Administratorhandbuch

AWS AppFabric

AWS AppFabric: Administratorhandbuch

Table of Contents

Was ist AWS AppFabric?

AWS AppFabric verbindet schnell Software-as-a-Service (SaaS) -Anwendungen in Ihrem gesamten Unternehmen, sodass IT- und Sicherheitsteams Anwendungen mithilfe eines Standardschemas einfach verwalten und sichern können und Mitarbeiter alltägliche Aufgaben mithilfe generativer KI schneller erledigen können.

Themen

Produkte

Erkunden Sie die beiden Aspekte AWS AppFabric: AppFabric für Sicherheit, konzipiert für optimierte Verwaltung und Sicherheit, und AppFabric für Produktivität (Vorversion), erweitert durch generative KI-Funktionen. Weitere Informationen finden Sie unter den folgenden Themen:

- Was ist AWS AppFabric für die Sicherheit?
- Was ist AWS AppFabric für die Produktivität?

Vorteile

Sie können verwenden AppFabric , um Folgendes zu tun:

- Connect Sie Ihre Anwendungen innerhalb von Minuten und reduzieren Sie die Betriebskosten.
- Erhöhen Sie die Transparenz aller SaaS-Anwendungsdaten, um Ihre Sicherheitslage zu verbessern.
- Erleichtern Sie Aufgaben automatisch anwendungsübergreifend mit generativer KI.

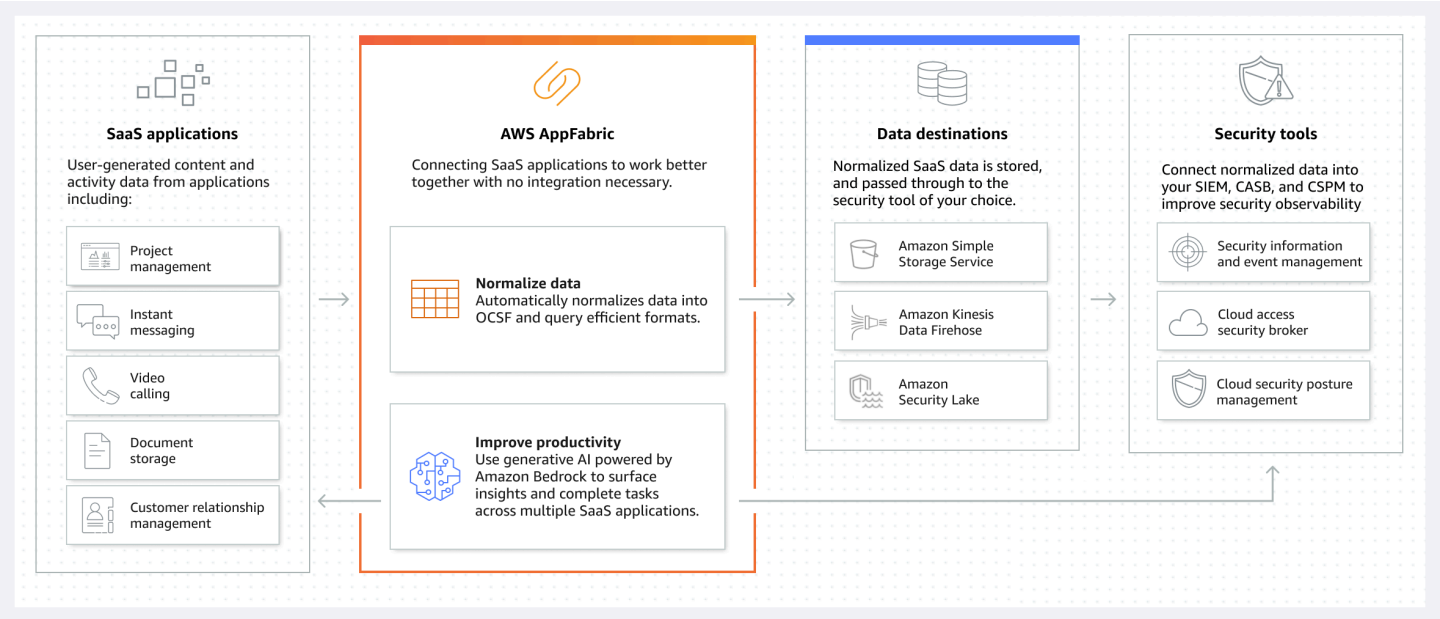
Anwendungsfälle

Sie können Folgendes AppFabric verwenden:

- Connect Ihre SaaS-Anwendungen schnell
  - AppFabric for Security verbindet native SaaS-Produktivitäts- und Sicherheitsanwendungen miteinander und bietet so eine vollständig verwaltete SaaS-Interoperabilitätslösung.
- Verbessern Sie Ihr Sicherheitsniveau
  - Anwendungsdaten werden automatisch normalisiert, sodass Administratoren gemeinsame Richtlinien festlegen, Sicherheitswarnungen standardisieren und den Benutzerzugriff für mehrere Anwendungen einfach verwalten können.
- Stellen Sie sich Produktivität neu vor
  - Mit einem gemeinsamen generativen KI-Assistenten ermöglicht AppFabric For Productivity Mitarbeitern, schnell Antworten zu erhalten, das Aufgabenmanagement zu automatisieren und Einblicke in ihre SaaS-Produktivitätsanwendungen zu gewinnen.

Wie funktioniert AppFabric

AppFabric verbindet schnell mehrere SaaS-Anwendungen, ohne dass eine Codierung erforderlich ist, um die Produktivität und Sicherheit zu erhöhen. Das folgende Diagramm zeigt die Vorteile von AppFabric.



> **Note**
>
> AppFabric For Productivity wird derzeit als Vorversion eingeführt und ist im Osten der USA (Nord-Virginia) erhältlich AWS-Region. Weitere Informationen zu finden Sie AWS-Regionen unter AWS AppFabric Endpunkte und Kontingente im Allgemeine AWS-Referenz.

Preisgestaltung

AppFabric Preisdetails und Beispiele finden Sie unter AWS AppFabric Preisgestaltung.

Verfügbarkeit

Die derzeit unterstützten AWS Regionen und Endpunkte für AppFabric finden Sie unter AWS AppFabric Endpunkte und Kontingente in der AWS Allgemeinen Referenz.

Was ist AWS AppFabric für die Sicherheit?

AWS AppFabric for Security verbindet schnell Software-as-a-Service (SaaS) -Anwendungen innerhalb Ihres Unternehmens, sodass IT- und Sicherheitsteams Anwendungen mithilfe eines Standardschemas einfach verwalten und sichern können.

Themen

Vorteile

Sie können AppFabric for Security verwenden, um Folgendes zu tun:

- Connect Sie Ihre Anwendungen innerhalb von Minuten und reduzieren Sie die Betriebskosten.
- Erhöhen Sie die Transparenz aller SaaS-Anwendungsdaten, um Ihre Sicherheitslage zu verbessern.

Anwendungsfälle

Aus AppFabric Sicherheitsgründen können Sie Folgendes verwenden:

- Connect Ihre SaaS-Anwendungen schnell
  - AppFabric for Security verbindet native SaaS-Produktivitäts- und Sicherheitsanwendungen miteinander und bietet so eine vollständig verwaltete SaaS-Interoperabilitätslösung.
- Verbessern Sie Ihr Sicherheitsniveau
  - Anwendungsdaten werden automatisch normalisiert, sodass Administratoren gemeinsame Richtlinien festlegen, Sicherheitswarnungen standardisieren und den Benutzerzugriff für mehrere Anwendungen einfach verwalten können.

Zugriff AppFabric aus Sicherheitsgründen

AppFabric Aus Sicherheitsgründen ist es im Osten der USA (Nord-Virginia), Europa (Irland) und im asiatisch-pazifischen Raum (Tokio) verfügbar AWS-Regionen. Weitere Informationen zu finden Sie AWS-Regionen unter AWS AppFabric Endpunkte und Kontingente im Allgemeine AWS-Referenz.

In jeder Region können Sie aus AppFabric Sicherheitsgründen auf eine der folgenden Arten zugreifen:

AWS Management Console

Das AWS Management Console ist eine browserbasierte Oberfläche, mit der Sie AWS Ressourcen erstellen und verwalten können. Die AppFabric Konsole bietet Zugriff auf Ihre AppFabric Ressourcen. Sie können die AppFabric Konsole verwenden, um alle AppFabric Ressourcen zu erstellen und zu verwalten.

AppFabric API

Verwenden Sie für den AppFabric programmgesteuerten Zugriff die AppFabric API und senden Sie HTTPS-Anfragen direkt an den Dienst. Weitere Informationen finden Sie in der AWS AppFabric API-Referenz.

AWS Command Line Interface (AWS CLI)

Mit dem AWS CLI können Sie Befehle an der Befehlszeile Ihres Systems ausgeben, um mit anderen AppFabric zu interagieren AWS -Services. Wenn Sie Skripts erstellen möchten, die Aufgaben ausführen, sind die Befehlszeilentools ebenfalls nützlich. Informationen zur Installation und Verwendung von finden Sie im AWS Command Line Interface Benutzerhandbuch für Version 2. AWS CLI Informationen zu den AWS CLI Befehlen für AppFabric finden Sie im AppFabric Abschnitt der AWS CLI Referenz.

Zugehörige Services

Aus Sicherheitsgründen können Sie Folgendes AWS -Services mit AppFabric verwenden:

Amazon Data Firehose

Amazon Data Firehose ist ein ETL-Service (Extrahieren, Transformieren und Laden), der Streaming-Daten zuverlässig erfasst, transformiert und an Data Lakes, Datenspeicher und Analysedienste weiterleitet. Bei der Verwendung können Sie wählen AppFabric, ob Sie Ihre Open Cybersecurity Schema Framework (OCSF) normalisierten oder rohen Audit-Logs im JSON-Format in einen Firehose-Stream als Ziel ausgeben möchten. Weitere Informationen finden Sie unter Erstellen eines Ausgabespeicherorts in Firehose.

Amazon Security Lake

Amazon Security Lake zentralisiert automatisch Sicherheitsdaten aus AWS Umgebungen, SaaS-Anbietern, lokalen und Cloud-Quellen in einem speziell entwickelten Data Lake, der in Ihrem Konto gespeichert ist. Sie können AppFabric Audit-Protokolldaten in Security Lake integrieren, indem Sie Amazon Data Firehose als Ziel auswählen und Firehose so konfigurieren, dass Daten im richtigen Format und Pfad in Security Lake bereitgestellt werden. Weitere Informationen finden Sie unter Sammeln von Daten aus benutzerdefinierten Quellen im Amazon Security Lake-Benutzerhandbuch.

Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet. Wenn Sie verwenden AppFabric, können Sie wählen, ob Sie Ihre normalisierten (JSON oderApache Parquet) oder rohen (JSON)

Audit-Logs in einen neuen oder vorhandenen Amazon S3 S3-Bucket als Ziel ausgeben möchten. Weitere Informationen finden Sie unter Erstellen eines Ausgabespeicherorts in Amazon S3.

Amazon QuickSight

Amazon QuickSight unterstützt datengesteuerte Unternehmen mit einheitlicher Business Intelligence (BI) auf höchstem Niveau. Dank moderner interaktiver Dashboards QuickSight, paginierter Berichte, eingebetteter Analysen und Abfragen in natürlicher Sprache können alle Benutzer unterschiedliche Analyseanforderungen von derselben Informationsquelle aus erfüllen. Sie können AppFabric Audit-Protokolldaten analysieren QuickSight, indem Sie den Amazon S3 S3-Bucket, in dem Ihre AppFabric Protokolle gespeichert sind, als Quelle auswählen. Weitere Informationen finden Sie unter Erstellen eines Datensatzes mithilfe von Amazon S3 S3-Dateien im QuickSight Amazon-Benutzerhandbuch. Sie können auch AppFabric Daten aus Amazon S3 nach Amazon Athena importieren und Amazon Athena als Datenquelle in auswählen. QuickSight Weitere Informationen finden Sie unter Erstellen eines Datensatzes mit Amazon Athena Athena-Daten im QuickSight Amazon-Benutzerhandbuch.

AWS Key Management Service

Mit AWS Key Management Service (AWS KMS) können Sie kryptografische Schlüssel für Ihre Anwendungen und Anwendungen erstellen, verwalten und kontrollieren. AWS -Services Wenn Sie ein App-Bundle in erstellen AppFabric, richten Sie einen Verschlüsselungsschlüssel ein, um Ihre autorisierten Anwendungsdaten sicher zu schützen. Dieser Schlüssel verschlüsselt Ihre Daten innerhalb des AppFabric Dienstes. AppFabric kann einen in AppFabric Ihrem Namen AWS-eigener Schlüssel erstellten und verwalteten Schlüssel oder einen vom Kunden verwalteten Schlüssel verwenden, mit dem Sie ihn erstellen und verwalten. AWS KMS Weitere Informationen finden Sie unter AWS KMS Schlüssel erstellen.

