일
생산성을 위한 AWS AppFabric 미리 보기 설명서 추가	생산성을 위한 AppFabric에 대한 자세한 내용은 AWS 생산성을 위한 AppFabric이란 무엇입니까?를 참조하세요.	2023년 11월 27일
지원되는 애플리케이션으로 GitHub 및 ServiceNow 추가	새로 지원되는 애플리케이션에 대한 자세한 내용은 지원되는 애플리케이션을 참조하세요.	2023년 10월 31일
AWS AppFabric에 대한 AWS 관리형 정책 추적 시작	AppFabric의 AWS 관리형 정책에 대한 자세한 내용은 AWSAWS AppFabric의 관리형 정책을 참조하세요.	2023년 6월 27일
최초 릴리스	AWS AppFabric 관리 안내서의 최초 릴리스입니다.	2023년 6월 27일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.