Öffnen Sie das Cybersecurity Schema Framework

Das Open Cybersecurity Schema Framework (OCSF) ist eine gemeinsame Open-Source-Initiative von AWS führenden Partnern in der Cybersicherheitsbranche. OCSFbietet ein Standardschema für allgemeine Sicherheitsereignisse, definiert Versionierungskriterien, um die Schemaentwicklung zu erleichtern, und beinhaltet einen Selbstverwaltungsprozess für Hersteller und Nutzer von Sicherheitsprotokollen. Der öffentliche Quellcode für OCSF wird auf gehostet. GitHub

OCSFbasiertes Schema in AppFabric

Das auf AWS AppFabric for Security OCSF1.1 basierende Schema ist speziell auf Ihre Bedürfnisse nach einer normalisierten, konsistenten und aufwandsarmen Beobachtbarkeit ihres Software-as-a-

Service (SaaS) -Portfolios zugeschnitten. AppFabric bestimmt die richtige Zuordnung für jedes Feld und jedes Ereignis. AppFabrichat in Zusammenarbeit mit der OCSF Open-Source-Community neue OCSF Veranstaltungskategorien, Ereignisklassen, Aktivitäten und Objekte eingeführt, sodass OCSF sie für SaaS-Anwendungsereignisse gelten. AppFabric normalisiert automatisch Prüfereignisse, die es von SaaS-Anwendungen empfängt, und übermittelt diese Daten an den Amazon Simple Storage Service (Amazon S3) oder Amazon Data Firehose Services in Ihrem. AWS-Konto Für ein Amazon S3 S3-Ziel können Sie zwischen zwei Normalisierungsoptionen (OCSFoder Raw) und zwei Datenformatoptionen (JSONoderParquet) wählen. Bei der Lieferung an Firehose können Sie auch zwischen zwei Normalisierungsoptionen (OCSFoder Raw) wählen, das Datenformat ist jedoch auf Folgendes beschränkt. JSON

Voraussetzungen und Empfehlungen

Wenn Sie ein neuer AWS Kunde sind, müssen Sie die auf dieser Seite aufgeführten Einrichtungsvoraussetzungen erfüllen, bevor Sie mit der Nutzung aus AWS AppFabric Sicherheitsgründen beginnen. Für diese Einrichtungsverfahren verwenden Sie den AWS Identity and Access Management (IAM)-Service. Umfassende Informationen zu IAM finden Sie im IAM-Benutzerhandbuch.

Themen

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS -Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

(Erforderlich) Vollständige Bewerbungsvoraussetzungen

AppFabric Für den Empfang von Benutzerinformationen und Auditprotokollen von Anwendungen sind für viele Anwendungen bestimmte Rollen- und Plantypen erforderlich. Stellen Sie aus Sicherheitsgründen sicher, dass Sie die Voraussetzungen für jede Anwendung, AppFabric für die Sie eine Autorisierung vornehmen möchten, überprüft haben und dass Sie über die richtigen Pläne und Rollen verfügen. Weitere Informationen zu den anwendungsspezifischen Voraussetzungen finden Sie unter Unterstützte Anwendungen. Sie können auch eines der folgenden anwendungsspezifischen Themen auswählen.

- 1Password

- Asana
- Azure Monitor
- Atlassian Confluence
- Atlassian Jira suite
- Box
- Cisco Duo
- Dropbox
- Genesys Cloud
- GitHub
- Google Analytics
- Google Workspace
- HubSpot
- IBM Security® Verify
- JumpCloud
- Microsoft365
- Miro
- Okta
- OneLogin by One Identity
- PagerDuty
- Ping Identity
- Salesforce
- ServiceNow
- Singularity Cloud
- Slack
- Smartsheet
- Terraform Cloud
- Webex by Cisco
- Zendesk

- Zoom

(Optional) Erstellen Sie einen Ausgabespeicherort

AppFabric unterstützt aus Sicherheitsgründen Amazon Simple Storage Service (Amazon S3) und Amazon Data Firehose als Ziele für die Erfassung von Auditprotokollen.

Amazon S3

Sie können mithilfe der AppFabric Konsole einen neuen Amazon S3 S3-Bucket erstellen, wenn Sie ein Aufnahmeziel erstellen. Sie können einen Bucket auch mit dem Amazon S3 S3-Service erstellen. Wenn Sie Ihren Bucket mit dem Amazon S3 S3-Service erstellen möchten, müssen Sie den Bucket erstellen, bevor Sie das AppFabric Aufnahmeziel erstellen, und dann den Bucket auswählen, wenn Sie das Aufnahmeziel erstellen. Sie können sich dafür entscheiden, einen vorhandenen Amazon S3 S3-Bucket in Ihrem zu verwenden AWS-Konto, sofern dieser die folgenden Anforderungen für bestehende Buckets erfüllt:

- AppFabric erfordert aus Sicherheitsgründen, dass sich Ihr Amazon S3 S3-Bucket mit Ihren Amazon S3 S3-Ressourcen befindet. AWS-Region
- Sie können Ihren Bucket mit einer der folgenden Methoden verschlüsseln:
  - Serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3)
  - Serverseitige Verschlüsselung mit AWS Key Management Service (AWS KMS) -Schlüsseln (SSE-KMS) unter Verwendung der Standardeinstellung (). Von AWS verwalteter Schlüssel `aws/s3`

Amazon Data Firehose

Sie können sich dafür entscheiden, Amazon Data Firehose als Ihr Aufnahmeziel AppFabric für Sicherheitsdaten zu verwenden. Um Firehose zu verwenden, können Sie den Firehose-Lieferstream in Ihrem erstellen, AWS-Konto bevor Sie eine Aufnahme erstellen, oder während Sie ein Aufnahmeziel in erstellen. AppFabric Sie können einen Firehose-Lieferstream mithilfe der AWS Management Console, AWS CLI, oder der AWS APIs oder SDKs erstellen. Anweisungen zur Stream-Konfiguration finden Sie in den folgenden Themen:

- AWS Management Console Anleitung — Einen Amazon Data Firehose Delivery Stream erstellen im Amazon Data Firehose Developer Guide
- AWS CLI Anweisungen — create-delivery-streamin der Befehlsreferenz AWS CLI

- AWS Anleitungen zu APIs und SDKs — CreateDeliveryStreamin der Amazon Data Firehose API-Referenz

Die Anforderungen bei der Verwendung von Amazon Data Firehose als Ziel AppFabric für die Sicherheitsausgabe lauten wie folgt:

- Sie müssen den Stream genauso erstellen AWS-Region wie Ihre vier AppFabric Sicherheitsressourcen.
- Sie müssen Direct PUT als Quelle auswählen.
- Hängen Sie Ihrem Benutzer eine AmazonKinesisFirehoseFullAccess AWS verwaltete Richtlinie an, oder weisen Sie Ihrem Benutzer die folgenden Berechtigungen zu:

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

Firehose unterstützt die Integration mit einer Vielzahl von Sicherheitstools von Drittanbietern wie Splunk undLogz.io. Informationen zur ordnungsgemäßen Konfiguration von Amazon Kinesis für die Ausgabe von Daten an diese Tools finden Sie unter Zieleinstellungen im Amazon Data Firehose Developer Guide.

(Optional) Erstellen Sie einen Schlüssel AWS KMS

Bei der Erstellung eines App-Bundles aus AppFabric Sicherheitsgründen wählen Sie einen Verschlüsselungsschlüssel aus oder richten ihn ein, um Ihre Daten sicher vor allen autorisierten Anwendungen zu schützen. Dieser Schlüssel wird verwendet, um Ihre Daten innerhalb des AppFabric Dienstes zu verschlüsseln.

AppFabric Aus Sicherheitsgründen werden Daten standardmäßig verschlüsselt. AppFabric aus Sicherheitsgründen können Sie einen in AppFabric Ihrem Namen AWS-eigener Schlüssel erstellten und verwalteten Schlüssel oder einen vom Kunden verwalteten Schlüssel verwenden, den Sie in AWS Key Management Service (AWS KMS) erstellen und verwalten. AWS-eigene Schlüssel sind

eine Sammlung von AWS KMS Schlüsseln, die ein Benutzer AWS -Service besitzt und verwaltet, sodass sie in mehreren Schlüsseln verwendet AWS-Konten werden können. Vom Kunden verwaltete Schlüssel sind AWS KMS Schlüssel in Ihrem AWS-Konto System, die Sie selbst erstellen, besitzen und verwalten. Weitere Informationen zu AWS-eigene Schlüssel und vom Kunden verwalteten Schlüsseln finden Sie unter Kundenschlüssel und AWS Schlüssel im AWS Key Management Service Entwicklerhandbuch.

Wenn Sie aus Sicherheitsgründen einen vom AppFabric Kunden verwalteten Schlüssel verwenden möchten, um Ihre Daten, z. B. Autorisierungstoken, zu verschlüsseln, können Sie einen mit AWS KMSerstellen. Weitere Informationen zur Berechtigungsrichtlinie, die Zugriff auf Ihren vom Kunden verwalteten Schlüssel gewährt AWS KMS, finden Sie im Abschnitt Schlüsselrichtlinie dieses Handbuchs.

Erste Schritte mit aus AWS AppFabric Sicherheitsgründen

Zu Beginn müssen Sie aus AWS AppFabric Sicherheitsgründen zunächst ein App-Bundle erstellen und dann Anwendungen autorisieren und mit Ihrem App-Bundle verbinden. Nachdem App-Autorisierungen mit Anwendungen verknüpft wurden, können Sie sie AppFabric für Sicherheitsfunktionen wie die Erfassung von Auditprotokollen und den Benutzerzugriff verwenden.

In diesem Abschnitt wird erklärt, wie Sie mit der Verwendung von AppFabric beginnen. AWS Management Console

Themen

- Voraussetzungen
- Schritt 1: App-Bundle erstellen
- Schritt 2: Anwendungen autorisieren
- Schritt 3: Richten Sie die Erfassung von Auditprotokollen ein
- Schritt 4: Verwenden Sie das Benutzerzugriffstool
- Schritt 5: Connect, AppFabric um Sicherheitsdaten in Sicherheitstools und anderen Zielen zu erhalten

Voraussetzungen

Bevor Sie beginnen, müssen Sie zunächst einen Benutzer AWS-Konto und einen Administratorbenutzer erstellen. Weitere Informationen finden Sie unter Melden Sie sich an für ein AWS-Konto und Erstellen Sie einen Benutzer mit Administratorzugriff.

Schritt 1: App-Bundle erstellen

In einem App-Bundle werden alle Autorisierungen und Eingaben Ihrer Apps aus AppFabric Sicherheitsgründen gespeichert. Um ein App-Bundle zu erstellen, richten Sie einen Verschlüsselungsschlüssel ein, um Ihre autorisierten Anwendungsdaten sicher zu schützen.

1. Öffnen Sie die AppFabric Konsole unter https://console.aws.amazon.com/appfabric/.
2. Wählen Sie in der Auswahl „Region auswählen“ in der oberen rechten Ecke der Seite eine aus. AWS-Region AppFabric ist nur in den Regionen USA Ost (Nord-Virginia), Europa (Irland) und Asien-Pazifik (Tokio) verfügbar.
3. Wählen Sie Getting started (Erste Schritte).
4. Auf der Seite Erste Schritte für Schritt 1. App-Bundle erstellen wählen Sie App-Bundle erstellen aus.
5. Richten Sie im Abschnitt Verschlüsselung einen Verschlüsselungsschlüssel ein, um Ihre Daten sicher vor allen autorisierten Anwendungen zu schützen. Dieser Schlüssel wird verwendet, um Ihre Daten innerhalb des AppFabric Sicherheitsdienstes zu verschlüsseln.

   AppFabric Aus Sicherheitsgründen werden Daten standardmäßig verschlüsselt. AppFabric kann einen in AppFabric Ihrem Namen AWS-eigener Schlüssel erstellten und verwalteten Schlüssel oder einen vom Kunden verwalteten Schlüssel verwenden, den Sie in AWS Key Management Service (AWS KMS) erstellen und verwalten.
6. Wählen Sie für AWS KMS Schlüssel entweder Verwenden AWS-eigener Schlüssel oder Vom Kunden verwalteten Schlüssel aus.

   Wenn Sie sich für die Verwendung eines vom Kunden verwalteten Schlüssels entscheiden, geben Sie entweder den Amazon-Ressourcennamen (ARN) oder die Schlüssel-ID des vorhandenen Schlüssels ein, den Sie verwenden möchten, oder wählen Sie AWS KMS Schlüssel erstellen.

   Beachten Sie bei der Auswahl eines AWS-eigener Schlüssel oder eines vom Kunden verwalteten Schlüssels Folgendes:

   - AWS-eigene Schlüsselsind eine Sammlung von AWS Key Management Service (AWS KMS) Schlüsseln, die ein Benutzer AWS -Service besitzt und verwaltet, sodass sie in mehreren Schlüsseln verwendet AWS-Konten werden können. Sie AWS-eigene Schlüssel befinden sich zwar nicht in Ihrem Konto AWS-Konto, aber ein AWS -Service kann sie verwenden AWS-eigener Schlüssel , um die Ressourcen in Ihrem Konto zu schützen. AWS-eigene Schlüssel

werden nicht auf die AWS KMS Kontingente für Ihr Konto angerechnet. Sie müssen den Schlüssel oder seine Schlüsselrichtlinie nicht erstellen oder pflegen. Die Rotation von AWS-eigene Schlüssel variiert je nach Dienst. Informationen zur Rotation eines Forums AWS-eigener Schlüssel finden Sie AppFabric unter Verschlüsselung im Ruhezustand.

- Von Kunden verwaltete Schlüssel sind KMS-Schlüssel in Ihrem AWS-Konto System, die Sie selbst erstellen, besitzen und verwalten. Sie haben die volle Kontrolle über diese AWS KMS Schlüssel. Sie können ihre wichtigsten Richtlinien, AWS Identity and Access Management (IAM-) Richtlinien und Zuschüsse einrichten und verwalten. Sie können sie aktivieren und deaktivieren, ihr kryptografisches Material rotieren, Tags hinzufügen, Aliase erstellen, die auf die AWS KMS Schlüssel verweisen, und das Löschen der AWS KMS Schlüssel planen. Vom Kunden verwaltete Schlüssel werden auf der Seite „Vom Kunden verwaltete Schlüssel“ des AWS Management Console für angezeigt. AWS KMS

  Verwenden Sie den `DescribeKey` Vorgang, um einen vom Kunden verwalteten Schlüssel eindeutig zu identifizieren. Für kundenverwaltete Schlüssel ist der Wert des `KeyManager`-Felds der `DescribeKey`-Antwort `CUSTOMER`. Sie können Ihren vom Kunden verwalteten Schlüssel für kryptografische Operationen verwenden und die Nutzung in AWS CloudTrail Protokollen überprüfen. Bei vielen AWS -Services Integrationen können Sie einen vom Kunden verwalteten Schlüssel angeben AWS KMS, um die für Sie gespeicherten und verwalteten Daten zu schützen. Für vom Kunden verwaltete Schlüssel fallen eine monatliche Gebühr und für die Nutzung, die über das AWS kostenlose Kontingent hinausgeht, eine Gebühr an. Von Kunden verwaltete Schlüssel werden auf die AWS KMS Kontingente für Ihr Konto angerechnet.

Weitere Informationen zu AWS-eigene Schlüssel und vom Kunden verwalteten Schlüsseln finden Sie unter Kundenschlüssel und AWS Schlüssel im AWS Key Management Service Entwicklerhandbuch.

> **Note**
>
> Wenn ein App-Bundle erstellt wird, erstellt es aus AppFabric Sicherheitsgründen auch eine spezielle IAM-Rolle in Ihrer AWS-Konto sogenannten serviceverknüpften Rolle (SLR) für. AppFabric Es ermöglicht dem Service, Metriken an Amazon zu senden CloudWatch. Nachdem Sie ein Audit-Log-Ziel hinzugefügt haben, ermöglicht die SLR dem AppFabric Sicherheitsservice den Zugriff auf Ihre AWS-Ressourcen (Amazon S3

S3-Buckets, Amazon Data Firehose-Lieferstreams). Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AppFabric.

7. (Optional) Bei Tags haben Sie die Möglichkeit, Ihrem App-Bundle Tags hinzuzufügen. Tags sind Schlüssel-Wert-Paare, die den von Ihnen erstellten Ressourcen Metadaten zuweisen. Weitere Informationen finden Sie unter Tagging Your AWS Resources im AWS Tag-Editor-Benutzerhandbuch.
8. Um Ihr App-Bundle zu erstellen, wählen Sie App-Bundle erstellen.

Schritt 2: Anwendungen autorisieren

Nachdem Ihr App-Bundle erfolgreich erstellt wurde, können Sie jetzt aus AppFabric Sicherheitsgründen autorisieren, eine Verbindung herzustellen und mit jeder Ihrer Anwendungen zu interagieren. Autorisierte Anwendungen werden verschlüsselt und in Ihrem App-Bundle gespeichert. Um mehrere App-Autorisierungen pro App-Bundle einzurichten, wiederholen Sie den App-Autorisierungsschritt nach Bedarf für jede Anwendung.

Bevor Sie mit den Schritten zur Autorisierung von Anwendungen beginnen, überprüfen und verifizieren Sie die Voraussetzungen für jede Anwendung, z. B. den benötigten Plantyp, unter. Unterstützte Anwendungen

1. Auf der Seite Erste Schritte für Schritt 2. Anwendungen autorisieren, wählen Sie App-Autorisierung erstellen aus.
2. Wählen Sie im Abschnitt App-Autorisierung aus der Dropdownliste Anwendung die Anwendung aus, der Sie aus AppFabric Sicherheitsgründen die Erlaubnis erteilen möchten, eine Verbindung herzustellen. Bei den angezeigten Anwendungen handelt es sich um diejenigen, die derzeit aus AppFabric Sicherheitsgründen von unterstützt werden.
3. Wenn Sie eine Anwendung auswählen, werden die erforderlichen Informationsfelder angezeigt. Diese Felder enthalten die Mandanten-ID und den Mandantennamen und können auch die Client-ID, den geheimen Clientschlüssel oder das persönliche Zugriffstoken enthalten. Die Eingabewerte für diese Felder variieren je nach Anwendung. Ausführliche anwendungsspezifische Anweisungen, wie Sie diese Werte finden, finden Sie unter. Unterstützte Anwendungen
4. (Optional) Bei Tags haben Sie die Möglichkeit, Ihrer App-Autorisierung Tags hinzuzufügen. Tags sind Schlüssel-Wert-Paare, die den von Ihnen erstellten Ressourcen Metadaten zuweisen. Weitere Informationen finden Sie unter Tagging Your AWS Resources im AWS Tag-Editor-Benutzerhandbuch.

5. Wählen Sie App-Autorisierung erstellen.
6. Wenn ein Popup-Fenster angezeigt wird (abhängig von der Anwendung, mit der eine Verbindung hergestellt wird), wählen Sie Zulassen aus, um aus AppFabric Sicherheitsgründen die Verbindung mit Ihrer Anwendung zu autorisieren.

   Wenn Ihre App-Autorisierung erfolgreich war, wird auf der Seite „Erste Schritte“ eine Erfolgsmeldung mit dem Hinweis „App-Autorisierung verbunden“ angezeigt.
7. Sie können den Status Ihrer App-Autorisierung jederzeit auf der Seite mit den App-Autorisierungen überprüfen, die im Navigationsbereich unter Status für jede Anwendung aufgeführt ist. Der Status Verbunden bedeutet, dass Ihre App-Autorisierung aus Sicherheitsgründen AppFabric für die Verbindung mit der Anwendung erteilt wurde und abgeschlossen ist.
8. Mögliche App-Autorisierungsstatus sind in der folgenden Tabelle aufgeführt, einschließlich der Schritte zur Fehlerbehebung, die Sie ergreifen können, um entsprechende Fehler zu beheben.

Name des Status	Beschreibung des Status	Fehlerbehebungsschritte
Ausstehend	Der Status Ausstehend bedeutet, dass eine App-Autorisierung für die Anwendung erstellt wurde, aber aus AppFabric Sicherheitsgründen noch nicht mit der Anwendung verbunden ist.	Wenn Sie diesen Status sehen, wählen Sie auf der App-Autorisierungsseite im Drop-down-Menü Aktionen die Option Connect aus, um eine Verbindung herzustellen. Wenn dieser Fehler weiterhin besteht, überprüfen Sie, ob der Popup-Blocker Ihres Browsers deaktiviert ist. Wenn im Popup-Fenster eine Fehlermeldung wie 400 Bad Request angezeigt wird, überprüfen Sie, ob alle Informationen wie Mandanten-ID, Client-ID und Client-Schlüssel korrekt eingegeben wurden. Es ist auch

Name des Status	Beschreibung des Status	Fehlerbehebungsschritte
		möglich, dass die App-Autorisierung der Anwendung nicht korrekt erstellt wurde. Weitere Informationen finden Sie unter Unterstützte Anwendungen.
Die Verbindungsüberprüfung ist fehlgeschlagen	Der Status „Verbindungsvalidierung fehlgeschlagen“ bedeutet, dass aus AppFabric Sicherheitsgründen die Verbindung der App-Autorisierung mit einer Anwendung nicht überprüft werden kann.	Stellen Sie sicher, dass alle Informationen, wie Mandanten-ID, Client-ID und Client-Geheimnis, für die App-Autorisierung korrekt eingegeben wurden.
Die automatische Token-Rotation ist fehlgeschlagen	Der Status „Automatische Rotation des Tokens ist fehlgeschlagen“ bedeutet, dass das OAuth-Aktualisierungstoken fehlgeschlagen ist, nachdem die App-Autorisierung erfolgreich hergestellt wurde.	Wenn dieser Fehler weiterhin besteht, überprüfen Sie die Authentifizierungsanwendung der Anwendung. Weitere Informationen finden Sie unter Unterstützte Anwendungen.

9. Um weitere Anwendungen zu autorisieren, wiederholen Sie bei Bedarf die Schritte 1 bis 8.

Schritt 3: Richten Sie die Erfassung von Auditprotokollen ein

Nachdem Sie mindestens eine App-Autorisierung in Ihrem App-Bundle erstellt haben, können Sie nun eine Audit-Log-Ingestion einrichten. Bei der Erfassung von Audit-Logs werden Audit-Logs aus einer autorisierten Anwendung verwendet und im Open Cybersecurity Schema Framework (OCSF) normalisiert. Anschließend werden sie an ein oder mehrere Ziele innerhalb weitergeleitet. AWS Sie können sich auch dafür entscheiden, rohe JSON-Dateien an Ihre Ziele zu liefern.

1. Auf der Seite Erste Schritte für Schritt 3. Wählen Sie im Bereich „Audit-Log-Erfassungen“ die Option „Schnelle Einrichtung von Datenerfassungen“ aus.

   > **Note**
   >
   > Um die Einrichtung zu beschleunigen, verwenden Sie die Schnelleinrichtungsseite Ingestions, auf die Sie nur von der Seite Erste Schritte aus zugreifen können, um Ingestions für mehrere App-Autorisierungen gleichzeitig mit demselben Aufnahmeziel zu erstellen. Zum Beispiel derselbe Amazon S3 S3-Bucket oder Amazon Data Firehose-Datenstream.
   >
   > Sie können Ingestions auch auf der Seite Ingestions erstellen, auf die Sie über den Navigationsbereich zugreifen können. Auf der Seite „Ingestions“ können Sie eine Aufnahme nach der anderen für unterschiedliche Ziele einrichten. Auf der Seite „Ingestions“ können Sie auch ein Tag für eine Aufnahme erstellen. Die folgenden Anweisungen beziehen sich auf die Schnelleinrichtungsseite für Ingestions.

2. Wählen Sie unter App-Autorisierungen auswählen die App-Autorisierungen aus, für die Sie ein Audit-Log-Ingestions erstellen möchten. Die Mandantennamen, die in der Dropdownliste App-Autorisierungen angezeigt werden, sind die Mandantennamen von Anwendungen, für die Sie zuvor aus Sicherheitsgründen eine App-Autorisierung erstellt haben. AppFabric
3. Wählen Sie unter Ziel hinzufügen ein Ziel für die Überwachungsprotokollaufnahmen der ausgewählten Anwendungen aus. Zu den Zieloptionen gehören Amazon S3 — Existing Bucket, Amazon S3 — New Bucket oder Amazon Data Firehose. Wenn Sie mehrere Mandantennamen auswählen, wird das von Ihnen gewählte Ziel auf jede Aufnahme einer App-Autorisierung angewendet.
4. Wenn Sie ein Ziel auswählen, werden zusätzliche Pflichtfelder angezeigt.

   a. Wenn Sie Amazon S3 — Neuer Bucket als Ziel wählen, müssen Sie den Namen des S3-Buckets eingeben, den Sie erstellen möchten. Weitere Anweisungen zum Erstellen eines Amazon S3 S3-Buckets finden Sie unter Ausgabeziel erstellen.

   b. Wenn Sie Amazon S3 — Existing Bucket als Ziel wählen, wählen Sie den Namen des Amazon S3 S3-Buckets aus, den Sie verwenden möchten.

   c. Wenn Sie Amazon Data Firehose als Ziel wählen, wählen Sie den Namen des Lieferstreams aus der Dropdownliste Firehose-Lieferstreamname aus. Weitere Anweisungen zum Erstellen eines Amazon Data Firehose-Lieferdatenstroms finden Sie unter Ausgabeziel erstellen. Beachten Sie auch die AppFabric für die Sicherheit erforderlichen Berechtigungsrichtlinien.

5. Für Schema und Format können Sie wählen, ob Sie Ihre Audit-Logs in Raw — JSON, OCSF — JSON, OCSF — Parquet für Amazon S3-Buckets oder Raw — JSON oder OCSF-JSON für Firehose speichern möchten.

   Das Raw-Datenformat stellt Ihre Audit-Protokolldaten bereit, die aus einer Datenfolge in JSON konvertiert wurden. Das OCSF-Datenformat normalisiert Ihre Auditprotokolldaten auf das AppFabric Open Cybersecurity Schema Framework (OCSF) -Schema aus Sicherheitsgründen. Weitere Informationen zur AppFabric Verwendung von OCSF finden Sie unter. Öffnen Sie das Cybersecurity Schema Framework Sie können jeweils nur einen Schema- und Formatdatentyp für eine Aufnahme auswählen. Wenn Sie ein zusätzliches Schema hinzufügen und den Datentyp formatieren möchten, können Sie ein zusätzliches Aufnahmeziel einrichten, indem Sie den Vorgang zur Erstellung der Aufnahme wiederholen.

6. (Optional) Wenn Sie einer Aufnahme ein Tag hinzufügen möchten, rufen Sie im Navigationsbereich die Seite „Ingestions“ auf. Um zur Seite mit den Aufnahmedetails zu gelangen, wählen Sie den Namen des Mandanten aus. Bei Stichwörtern haben Sie die Möglichkeit, Ihrer Erfassung Stichwörter hinzuzufügen. Tags sind Schlüssel-Wert-Paare, die den von Ihnen erstellten Ressourcen Metadaten zuweisen. Weitere Informationen finden Sie unter Tagging Your AWS Resources im AWS Tag-Editor-Benutzerhandbuch.

7. Wählen Sie „Ingestions einrichten“.

   Wenn Sie eine Erfassung erfolgreich eingerichtet haben, wird auf der Seite „Erste Schritte“ eine Erfolgsmeldung mit dem Hinweis „Erfassung“ erstellt.

8. Sie können den Status Ihrer Ingestionen und den Status Ihrer Aufnahmeziele auch jederzeit auf der Seite Ingestions im Navigationsbereich überprüfen. Auf dieser Seite sehen Sie den Mandantennamen, der bei der Erstellung der App-Autorisierung erstellt wurde, das Ziel und den Status Ihrer Datenerfassungen. Der Status Aktiviert für Ihre Erfassung bedeutet, dass Ihre Aufnahme aktiviert ist. Wenn Sie auf dieser Seite den Mandantennamen einer App-Autorisierung auswählen, wird eine Detailseite für diese App-Autorisierung angezeigt, einschließlich Zieldetails und Status. Der Status Aktiv für Ihr Aufnahmeziel bedeutet, dass das Ziel ordnungsgemäß eingerichtet und aktiv ist. Wenn die App-Autorisierung den Status Verbunden und das Aufnahmeziel den Status Aktiv hat, sollte das Auditprotokoll verarbeitet und übermittelt werden. Wenn der App-Autorisierungsstatus oder der Status des Aufnahmeziels einer der Status Fehlgeschlagen ist, wird das Auditprotokoll auch dann nicht verarbeitet oder zugestellt, wenn der Aufnahmestatus aktiviert ist. Informationen zur Behebung eines Fehlers bei der App-Autorisierung finden Sie in Schritt 2. Autorisieren Sie Anwendungen.

9. In der folgenden Tabelle sind die möglichen Statusangaben für die Aufnahme und das Aufnahmeziel aufgeführt. Sie enthält auch Schritte zur Fehlerbehebung, die Sie ergreifen können, um jeden Fehlerstatus zu korrigieren.

Name des Bundesstaats oder des Status	Beschreibung	Fehlerbehebungsschritte
Deaktiviert	Der Status Deaktiviert für die Aufnahme bedeutet, dass Ihre Aufnahme deaktiviert ist.	Sie können die Aufnahme aktivieren, indem Sie auf der Seite „Ingestions“ im Drop-down-Menü „Aktionen“ die Option Aktivieren auswählen.
Fehlgeschlagen	Der Status Fehlgesch lagen für das Aufnahmez iel bedeutet, dass das Aufnahmeziel das Auditprot okoll nicht akzeptiert. Dieser Status kann beispielsweise aufgrund eines vollen Speicherorts auftreten.	Um diese Probleme zu beheben, rufen Sie die Amazon S3- oder Firehose-Konsolen auf.

Schritt 4: Verwenden Sie das Benutzerzugriffstool

Mit dem Sicherheitstool AppFabric für den Benutzerzugriff können Sicherheits- und IT-Administratorteams schnell herausfinden, wer Zugriff auf bestimmte Anwendungen hat, indem sie eine einfache Suche anhand der Unternehmens-E-Mail-Adresse des Mitarbeiters durchführen. Dieser Ansatz kann hilfreich sein, um den Zeitaufwand für Aufgaben wie die Deprovisionierung von Benutzern zu reduzieren, bei denen der Zugriff eines Benutzers auf SaaS-Anwendungen möglicherweise manuell überprüft oder überwacht werden muss. Wenn ein Benutzer gefunden wird, gibt er aus AppFabric Sicherheitsgründen den Namen des Benutzers in der Anwendung und seinen In-App-Benutzerstatus (z. B. Aktiv) an, sofern er von der Anwendung bereitgestellt wird. AppFabric durchsucht aus Sicherheitsgründen alle autorisierten Anwendungen in einem App-Bundle, um eine Liste der Anwendungen zurückzugeben, auf die der Benutzer Zugriff hat.

1. Auf der Seite „Erste Schritte“ für Schritt 4. Verwenden Sie das Benutzerzugriffstool und wählen Sie Benutzer suchen aus.

2. Geben Sie im Feld E-Mail-Adresse die E-Mail-Adresse eines Benutzers ein und wählen Sie Suchen aus.
3. Im Bereich Suchergebnisse sehen Sie eine Liste aller autorisierten Anwendungen, auf die der Benutzer Zugriff hat. Um den Namen des Benutzers in der Anwendung und seinen Status (falls verfügbar) anzuzeigen, wählen Sie ein Suchergebnis aus.
4. Die Meldung „Benutzer gefunden“ in der Spalte mit den Suchergebnissen bedeutet, dass der Benutzer auf die aufgelistete App zugreifen kann. Die folgende Tabelle zeigt die möglichen Suchergebnisse, Fehler und die Maßnahmen, die Sie zur Behebung der Fehler ergreifen können.

Ergebnis der Suche	Beschreibung
Der Benutzer wurde nicht gefunden	Es wurde kein Benutzer mit der verwendeten E-Mail-Adresse gefunden.
Ein Autorisierungstoken wurde nicht gefunden. Connect die App-Autorisierung für die Anwendung.	Vergewissern Sie sich, dass alle Informati onen, wie Mandanten-ID, Client-ID und Client-Schlüssel, für die App-Autorisierung korrekt eingegeben wurden.
Das Autorisierungstoken wurde gesperrt. Connect die App-Autorisierung für die Anwendung.	Vergewissern Sie sich, dass alle Informati onen, wie Mandanten-ID, Client-ID und Client-Schlüssel, für die App-Autorisierung korrekt eingegeben wurden.
Wir konnten das Autorisierungstoken nicht rotieren. Connect die App-Autorisierung für die Anwendung.	Das OAuth-Aktualisierungstoken ist fehlgeschlagen, nachdem die App-Autor isierung erfolgreich hergestellt wurde. Wenn dieser Fehler weiterhin besteht, überprüfe n Sie die Authentifizierungsanwendung der Anwendung. Weitere Informationen finden Sie unter Unterstützte Anwendungen.
Die erforderlichen Berechtigungen wurden nicht gefunden. Connect die App-Autor isierung für die Anwendung.	Vergewissern Sie sich, dass alle Informati onen, wie Mandanten-ID, Client-ID und Client-Schlüssel, für die App-Autorisierung korrekt eingegeben wurden.

Ergebnis der Suche	Beschreibung
Die App-Autorisierung ist nicht gültig.	Vergewissern Sie sich, dass alle Informationen, wie Mandanten-ID, Client-ID und Client-Schlüssel, für die App-Autorisierung korrekt eingegeben wurden.
Wir konnten die Anwendungs-API aufgrund unzureichender Berechtigungen nicht aufrufen.	Vergewissern Sie sich, dass alle Informationen, wie Mandanten-ID, Client-ID und Client-Geheimnis, für die App-Autorisierung korrekt eingegeben wurden.
Das Limit für Anwendungsanfragen wurde überschritten.	Dies ist eine Fehlermeldung, die von der Anwendung empfangen wurde. Sie können später versuchen, nach einer E-Mail-Adresse zu suchen.
In der Anwendung ist ein interner Serverfehler aufgetreten	Dies ist eine Fehlermeldung, die von der Anwendung empfangen wurde. Sie können später versuchen, nach einer E-Mail-Adresse zu suchen.
In der Anwendung ist ein fehlerhafter Gateway-Fehler aufgetreten	Dies ist eine Fehlermeldung, die von der Anwendung empfangen wurde. Sie können später versuchen, nach einer E-Mail-Adresse zu suchen.
Die Anwendung ist nicht bereit, die Anfrage zu bearbeiten	Dies ist eine Fehlermeldung, die von der Anwendung empfangen wurde. Sie können später versuchen, nach einer E-Mail-Adresse zu suchen.
In der Anwendung ist ein Fehler bei der fehlerhaften Anfrage aufgetreten.	Dies ist eine Fehlermeldung, die wir von der Anwendung erhalten haben. Sie können später erneut versuchen, nach einer E-Mail zu suchen.

Ergebnis der Suche	Beschreibung
In der Anwendung ist ein Fehler aufgetreten, bei dem der Dienst nicht verfügbar ist.	Dies ist eine Fehlermeldung, die wir von der Anwendung erhalten haben. Sie können später erneut versuchen, nach einer E-Mail zu suchen.

Schritt 5: Connect, AppFabric um Sicherheitsdaten in Sicherheitstools und anderen Zielen zu erhalten

Normalisierte (oder rohe) Anwendungsdaten von AppFabric sind mit jedem Tool kompatibel, das die Datenaufnahme von Amazon S3 und die Integration mit Firehose unterstützt, einschließlich Sicherheitstools wieBarracuda XDR,,,Dynatrace,Logz.io, und Netskope NetWitness Rapid7Splunk, oder Ihrer eigenen Sicherheitslösung. Um normalisierte (oder rohe) Anwendungsdaten von zu erhalten AppFabric, folgen Sie den vorherigen Schritten 1 bis 3. Weitere Informationen zur Einrichtung bestimmter Sicherheitstools und -dienste finden Sie unter Kompatible Sicherheitstools und -dienste.

Unterstützte Anwendungen

AWS AppFabric for Security unterstützt die Integration mit den folgenden Anwendungen. Wählen Sie den Namen einer Anwendung, um weitere Informationen darüber zu erhalten, wie Sie die AppFabric Sicherheitseinstellungen für die Verbindung zu dieser Anwendung einrichten.

Themen

- 1Password
- Asana
- Azure Monitor
- Atlassian Confluence
- Atlassian Jira suite
- Box
- Cisco Duo
- Dropbox
- Genesys Cloud

- GitHub
- Google Analytics
- Google Workspace
- HubSpot
- IBM Security® Verify
- JumpCloud
- Microsoft365
- Miro
- Okta
- OneLogin by One Identity
- PagerDuty
- Ping Identity
- Salesforce
- ServiceNow
- Singularity Cloud
- Slack
- Smartsheet
- Terraform Cloud
- Webex by Cisco
- Zendesk
- Zoom

1Password

1Passwordist ein Passwort-Manager, der dir hilft, sichere Passwörter für all deine Online-Konten zu erstellen, zu speichern und zu verwenden. Außerdem schützt er Ihre Daten durch Verschlüsselung, warnt Sie vor Sicherheitsverstößen und ermöglicht es Ihnen, Passwörter auszutauschen.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangen1Password, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für 1Password

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen von1Password.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von 1Password zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über ein aktives kostenpflichtiges 1Password Business- oder Enterprise-Abonnement verfügen. Weitere Informationen finden Sie auf der 1Password Website unter 1PasswordEnterprise.
- Sie müssen über eine Administratorrolle oder einen Teambesitzer für das 1Password Konto verfügen. Weitere Informationen finden Sie auf der 1Password Support-Website unter Gruppen.

Überlegungen zur Ratenbegrenzung

Die 1Password AuditLog Events-API begrenzt Anfragen auf 600 pro Minute und bis zu 30.000 pro Stunde. Bei Überschreitung dieser Grenzwerte wird ein Fehler zurückgegeben. Weitere Informationen finden Sie unter 1PasswordAPI-Ratenbegrenzungen in der 1PasswordEvents-API-Referenz.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem 1Password Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit 1Password autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung 1Password erforderlichen Informationen zu finden. AppFabric

Erstellen Sie ein persönliches 1Password Zugriffstoken

1Passwordunterstützt persönliche Zugriffstoken für öffentliche Kunden. Gehen Sie wie folgt vor, um ein persönliches Zugriffstoken zu generieren.

1. Melden Sie sich bei Ihrem 1Password-Konto an.
2. Wählen Sie im Navigationsbereich Integrationen aus.
3. Wenn bereits Integrationen vorhanden sind, wählen Sie Verzeichnis aus. Andernfalls fahren Sie mit dem nächsten Schritt fort.
4. Wählen Sie unter Integration der Ereignisberichterstattung die Option Andere aus.
5. Geben Sie auf der Seite „Integration hinzufügen“ Ihren SIEM-Systemnamen (Security Information and Event Management) ein (z. B. AppFabric Secure)
6. Wählen Sie „Integration hinzufügen“ und führen Sie dann auf der Seite „Token einrichten“ die folgenden Schritte aus.
    a. Geben Sie den Token-Namen an, der in der AppFabric sicheren Umgebung verwendet werden soll.
    b. Wir empfehlen, dass Sie in der Dropdownliste „Läuft ab“ die Option „Nie“ auswählen. Wenn ein anderer Wert ausgewählt ist, wird das 1Password Token nach Ablauf der Ablaufzeit gesperrt.
    c. Wählen Sie im Abschnitt Zu meldende Ereignisse die Optionen Anmeldeversuche, Artikelnutzungsereignisse und Prüfereignisse aus.
7. Wählen Sie Issue Token aus, um das Token zu erstellen.
8. Wählen Sie Speichern in 1Password und führen Sie die folgenden Schritte aus.
    a. Der Titel wird basierend auf Ihren System- und Token-Namen automatisch ausgefüllt.
    b. Wählen Sie unter Tresor auswählen die Option Privat aus.
    c. Wählen Sie Speichern.

Weitere Informationen finden Sie auf der 1Password Website unter Erste Schritte mit der 1Password Ereignisberichterstattung.

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die angegebene Mieter-ID ist AppFabric Ihre 1Password Anmeldeadresse. Gehen Sie wie folgt vor, um Ihre Mandanten-ID zu finden.

1. Melden Sie sich bei Ihrem 1Password-Konto an.
2. Wählen Sie im Navigationsbereich Settings (Einstellungen) aus.
3. Ihre 1Password Anmeldung ist auf der Seite aufgeführt. Zum Beispiel example-account.1password.com.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige 1Password Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle aus der App-Autorisierung erstellten Dateneingaben zu kennzeichnen.

Dienstkonto-Token

Sie benötigen ein Dienstkonto-Token von einem 1Password Dienstkonto, um an der AppFabric 1Password App-Autorisierung teilnehmen zu können. Wenn Sie kein Dienstkonto-Token haben, gehen Sie wie folgt vor:

AppFabric fordert ein Dienstkonto-Token an. Das Dienstkonto-Token in AppFabric ist das persönliche Zugriffstoken, das Sie erstellt haben. Führen Sie die folgenden Schritte im 1Password-Portal aus, um das persönliche Zugriffstoken zu finden.

1. Wählen Sie Dashboard.
2. Wählen Sie Personen.
3. Wählen Sie den Namen des Kontoinhabers.
4. Wählen Sie Private (Privat) aus.
5. Wählen Sie „Tresor anzeigen“.
6. Wählen Sie Token-Name.

Client-Autorisierung

Erstellen Sie eine App-Autorisierung AppFabric mithilfe der Mandanten-ID, des Mandantennamens und des Dienstkonto-Tokens. Wählen Sie dann Connect, um die Autorisierung zu aktivieren.

Asana

Asanaist eine Work-Management-Plattform, die Einzelpersonen, Teams und Organisationen bei der Orchestrierung ihrer Arbeit unterstützt — von täglichen Aufgaben bis hin zu funktionsübergreifenden strategischen Initiativen. Es bietet ein lebendiges System der Klarheit, in dem jeder kommunizieren, zusammenarbeiten und die Arbeit koordinieren kann. Damit Asana integrieren Teams wichtige Geschäftstools an einem Ort, sodass die Arbeit voranschreitet, egal wo sie stattfindet.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenAsana, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für Asana
- Verbindung AppFabric zu Ihrem Asana Konto herstellen

AppFabric Unterstützung für Asana

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonAsana.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Asana zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie benötigen ein Enterprise-Konto beiAsana. Weitere Informationen zur Erstellung oder zum Upgrade auf ein Asana Enterprise-Konto finden Sie auf der Asana Website unter AsanaEnterprise.
- Sie müssen einen Benutzer mit der Super-Admin-Rolle in Ihrem Asana Konto haben. Weitere Informationen zu Rollen finden Sie unter Admin- und Superadmin-Rollen Asana auf der Asana Website.

Überlegungen zur Ratenbegrenzung

Asanalegt der Asana API Ratenbegrenzungen fest. Weitere Informationen zu den Asana API-Ratenbegrenzungen finden Sie unter Ratenlimits auf der Website des AsanaEntwicklerhandbuchs. Wenn die Kombination aus AppFabric und Ihre vorhandenen Asana Anwendungen das Limit überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Protokollen kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Asana Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Asana autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Asana erforderlichen Informationen zu finden. AppFabric

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die Mandanten-ID in AppFabric wird als Domain-ID in bezeichnetAsana. Verwenden Sie die folgenden Anweisungen auf dem Asana Startbildschirm, um die Domain-ID zu finden:

1. Wählen Sie Ihr Kontoprofilbild und dann Admin-Konsole aus.
2. Wählen Sie dann Einstellungen aus.
3. Scrollen Sie zu den Domain-Einstellungen.
4. Geben Sie die Domain-ID aus diesem Abschnitt in die AppFabric Mandanten-ID-Konfiguration ein.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Asana Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Dienstkonto-Token

Sie benötigen ein Dienstkonto-Token von einem Asana Dienstkonto, um an der AppFabric Asana App-Autorisierung teilnehmen zu können. Wenn Sie kein Dienstkonto-Token haben, gehen Sie wie folgt vor:

1. Folgen Sie den Anweisungen unter Dienstkonten auf der AsanaGuide-Website, um ein Dienstkonto zu erstellen.
2. Kopieren und speichern Sie das Token unten auf der Seite Dienstkonto hinzufügen, wenn Sie die Seite Dienstkonto hinzufügen zum ersten Mal aufrufen.
3. Wenn Sie die Seite Dienstkonto hinzufügen schließen, bevor Sie das Token speichern, müssen Sie Ihr Dienstkonto bearbeiten, ein neues Token generieren und es speichern.

Azure Monitor

Azure Monitorist eine umfassende Überwachungslösung für die Erfassung, Analyse und Beantwortung von Überwachungsdaten aus Ihren Cloud- und lokalen Umgebungen. Sie können Azure Monitor sie verwenden, um die Verfügbarkeit und Leistung Ihrer Anwendungen und Dienste zu maximieren. Es hilft Ihnen, die Leistung Ihrer Anwendungen zu verstehen, und ermöglicht es Ihnen, manuell und programmgesteuert auf Systemereignisse zu reagieren.

Azure Monitorsammelt und aggregiert die Daten aus allen Ebenen und Komponenten Ihres Systems über mehrere Azure- und Nicht-Azure-Abonnements und -Mandanten hinweg. Sie werden auf einer gemeinsamen Datenplattform gespeichert, sodass sie von einem gemeinsamen Satz von Tools genutzt werden können, mit denen die Daten korreliert, analysiert, visualisiert und/oder beantwortet werden können. Sie können auch andere Tools von Microsoft und Drittanbietern integrieren. Das Azure Monitor Aktivitätsprotokoll ist ein Plattformprotokoll, das Einblicke in Ereignisse auf Abonnementebene bietet. Das Aktivitätsprotokoll enthält beispielsweise Informationen darüber, wann eine Ressource geändert oder eine virtuelle Maschine gestartet wurde.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenAzure Monitor, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für Azure Monitor
- Verbindung AppFabric zu Ihrem Azure Monitor Konto herstellen

AppFabric Unterstützung für Azure Monitor

AppFabric ist in der Lage, Benutzerinformationen und Auditprotokolle von den folgenden Azure Monitor Diensten zu empfangen:

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

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Azure Monitor zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie benötigen ein Microsoft Azure Konto mit einer kostenlosen Testversion oder einem pay-as-you-go Abonnement.
- Zum Abrufen der Ereignisse in diesem Abonnement ist mindestens ein Abonnement erforderlich.

Überlegungen zur Ratenbegrenzung

Azure Monitorlegt dem Sicherheitsprinzipal (Benutzer oder Anwendung), der die Anfragen stellt, und der Abonnement-ID oder Mandanten-ID Ratenbegrenzungen fest. Weitere Informationen zu den Azure Monitor API-Ratenbegrenzungen finden Sie auf der Entwickler-Website unter Azure Resource Manager Grundlegendes zur Drosselung von Anfragen. Azure Monitor

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Azure Monitor Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Azure Monitor autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Azure Monitor erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Azure Monitor Verwendung von OAuth2. Gehen Sie wie folgt vor, um eine OAuth2-Anwendung zu erstellen in: Azure Monitor

1. Navigieren Sie zum Microsoft AzurePortal und melden Sie sich an.
2. Navigieren Sie zu Microsoft EntraID.
3. Wählen Sie App-Registrierungen aus.
4. Wählen Sie Neue Registrierung.
5. Geben Sie einen Namen für den Client ein, z. B. Azure Monitor OAuth Client. Dies wird der Name der registrierten Anwendung sein.
6. Stellen Sie sicher, dass die unterstützten Kontotypen auf Single Tenant eingestellt sind.
7. Wählen Sie für den Umleitungs-URI Web als Plattform aus und fügen Sie einen Umleitungs-URI hinzu. Verwenden Sie das folgende Format für die Umleitungs-URI:

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

   In dieser Adresse *<region>* befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

   Die Authentifizierungsantwort wird nach erfolgreicher Authentifizierung des Benutzers an die angegebene URI gesendet. Dies jetzt anzugeben ist optional und kann später geändert werden, aber für die meisten Authentifizierungsszenarien ist ein Wert erforderlich.
8. Wählen Sie Register aus.
9. Wählen Sie in der registrierten App Certificates & Secrets und dann New client secret aus.
10. Fügen Sie eine Beschreibung für das Geheimnis hinzu.
11. Wählen Sie die Ablaufdauer des Geheimnisses aus. Sie können eine beliebige voreingestellte Dauer aus dem Drop-down-Menü auswählen oder eine benutzerdefinierte Dauer festlegen.
12. Wählen Sie Hinzufügen aus. Geheime Client-Werte können nur unmittelbar nach der Erstellung angezeigt werden. Achten Sie darauf, das Geheimnis an einem sicheren Ort zu speichern, bevor Sie die Seite verlassen.

Erforderliche Berechtigungen

Sie müssen Ihrer OAuth-Anwendung die folgenden Berechtigungen hinzufügen. Um Berechtigungen hinzuzufügen, folgen Sie den Anweisungen im Abschnitt Hinzufügen von Berechtigungen für den Zugriff auf Ihre Web-API im Microsoft EntraEntwicklerhandbuch.

- Microsoft GraphBenutzerzugriffs-API > User.Read.All (Delegierten Typ auswählen)
- Microsoft GraphBenutzerzugriffs-API > offline_access (Delegierten Typ auswählen)
- AzureService Management Audit Log API > user_impersonation (wählen Sie den delegierten Typ aus)

Nachdem Sie die Berechtigungen hinzugefügt haben, folgen Sie den Anweisungen im Abschnitt Admin-Zustimmungsschaltfläche im Entwicklerhandbuch, um die Zustimmung des Administrators zu den Berechtigungen zu erteilen. Microsoft Entra

App-Autorisierungen

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen von Ihrem Azure Monitor Konto. Um sowohl Audit-Logs als auch Benutzerdaten von zu erhaltenAzure Monitor, müssen Sie zwei App-Autorisierungen erstellen: eine mit einem Namen Azure Monitorin der Dropdownliste für die App-Autorisierung und eine weitere mit dem Namen Azure MonitorAudit-Logs in der Dropdownliste für die App-Autorisierung. Sie können dieselbe Mandanten-ID, Client-ID und denselben geheimen Clientschlüssel für beide App-Autorisierungen verwenden. Um Audit-Logs von Azure Monitor Ihnen zu erhalten, benötigen Sie Azure Monitorsowohl die Autorisierungen als auch die Azure MonitorAudit Logs-App. Um das Benutzerzugriffstool alleine zu verwenden, ist nur die Azure MonitorApp-Autorisierung erforderlich.

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Gehen Sie wie folgt vor, um Ihre Client-ID in Azure Monitor zu finden:

1. Navigieren Sie zum Microsoft AzurePortal.
2. Navigieren Sie zu Azure Active Directory.
3. Wählen Sie im Abschnitt App-Registrierungen die App aus, die zuvor erstellt wurde.
4. Kopieren Sie im Abschnitt Übersicht die Mandanten-ID aus dem Feld Verzeichnis-ID (Mandanten-ID).

Name des Mandanten

Geben Sie einen Namen ein, der dieses eindeutige Azure Monitor Abonnement identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

> **Note**
>
> Der Mandantenname sollte maximal 2.048 Zeichen lang sein und aus Zahlen, Klein-/Großbuchstaben und den folgenden Sonderzeichen bestehen: Punkt (.), Unterstrich (_), Bindestrich (-) und Leerzeichen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vor, um Ihre Kunden-ID in zu findenAzure Monitor:

1. Navigieren Sie zum Microsoft AzurePortal.
2. Navigieren Sie zu Azure Active Directory.
3. Wählen Sie im Abschnitt App-Registrierungen die App aus, die zuvor erstellt wurde.
4. Kopieren Sie im Abschnitt Übersicht die Client-ID aus dem Feld Anwendungs-ID (Client).

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Das Client-Geheimnis für die registrierte OAuth-App haben Sie in Schritt 11 des Abschnitts zur Erstellung der OAuth-App generiert. Wenn Sie das bei der Erstellung der OAuth-App generierte Client-Geheimnis falsch platzieren, wiederholen Sie die Schritte 8-11 im Abschnitt zur Erstellung der OAuth-App, um ein neues zu generieren.

App-Autorisierung

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Microsoft Azure können. Melden Sie sich im Fenster bei Ihrem Konto an und genehmigen Sie die AppFabric Autorisierung, indem Sie Zulassen wählen.

Atlassian Confluence

Erstelle, arbeite zusammen und organisiere all deine Arbeit an einem Ort. Confluenceist ein Teamarbeitsraum, in dem Wissen und Zusammenarbeit aufeinandertreffen. Dynamische Seiten

bieten Ihrem Team die Möglichkeit, jedes Projekt oder jede Idee zu erstellen, festzuhalten und gemeinsam daran zu arbeiten. Bereiche helfen Ihrem Team dabei, Arbeit zu strukturieren, zu organisieren und gemeinsam zu nutzen, sodass jedes Teammitglied Einblick in das institutionelle Wissen hat und Zugriff auf die Informationen hat, die es benötigt, um seine Arbeit optimal zu erledigen. Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenConfluence, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für Atlassian Confluence

AppFabric unterstützt den Empfang von Auditprotokollen vonAtlassian Confluence.

Voraussetzungen

Damit Sie AppFabric Prüfprotokolle von Atlassian Confluence zu unterstützten Zielen übertragen können, müssen Sie die folgenden Anforderungen erfüllen:

- Um auf die Audit-Logs zugreifen zu können, benötigen Sie ein Standard-, Premium- oder Enterprise-Konto. Weitere Informationen zur Erstellung oder zum Upgrade auf den entsprechenden Confluence Tarif finden Sie auf der Atlassian Website unter ConfluencePreise.
- Um auf die Audit-Logs zugreifen zu können, benötigen Sie Administratorrechte für Ihr Konto. Weitere Informationen zu Rollen finden Sie auf der Atlassian Support-Website unter Benutzern Administratorberechtigungen erteilen.

Überlegungen zur Ratenbegrenzung

Confluencelegt der Atlassian Confluence API Ratenbegrenzungen fest. Wenn die Kombination aus AppFabric und Ihre vorhandenen Atlassian Confluence API-Anwendungen die Grenzwerte überschreiten, AppFabric kann Atlassian Confluence es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Atlassian Confluence Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Atlassian Confluence autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Atlassian Confluence erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Atlassian Confluence Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Atlassian Confluence zu erstellen.

1. Navigieren Sie zur AtlassianDeveloper Console.
2. Wählen Sie oben rechts Ihr Profilsymbol und dann Developer Console.
3. Wählen Sie neben Meine Apps die Option Create, OAuth 2.0-Integration aus.
4. Wählen Sie im linken Navigationsbereich Berechtigungen und dann neben API die Option Hinzufügen aus. Confluence
5. Wählen Sie unter Klassische Bereiche die Option Benutzer lesen (`read:confluence-user`) aus.
6. Wählen Sie unter Granularer Geltungsbereich die Option Auditdatensätze anzeigen () aus. `read:audit-log:confluence`
7. Wählen Sie im linken Navigationsbereich Autorisierung und dann neben OAuth 2.0 (3LO) die Option Hinzufügen aus.
8. Verwenden Sie im Textfeld Rückruf-URL eine Weiterleitungs-URL mit dem folgenden Format und wählen Sie Änderungen speichern aus.

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

   In dieser URL <region>befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet

beispielsweiseus-east-1. Für diese Region lautet die Weiterleitungs-URLhttps://*us-east-1*.console.aws.amazon.com/appfabric/oauth2.

Erforderliche Bereiche

Sie müssen Ihrer Atlassian Confluence OAuth-Anwendung einen der folgenden Bereiche hinzufügen. Weitere Informationen zu Bereichen finden Sie unter Bereiche für OAuth 2.0 (3LO) und Forge-Apps auf der Entwickler-Website. Atlassian Verwenden Sie den klassischen Geltungsbereich, sofern verfügbar.

- Klassische Zielfernrohre:
  - `read:confluence-user`
- Granulierte Zielfernrohre:
  - `read:audit-log:confluence`

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die darin angegebene Mandanten-ID AppFabric ist Ihre Atlassian ConfluenceInstanz-Subdomain. Sie finden Ihre Atlassian ConfluenceInstanz-Subdomain in der Adressleiste Ihres Browsers zwischen https://und. atlassian.net.

Name des Mieters

Geben Sie einen Namen ein, der diese eindeutige Atlassian Confluence Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vorAtlassian Confluence, um Ihre Kunden-ID in zu finden:

1. Navigieren Sie zur AtlassianDeveloper Console.
2. Wählen Sie oben rechts Ihr Profilsymbol und dann Developer Console, Meine Apps.
3. Wählen Sie die OAuth-Anwendung aus, mit der Sie eine Verbindung herstellen. AppFabric

4. Geben Sie die Client-ID von der Seite Einstellungen in das Client-ID-Feld unter ein. AppFabric

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Gehen Sie wie folgt vorAtlassian Confluence, um Ihr Kundengeheimnis in zu finden:

1. Navigieren Sie zur AtlassianDeveloper Console.
2. Wählen Sie oben rechts Ihr Profilsymbol und dann Developer Console, Meine Apps.
3. Wählen Sie die OAuth-Anwendung aus, mit der Sie eine Verbindung herstellen. AppFabric
4. Geben Sie den geheimen Schlüssel von der Seite Einstellungen in das Feld Client Secret unter ein. AppFabric

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Atlassian Confluence können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen.

Atlassian Jira suite

Atlassiansetzt das Potenzial jedes Teams frei. Ihre agile und DevOps IT-Servicemanagement- und Arbeitsmanagement-Software hilft Teams dabei, gemeinsame Arbeit zu organisieren, zu besprechen und abzuschließen. Die Mehrheit der Fortune-500-Unternehmen und über 240.000 Unternehmen aller Größen weltweit — darunter NASA,, KivaDeutsche Bank, und Salesforce — verlassen sich auf Atlassian Lösungen, die ihren Teams helfen, besser zusammenzuarbeiten und qualitativ hochwertige Ergebnisse pünktlich zu liefern. Erfahren Sie mehr über Atlassian ProdukteJira Software,Confluence,Jira Service Management, TrelloBitbucket, und Jira Align unter Atlassian.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten aus dem Jira suite (anderen alsJira Align) empfangen, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose ausgeben.

Themen

- AppFabric Unterstützung für Jira suite
- Verbindung AppFabric zu Ihrem Jira Konto herstellen

AppFabric Unterstützung für Jira suite

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonJira suite, mit Ausnahme vonJira Align.

Voraussetzungen

Für AppFabric die Übertragung von Auditprotokollen von den Jira suite zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über einen Jira Standardplan oder höher verfügen. Weitere Informationen zu den Funktionen der Jira Pläne finden Sie auf den Preisseiten für JiraSoftware, JiraService Management, Jira Work Management und JiraProduct Discovery.
- In Ihrem Jira Konto muss ein Benutzer mit der Rolle „Unternehmensadministrator“ vorhanden sein. Weitere Informationen zu Rollen finden Sie auf der Atlassian Support-Website unter Benutzern Administratorberechtigungen erteilen.

Überlegungen zur Ratenbegrenzung

Die Jira Suite legt Ratenbegrenzungen für die Jira API fest. Weitere Informationen zu den Jira suite API-Ratenbegrenzungen finden Sie unter Ratenbegrenzung auf der Website des AtlassianEntwicklerhandbuchs. Wenn die Kombination von API-Anwendungen AppFabric und Ihre vorhandenen Jira API-Anwendungen das Limit überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Jira Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Jira autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Jira erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Jira suite Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Jira zu erstellen:

1. Navigieren Sie zur AtlassianDeveloper Console.
2. Wählen Sie neben Meine Apps die Option Create, OAuth 2.0-Integration aus.
3. Geben Sie Ihrer App einen Namen und wählen Sie Erstellen.
4. Navigieren Sie zum Abschnitt Autorisierung und wählen Sie neben OAuth 2.0 die Option Hinzufügen aus.
5. Verwenden Sie im Feld Callback-URL eine URL mit dem folgenden Format und wählen Sie Änderungen speichern aus.

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

   In dieser URL <region>befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
6. Navigieren Sie zum Abschnitt Einstellungen, kopieren Sie Ihre Client-ID und Ihren geheimen Client-Schlüssel und speichern Sie sie, um sie für die AppFabric App-Autorisierung zu verwenden.

Erforderliche Bereiche

Sie müssen der Seite „Berechtigungen“ Ihrer Jira OAuth-Anwendung die folgenden Bereiche hinzufügen:

- Unter Klassische Bereiche:
  - JiraAPI > `read:jira-user`
- Unter Granular Scopes:
  - JiraAPI > `read:audit-log:jira`
  - JiraAPI > `read:user:jira`

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die darin angegebene Mandanten-ID AppFabric ist Ihre JiraInstanz-Subdomain. Sie finden Ihre JiraInstanz-Subdomain in der Adressleiste Ihres Browsers zwischen https://und. atlassian.net.

Name des Mieters

Geben Sie einen Namen ein, der diesen eindeutigen Jira Server identifiziert. AppFabricverwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert Ihre Kunden-ID an. Gehen Sie wie folgt vor, um Ihre Kunden-ID in Jira zu finden:

1. Navigieren Sie zur AtlassianDeveloper Console.
2. Wählen Sie die OAuth-Anwendung aus, mit der Sie eine Verbindung herstellen. AppFabric
3. Geben Sie die Client-ID von der Seite Einstellungen in das Client-ID-Feld unter ein. AppFabric

Clientschlüssel

AppFabric fordert Ihr Client-Geheimnis an. Der geheime Eingang des Kunden AppFabric ist der geheime EingangJira. Gehen Sie wie folgt vorJira, um Ihren Secret in zu finden:

1. Navigieren Sie zur AtlassianDeveloper Console.
2. Wählen Sie die OAuth-Anwendung aus, mit der Sie eine Verbindung herstellen. AppFabric
3. Geben Sie den geheimen Schlüssel von der Seite Einstellungen in das Feld Client Secret unter ein. AppFabric

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung erstellt haben, erhalten AppFabric Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Jira können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen.

Box

Boxist die führende Content Cloud, eine zentrale Plattform, die es Unternehmen ermöglicht, den gesamten Inhaltslebenszyklus zu verwalten, von überall aus sicher zu arbeiten und best-of-breed Apps zu integrieren.

Sie können AWS AppFabric damit Auditprotokolle und Benutzerdaten empfangenBox, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für Box

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonBox.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Box zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Um auf die Auditprotokolle zugreifen zu können, benötigen Sie ein aktives kostenpflichtiges Abonnement für die Tarife Business, Business Plus, Enterprise oder Enterprise Plus.
- Sie müssen über einen Benutzer mit Administratorrechten verfügen.
- Sie müssen die 2-Faktor-Authentifizierung für Ihr Box Konto aktiviert haben, um den geheimen Client-Schlüssel der Anwendung auf der Registerkarte Konfiguration anzeigen und kopieren zu können.

Überlegungen zur Ratenbegrenzung

Boxlegt der Box API Ratenbegrenzungen fest. Weitere Informationen zu den Box API-Ratenbegrenzungen finden Sie unter Ratenlimits auf der Website des Box Entwicklerhandbuchs. Wenn die Kombination aus AppFabric und Ihre vorhandenen Box Anwendungen das Limit überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Protokollen kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihren Bestimmungsort geliefert wird. Dies ist auf Verzögerungen bei den Prüfungsereignissen zurückzuführen, die von der Anwendung bereitgestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an AWS Support.

Verbindung AppFabric zu Ihrem Box Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Box autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Box erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Box Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Box zu erstellen. Weitere Informationen finden Sie unter Erstellen einer OAuth-App auf der Website. Box

1. Melden Sie sich bei der Developer Box Console an und rufen Sie sie auf.
2. Wählen Sie Neue App erstellen.
3. Wählen Sie aus der Liste der Anwendungstypen die Option Benutzerdefinierte App aus. Es erscheint ein Modal, das Sie zur Auswahl für den nächsten Schritt auffordert.
4. Geben Sie einen Namen und eine Beschreibung der App ein.
5. Wählen Sie Integration aus der Dropdownliste Zweck aus.
    a. Wählen Sie in der Dropdownliste „Kategorien“ die Option „Sicherheit und Compliance“ aus.
    b. Geben Sie AWS AppFabric Secureim Feld Welches externe System integrieren Sie ein? Textfeld.
6. Wählen Sie Serverauthentifizierung (Client Credentials Grant), wenn Sie die Anwendungsidentität anhand einer Client-ID und eines geheimen Client-Schlüssels überprüfen möchten.
7. Wählen Sie Create app (App erstellen).
8. Wählen Sie die Registerkarte Konfiguration aus.
9. Wählen Sie auf der Seite im Abschnitt App-Zugriffsebene die Option App + Enterprise Access aus.

10. Wählen Sie im Abschnitt Anwendungsbereiche der Seite die Optionen Benutzer verwalten und Unternehmenseigenschaften verwalten aus.
11. Wählen Sie Save Changes.

    Ein Box Administrator muss die Anwendung in der Box Admin-Konsole autorisieren, bevor die Anwendung verwendet werden kann. Gehen Sie wie folgt vor, um eine Autorisierung anzufordern.

    a. Wählen Sie in der Developer Console die Registerkarte Autorisierung für Ihre Anwendung.
    b. Wählen Sie Überprüfen und Absenden, um eine E-Mail zur Genehmigung an Ihren Box Unternehmensadministrator zu senden. Weitere Informationen finden Sie im BoxLeitfaden unter Autorisierung.

    > **Note**
    >
    > Sie müssen Ihre App erneut einreichen, falls nach der Einreichung Änderungen vorgenommen werden.

Erforderliche Bereiche

Die folgenden Anwendungsbereiche sind erforderlich. Weitere Informationen zu Bereichen finden Sie unter Bereiche auf der Box-Dokumentationswebsite.

- Unternehmenseigenschaften verwalten () `manage_enterprise_properties`
- Benutzer verwalten (`manage_managed_users`)

App-Autorisierungen

Tenant-ID

AppFabric fordert eine Mandanten-ID an. Die angegebene Mandanten-ID AppFabric ist die Box Unternehmens-ID. Die Box Enterprise ID finden Sie in der Admin-Konsole unter Konto und Abrechnung > Kontoinformationen > Enterprise ID. Weitere Informationen finden Sie unter Enterprise ID auf der Box-Dokumentationswebsite.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Box Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Daten zu kennzeichnen.

Client-ID und Client-Schlüssel

1. Melden Sie sich bei der Developer Console an Box und gehen Sie zur Developer Console.
2. Wählen Sie im Navigationsmenü Meine Apps aus.
3. Wählen Sie die OAuth-Anwendung aus, mit der Sie eine Verbindung herstellen. AppFabric
4. Wählen Sie die Registerkarte Konfiguration aus.
5. Scrollen Sie auf der Seite zum Abschnitt OAuth 2.0-Anmeldeinformationen.
6. Geben Sie die Client-ID aus Ihrer OAuth-Client-ID in das Client-ID-Feld unter ein. AppFabric
7. Wählen Sie Fetch Client Secret aus.
8. Geben Sie das Client-Geheimnis aus Ihrem OAuth-Clientgeheimnis in das Feld Client Secret ein. AppFabric

Cisco Duo

Cisco Duoschützt vor Sicherheitsverstößen mit einer führenden Access-Management-Suite, die starke, mehrschichtige Schutzmaßnahmen und innovative Funktionen bietet, die legitimen Benutzern den Zugang ermöglichen und böswillige Akteure fernhalten. Für jedes Unternehmen, das Angst vor Sicherheitsverletzungen hat und Cisco Duo schnell eine Lösung benötigt, die hohe Sicherheit bietet und gleichzeitig die Benutzerproduktivität verbessert. Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenCisco Duo, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für Cisco Duo
- Connect AppFabric zu Ihrem Cisco Duo Konto her

AppFabric Unterstützung für Cisco Duo

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonCisco Duo.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Cisco Duo zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Um auf die Auditprotokolle zugreifen zu können, benötigen Sie ein aktives Abonnement für eine Duo Essentials-, Duo Advantage- oder Duo Premier Edition. Alternativ können auch Neukunden mit einer Advantage- oder Premier-Testversion darauf zugreifen. Weitere Informationen zu Cisco Duo Editionen finden Sie unter Editionen und Preise.
- Sie müssen ein Administrator mit der Rolle „Besitzer“ sein, um die Admin-API erstellen oder ändern zu können.
- Sie müssen in der Admin-API die Berechtigungen „Protokollressource gewähren“ hinzufügen, um auf Audit-Logs zugreifen zu können.

Überlegungen zur Ratenbegrenzung

Cisco Duolegt der Cisco Duo API Ratenbegrenzungen fest. Weitere Informationen zu den Cisco Duo API-Ratenbegrenzungen finden Sie unter den Ratenlimits unter Authentifizierungsprotokolle. Wenn die Kombination aus AppFabric und Ihre vorhandenen Cisco Duo API-Anwendungen die Grenzwerte überschreiten, AppFabric kann Cisco Duo es zu Verzögerungen bei der Anzeige von Audit-Logs kommen. Wenden Sie sich an Cisco Duo, wenn Sie eine Erhöhung des Ratenlimits benötigen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Connect AppFabric zu Ihrem Cisco Duo Konto her

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Cisco Duo autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Cisco Duo erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine Cisco Duo Admin-API-Anwendung

AppFabric integriert sich in Cisco Duo die Verwendung eines API-Servicetokens. Gehen Sie wie folgt vorCisco Duo, um eine Anwendung in zu erstellen.

- Um eine Cisco Duo Admin-API-Anwendung zu erstellen, folgen Sie den Anweisungen unter Erste Schritte in der Cisco DuoAdmin-API.

Erforderliche Berechtigungen

Sie müssen Ihrer Cisco Duo Anwendung die folgenden Bereiche hinzufügen:

- Leselogbuch gewähren
- Leseressource gewähren

App-Autorisierungen

Tenant-ID

AppFabric fordert eine Mandanten-ID an. Sie finden die Mandanten-ID im Cisco Duo Hostnamen. Gehen Sie folgendermaßen vorCisco Duo, um den Hostnamen in zu finden.

1. Navigieren Sie zur Cisco DuoAdmin-Anmeldeseite und melden Sie sich an.
2. Navigieren Sie zu Anwendungen und wählen Sie dann Anwendung schützen aus.
3. Suchen Sie in der Anwendungsliste nach dem Eintrag für Admin-API und wählen Sie dann ganz rechts die Option Schützen aus, um Ihre Anwendung zu konfigurieren und Ihren API-Hostnamen abzurufen.
4. Der API-Hostname ist formatiert als`api-`*`<tenant-id>`*`.duosecurity.com`, wobei es sich um die Mandanten-ID *`<tenant-id>`* handelt.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Cisco Duo Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Diensttoken

AppFabric fordert ein Service-Token an. Das Diensttoken ist ein durch Doppelpunkte getrennter Integrationsschlüssel und ein geheimer Schlüssel mit dem folgenden Format.

```
integrationkey:secretkey
```

Gehen Sie wie folgt vor, um Ihren Integrationsschlüssel und Ihren geheimen Schlüssel in Cisco Duo zu finden.

1. Navigieren Sie zur Cisco DuoAdmin-Anmeldeseite und melden Sie sich an.
2. Navigieren Sie zu Anwendungen und wählen Sie dann Anwendung schützen aus.
3. „Klicken Sie auf Eine Anwendung schützen und suchen Sie den Eintrag für die Admin-API in der Anwendungsliste. Klicken Sie ganz rechts auf Schützen, um die Anwendung zu konfigurieren. Scrollen Sie nach unten zum Bereich Bereiche und fügen Sie und hinzu**`Grant read log`**. **`Grant read resource`**

Dropbox

Dropboxhilft Ihrem Unternehmen, bessere Arbeit schneller zu erledigen, indem es Ihre Mitarbeiter zusammenbringt — unabhängig davon, woran sie gerade arbeiten, wo sie arbeiten oder welche Tools sie gerade verwenden. Es ermöglicht Benutzern, Innovation und Effizienz zu beschleunigen, indem es eine einfache und sichere Möglichkeit bietet, Inhalte zu teilen. Dropboxist ein Ort, um das Leben zu organisieren und die Arbeit in Bewegung zu halten. Mit mehr als 700 Millionen registrierten Benutzern in 180 Ländern hat Dropbox sich das Unternehmen zum Ziel gesetzt, eine intelligentere Arbeitsweise zu entwickeln.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenDropbox, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für Dropbox
- Verbindung AppFabric zu Ihrem Dropbox Konto herstellen

AppFabric Unterstützung für Dropbox

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonDropbox.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Dropbox zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über ein Dropbox Geschäftskonto verfügen. Weitere Informationen zum Erstellen eines Geschäftskontos oder zum Upgrade auf ein Dropbox Unternehmenskonto finden Sie auf der Dropbox Website unter DropboxUnternehmen.
- Sie müssen einen Benutzer mit der Rolle Team-Admin in Ihrem Dropbox Konto haben. Weitere Informationen zu Rollen findest du auf der DropboxHelp-Center-Website unter So änderst du die Administratorrechte für dein Dropbox Team.

Überlegungen zur Ratenbegrenzung

Dropboxlegt der Dropbox API Ratenbegrenzungen fest. Weitere Informationen zu den Dropbox API-Ratenbegrenzungen finden Sie unter Ratenlimits auf der DropboxPerformance Guide-Website. Wenn die Kombination von API-Anwendungen AppFabric und Ihre vorhandenen Dropbox API-Anwendungen das Limit überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Dropbox Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Dropbox autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Dropbox erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Dropbox Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Dropbox zu erstellen:

1. Wählen Sie in der App Console unter https://www.dropbox.com/developers/apps die Option Dropbox App erstellen aus.
2. Wählen Sie auf der Seite mit der neuen Anwendungskonfiguration die Option Bereichsbezogener Zugriff für die API aus.
3. Wählen Sie als Nächstes Vollständig als Dropbox Zugriffstyp aus.

4. Geben Sie Ihrer OAuth-Anwendung einen Namen und wählen Sie dann App erstellen, um die anfängliche Einrichtung der OAuth-Anwendung abzuschließen.
5. Fügen Sie auf der Seite mit den Anwendungsinformationen eine Umleitungs-URL mit dem folgenden Format in das Feld OAuth2-Umleitungs-URIs ein.

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

   In dieser URL *<region>* befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
6. Wählen Sie Hinzufügen aus.
7. Kopieren und speichern Sie Ihren App-Schlüssel und Ihren App-Secret zur Verwendung bei der AppFabric App-Autorisierung.
8. Sie können alle anderen Felder auf der Registerkarte Einstellungen mit ihren Standardwerten belassen.

Erforderliche Bereiche

Sie müssen Ihrer Dropbox App über den Tab „Berechtigungen“ auf dem App-Informationsbildschirm die folgenden Bereiche hinzufügen:

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

Wählen Sie Senden, wenn Sie fertig sind.

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Geben Sie einen beliebigen Wert ein, der Ihr Dropbox Konto eindeutig identifiziert, z. B. den Teamnamen.

Name des Mandanten

Geben Sie einen Namen ein, der dieses eindeutige Dropbox Konto identifiziert. AppFabricverwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Die angegebene Client-ID AppFabric ist Ihr Dropbox App-Schlüssel. Gehen Sie wie folgt vor, um Ihren Dropbox-App-Key zu finden:

1. Navigieren Sie zur Dropbox App Console unter https://www.dropbox.com/developers/apps.
2. Suchen Sie die App, mit der Sie eine Verbindung herstellen AppFabric.
3. Suchen Sie den App-Schlüssel im Abschnitt Status auf der Informationsseite der App.
4. Geben Sie den App-Schlüssel für Ihre Dropbox App in das Feld Client-ID unter ein AppFabric.

Clientschlüssel

AppFabric fordert ein geheimes Kundengeheimnis an. Das Client-Geheimnis in AppFabric ist Ihr Dropbox App-Secret. Gehen Sie wie folgt vor, um Ihren geheimen Dropbox App-Schlüssel zu ermitteln:

1. Navigieren Sie zur Dropbox App Console unter https://www.dropbox.com/developers/apps.
2. Suchen Sie die App, mit der Sie eine Verbindung herstellen AppFabric.
3. Suchen Sie auf der Informationsseite der App im Abschnitt Status nach dem geheimen Schlüssel der App.
4. Geben Sie den geheimen App-Schlüssel für Ihre Dropbox App in das Feld Client Secret unter ein AppFabric.

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Dropbox können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen.

Genesys Cloud

Genesys Cloudermöglicht reibungslose Konversationen über digitale Kanäle und Sprachkanäle auf einer einfachen all-in-one Oberfläche. Dies versetzt Unternehmen in die Lage, Mitarbeitern und Kunden außergewöhnliche Erlebnisse zu bieten und die Vorteile schneller Implementierungen, reduzierter Komplexität und einfacher Verwaltung zu nutzen. Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenGenesys Cloud, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für Genesys Cloud

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonGenesys Cloud.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Genesys Cloud zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über ein Genesys Cloud Konto verfügen.
- Sie müssen einen Benutzer mit der Administratorrolle in Ihrem Genesys Cloud Konto haben.

Überlegungen zur Ratenbegrenzung

Genesys Cloudlegt der Genesys Cloud API Ratenbegrenzungen fest. Weitere Informationen zu den Genesys Cloud API-Ratenbegrenzungen finden Sie auf der Genesys Cloud Developer Website unter Ratenbegrenzungen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von

Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Genesys Cloud Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Genesys Cloud autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Genesys Cloud erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Genesys Cloud Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Genesys Cloud zu erstellen:

1. Folgen Sie den Anweisungen unter Einen OAuth-Client erstellen auf der Resource Center-Website. Genesys Cloud

   Wählen Sie für Grant-Typen die Option Code Authorization aus.
2. Verwenden Sie eine Weiterleitungs-URL mit dem folgenden Format als Autorisierte Umleitungs-URIs.

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

   In dieser URL <region>befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
3. Wählen Sie das Feld Umfang aus, um eine Liste der Bereiche anzuzeigen, die für Ihre App verfügbar sind. Wählen Sie Umfang `audits:readonly` und. `users:readonly` Informationen zu Bereichen finden Sie unter OAuth Scopes im Developer Center. Genesys Cloud
4. Wählen Sie Speichern. Genesys Clouderstellt eine Client-ID und ein Client Secret (Token).

Erforderliche Bereiche

Sie müssen Ihrer Genesys Cloud OAuth-Anwendung die folgenden Bereiche hinzufügen:

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

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die angegebene Mandanten-ID AppFabric ist Ihr Genesys Cloud Instanzname. Sie finden Ihre Mandanten-ID in der Adressleiste Ihres Browsers. Zum Beispiel `usw2.pure.cloud` ist die Mandanten-ID in der folgenden URL enthalten`https://login.usw2.pure.cloud`.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Genesys Cloud Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vorGenesys Cloud, um Ihre Kunden-ID in zu finden:

1. Wählen Sie Admin.
2. Wählen Sie unter Integrationen die Option OAuth aus.
3. Wählen Sie den OAuth-Client aus, um die Client-ID zu erhalten.

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Gehen Sie wie folgt vorGenesys Cloud, um Ihr Kundengeheimnis in zu finden:

1. Wählen Sie Admin.
2. Wählen Sie unter Integrationen die Option OAuth aus.
3. Wählen Sie den OAuth-Client aus, um das Client Secret abzurufen.

GitHub

GitHubist eine Plattform und ein cloudbasierter Dienst für Softwareentwicklung und Versionskontrolle mit Git, der es Entwicklern ermöglicht, ihren Code zu speichern und zu verwalten. Es bietet die verteilte Versionskontrolle von Git sowie Zugriffskontrolle, Bugtracking, Softwarefunktionsanfragen,

Aufgabenverwaltung, kontinuierliche Integration und Wikis für jedes Projekt. Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenGitHub, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für GitHub

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonGitHub.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von GitHub zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Um auf die Audit-Logs zugreifen zu können, benötigen Sie ein Unternehmenskonto.
- Um auf die Enterprise-Audit-Logs zugreifen zu können, benötigen Sie die Administratorrolle für Ihr Unternehmenskonto.
- Um Auditprotokolle von der Organisation zu erhalten, müssen Sie Eigentümer der Organisation sein.

Überlegungen zur Ratenbegrenzung

GitHublegt der GitHub API Ratenbegrenzungen fest. Weitere Informationen zu den GitHub API-Ratenlimits finden Sie auf der Website unter API-Anforderungslimits und -zuweisungen. GitHub Wenn die Kombination aus AppFabric und Ihre vorhandenen GitHub API-Anwendungen die GitHub's Grenzwerte überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung bereitgestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten.

Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem GitHub Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit GitHub autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung GitHub erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die GitHub Verwendung von OAuth. Verwenden Sie die folgenden Schritte, um eine OAuth-Anwendung in zu erstellen. GitHub Weitere Informationen finden Sie unter GitHubs Apps erstellen auf der GitHub Website.

1. Wählen Sie Ihr Profilfoto in der oberen rechten Ecke der Seite und dann Einstellungen aus.
2. Wählen Sie im linken Navigationsbereich Entwicklereinstellungen aus.
3. Wählen Sie im linken Navigationsbereich OAuth-Apps aus.
4. Wählen Sie Neue OAuth-App.

> **Note**
>
> Diese Schaltfläche trägt die Bezeichnung Neue Anwendung registrieren, falls Sie noch keine OAuth-App erstellt haben.

5. Geben Sie den Namen Ihrer App in das Textfeld Anwendungsname ein.
6. Geben Sie die vollständige URL der Anwendungsinstanz in das Textfeld Homepage-URL ein.
7. (Optional) Geben Sie eine Beschreibung für Ihre App in das Textfeld Anwendungsbeschreibung ein. Den Benutzern wird diese Beschreibung angezeigt.
8. Geben Sie eine URL mit dem folgenden Format in das Textfeld Authorization Callback URL ein.

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

In dieser URL <region>befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

9. Wählen Sie Gerätefluss aktivieren, wenn Ihre OAuth-App den Gerätefluss verwendet, um Benutzer zu identifizieren und zu autorisieren. Weitere Informationen zum Gerätefluss finden Sie auf der Website unter Autorisieren von OAuth-Apps. GitHub
10. Wählen Sie Anwendung registrieren.

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die Mandanten-ID sollte in einem der folgenden Formate angegeben werden:

Auditprotokoll des Unternehmens:

Verwenden Sie das Auditprotokoll des Unternehmens, wenn Sie Informationen zu den aggregierten Aktionen aller Organisationen erhalten möchten, die Ihrem Unternehmenskonto gehören.

Um das Enterprise-Audit-Log zu verwenden, ist die Mandanten-ID die Unternehmens-ID Ihres Kontos. Sie finden Ihre Unternehmens-ID in der Adressleiste Ihres Browsers. Zum Beispiel *`exampleenterprise`* ist die Unternehmens-ID in der folgenden URL enthaltenhttps://github.com/settings/enterprises/*`examplenterprise`*.

Wenn Sie die Mandanten-ID für das Enterprise Audit Log angeben, müssen Sie ihr ein Präfix voranstellenenterprise:. Geben Sie das vorherige Beispiel daher als anenterprise:examplenterprise.

Auditprotokoll der Organisation:

Verwenden Sie das Auditprotokoll der Organisation als Organisationsadministrator, wenn Sie wissen möchten, welche Aktionen von Mitgliedern Ihrer Organisation ausgeführt wurden. Es enthält Informationen darüber, wer die Aktion ausgeführt hat, um welche Aktion es sich handelt und wann sie ausgeführt wurde.

Um das Auditprotokoll der Organisation zu verwenden, ist die Mandanten-ID Ihre Organisations-ID. Sie finden Ihre Organisations-ID in der Adressleiste Ihres Browsers. Zum Beispiel *`exampleorganization`* ist die Organisations-ID in der folgenden URL enthaltenhttps://github.com/settings/organizations/*`exampleorganization`*.

Wenn Sie die Mandanten-ID für das Auditprotokoll der Organisation angeben, müssen Sie ihr ein Präfix voranstellenorganization:. Geben Sie das vorherige Beispiel daher als anorganization:exampleorganization.

Name des Mandanten

Geben Sie einen Namen ein, der dieses einzigartige GitHub Unternehmen oder diese Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle aus der App-Autorisierung erstellten Datenmengen zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vor, um Ihre Kunden-ID zu finden in GitHub

1. Wählen Sie Ihr Profilfoto in der oberen rechten Ecke der Seite aus und wählen Sie dann Einstellungen.
2. Wählen Sie im linken Navigationsbereich Entwicklereinstellungen aus.
3. Wählen Sie im linken Navigationsbereich OAuth-Apps aus.
4. Wählen Sie die spezifische OAuth-App aus und suchen Sie dann nach dem Client-ID-Wert.

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Gehen Sie wie folgt vor, um Ihr Kundengeheimnis in zu findenGitHub.

1. Wählen Sie Ihr Profilfoto in der oberen rechten Ecke der Seite aus und wählen Sie dann Einstellungen.
2. Wählen Sie im linken Navigationsbereich Entwicklereinstellungen aus.
3. Wählen Sie im linken Navigationsbereich OAuth-Apps aus.
4. Wählen Sie die spezifische OAuth-App aus und suchen Sie dann nach dem Wert Client Secret. Wenn Sie kein vorhandenes Client-Geheimnis finden können, müssen Sie möglicherweise ein neues generieren.

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen GitHub können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen.

Vergewissern Sie sich, dass Ihre Organisationen Zugriff auf die OAuth-App gewährt haben, sofern die Zugriffsbeschränkungen für die OAuth-App aktiviert sind.

Google Analytics

Google Analyticsist ein Webanalysedienst, der Statistiken und grundlegende Analysetools für Suchmaschinenoptimierung (SEO) und Marketingzwecke bereitstellt. Google Analyticswird verwendet, um die Leistung der Website zu verfolgen und Besucherinformationen zu sammeln. Es kann Unternehmen dabei helfen, die wichtigsten Quellen für Nutzer-Traffic zu ermitteln, den Erfolg ihrer Marketingaktivitäten und Kampagnen zu messen, Zielerreichungen (wie Käufe, Hinzufügen von Produkten zum Einkaufswagen) zu verfolgen, Muster und Trends in der Nutzerinteraktion zu entdecken und andere Besucherinformationen wie demografische Daten zu erhalten. Kleine und mittelgroße Einzelhandelswebsites verwenden häufig verschiedene Analysen Google Analytics zum Kundenverhalten, die zur Verbesserung von Marketingkampagnen, zur Steigerung des Webseitenverkehrs und zur besseren Bindung von Besuchern verwendet werden können.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenAzure Monitor, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für Google Analytics

AppFabric unterstützt den Empfang von Auditprotokollen vonGoogle Analytics.

Voraussetzungen

Damit Sie AppFabric Prüfprotokolle von Google Analytics zu unterstützten Zielen übertragen können, müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen Administrator des Google Analytics Kontos sein.
- AppFabric Um Protokolle zu liefern, müssen Sie die Google AnalyticsAdmin-API für Ihr Google Cloud Projekt aktivieren. Achten Sie darauf, ein neues Projekt zu verwenden, wenn Sie die Google Analytics OAuth-Anwendung einrichten.

Überlegungen zur Ratenbegrenzung

Google Analyticslegt der Google Analytics API Ratenbegrenzungen fest. Weitere Informationen zu Google Analytics API-Ratenbegrenzungen finden Sie unter Limits und Kontingente auf der Google Analytics-Website. Wenn die Kombination aus AppFabric und Ihren vorhandenen Google Analytics-API-Anwendungen das Limit überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Google Analytics Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Google Analytics autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Google Analytics erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Google Analytics Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in zu erstellen: Google Analytics

1. Folgen Sie zur Konfiguration Ihres OAuth-Zustimmungsbildschirms den Anweisungen unter Konfiguration des OAuth-Zustimmungsbildschirms im Google Developer Guide auf der Google-Website.
2. Wählen Sie Extern als Benutzertyp
3. Um OAuth-Anmeldeinformationen für zu konfigurieren AppFabric, folgen Sie den Anweisungen im Abschnitt OAuth-Client-ID-Anmeldeinformationen auf der Seite Zugangsdaten erstellen im Google Developer Guide.
4. Verwenden Sie eine Weiterleitungs-URL mit dem folgenden Format.

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

In dieser Adresse *<region>* befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2`.

Erforderliche Bereiche

Sie müssen Ihrer Google Analytics OAuth-Anwendung den folgenden Bereich hinzufügen:

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

App-Autorisierungen

Tenant-ID

AppFabric fordert eine Mandanten-ID an. Die angegebene Mandanten-ID AppFabric ist Ihre Google Analytics Konto-ID.

1. Gehen Sie zur Google AnalyticsStartseite.
2. Wählen Sie im Navigationsbereich Admin aus.
3. Sie finden Ihre Konto-ID unter Konto > Kontoeinstellungen > Kontodetails > Konto-ID.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Google Analytics Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vor, um Ihre Kunden-ID in zu findenGoogle Analytics:

1. Gehen Sie zur Seite mit den Anmeldeinformationen.
2. Wählen Sie im Abschnitt OAuth 2.0-Client-IDs die Client-ID aus, die Sie erstellt haben.
3. Die Client-ID ist im Abschnitt Zusätzliche Informationen auf der Seite aufgeführt.

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Gehen Sie wie folgt vor, um Ihr Kundengeheimnis zu finden inGoogle Analytics:

1. Gehen Sie zur Seite mit den Anmeldeinformationen.
2. Wählen Sie im Abschnitt OAuth 2.0-Client-IDs den Client-Namen aus.
3. Der geheime Client-Schlüssel ist auf der Seite im Abschnitt Client-Geheimnisse aufgeführt.

App-Autorisierung

Nachdem Sie die App-Autorisierung in erstellt haben, erhalten AppFabric Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Google Analytics können. Um die AppFabric Autorisierung zu genehmigen, indem Sie Zulassen wählen.

Google Workspace

Google Workspaceist eine Sammlung von Tools, Software und Produkten für Cloud-Computing, Produktivität und Zusammenarbeit, die von Google entwickelt und vermarktet werden.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenGoogle Workspace, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für Google Workspace
- Verbindung AppFabric zu Ihrem Google Workspace Konto herstellen

AppFabric Unterstützung für Google Workspace

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonGoogle Workspace.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Google Workspace zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen den Google Workspace Enterprise Standard-Plan abonnieren. Weitere Informationen zur Erstellung oder zum Upgrade auf den Google Workspace Enterprise Standard-Plan finden Sie auf der Website mit den Google WorkspacePlänen.
- Sie müssen einen Benutzer mit der Administratorrolle in Ihrem habenGoogle Workspace.
- AppFabric Um Protokolle bereitstellen zu können, müssen Sie die Google Admin SDK-API in Ihrem Google Cloud-Projekt aktivieren. Weitere Informationen finden Sie unter Aktivieren von Google Workspace-APIs im Google WorkspaceEntwicklerhandbuch.

Überlegungen zur Ratenbegrenzung

Google Workspacelegt der Google Workspace API Ratenbegrenzungen fest. Weitere Informationen zu Google Workspace API-Ratenbegrenzungen finden Sie unter Limits and Quotas im Google WorkspaceAdmin-Leitfaden auf der Google Workspace Website. Wenn die Kombination von API-Anwendungen AppFabric und Ihre vorhandenen Google Workspace API-Anwendungen das Limit überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Bei den meisten Prüfungsereignissen kann es zu einer Verzögerung von bis zu 30 Minuten und bei bestimmten Prüfereignissen zu einer Verzögerung von bis zu 4 Stunden kommen. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Weitere Informationen finden Sie unter Datenspeicherung und Verzögerungszeiten auf der Google WorkSpace Admin-Hilfeseite. Dies kann jedoch auf Kontoebene angepasst werden. Für Unterstützung wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Google Workspace Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Google Workspace autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Google Workspace erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Google Workspace Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Google Workspace zu erstellen:

1. Um Ihren OAuth-Zustimmungsbildschirm zu konfigurieren, folgen Sie den Anweisungen unter Konfiguration des OAuth-Zustimmungsbildschirms im Entwicklerhandbuch auf der Google Workspace Website. Google Workspace

   Wählen Sie Intern als Benutzertyp aus.

2. Um OAuth-Anmeldeinformationen für zu konfigurieren AppFabric, folgen Sie den Anweisungen im Abschnitt OAuth-Client-ID-Anmeldeinformationen auf der Seite Zugangsdaten erstellen im Entwicklerhandbuch. Google Workspace

3. Verwenden Sie eine Umleitungs-URL mit dem folgenden Format.

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

   In dieser URL *<region>* befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2`.

Erforderliche Bereiche

Sie müssen Ihrer Google Workspace OAuth-Anwendung die folgenden Bereiche hinzufügen:

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

Wenn Sie diese Bereiche nicht sehen, fügen Sie die Admin-SDK-API zu Ihrer Google Cloud-API-Bibliothek hinzu.

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die angegebene Mandanten-ID AppFabric ist Ihre Google Workspace Projekt-ID. Ihre Projekt-ID finden Sie auf der Hilfeseite zur Google API-Konsole unter Suchen der Projekt-ID.

Name des Mandanten

Geben Sie einen Namen ein, der diesen eindeutigen Namen kennzeichnetGoogle Workspace. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert Ihre Kunden-ID an. Gehen Sie wie folgt vor, um Ihre Kunden-ID zu finden:

1. Finden Sie Ihre Client-ID anhand der Informationen im Abschnitt „Anmeldeinformationen anzeigen“ auf der Seite „Anmeldeinformationen verwalten“ im Google WorkspaceEntwicklerhandbuch.
2. Geben Sie die Client-ID für Ihren OAuth-Client in das Feld Client-ID unter ein. AppFabric

Clientschlüssel

AppFabric fordert Ihr Client-Geheimnis an. Gehen Sie wie folgt vor, um Ihr Kundengeheimnis herauszufinden:

1. Finden Sie Ihren geheimen Client-Schlüssel mithilfe der Informationen im Abschnitt „Anmeldeinformationen anzeigen“ auf der Seite „Anmeldeinformationen verwalten“ im Google WorkspaceEntwicklerhandbuch.
2. Wenn Sie Ihren geheimen Client-Schlüssel zurücksetzen müssen, folgen Sie den Anweisungen im Abschnitt „Geheime Client-Schlüssel zurücksetzen“ auf der Seite „Zugangsdaten verwalten“ im Google WorkspaceEntwicklerhandbuch.
3. Geben Sie Ihr Client-Geheimnis in das Feld Client-Geheimnis unter ein AppFabric.

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung erstellt haben, erhalten AppFabric Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Google Workspace können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen.

HubSpot

HubSpotist eine Kundenplattform mit all der Software, Integrationen und Ressourcen, die Sie benötigen, um Ihr Marketing, Ihren Vertrieb, Ihr Content-Management und Ihren Kundenservice

miteinander zu verbinden. HubSpotDie vernetzte Plattform ermöglicht es Ihnen, Ihr Geschäft schneller auszubauen, indem Sie sich auf das konzentrieren, was am wichtigsten ist: Ihre Kunden. Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenHubSpot, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für HubSpot

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonHubSpot.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von HubSpot zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über ein Konto mit dem Enterprise-Abonnement verfügenHubSpot, um auf Audit-Logs zugreifen zu können. Weitere Informationen zu HubSpot Abonnements finden Sie in der HubSpot Knowledge Base unter HubSpotAbonnement verwalten.
- Sie müssen über ein Entwicklerkonto und eine App verfügen, die mit dem Konto verknüpft ist.
- Sie sollten ein Superadministrator sein, um Apps in Ihrem HubSpot Konto zu installieren, oder über die App Marketplace-Zugriffsberechtigung sowie die Benutzerberechtigungen verfügen, um die Bereiche zu akzeptieren, die die App anfordert.

Überlegungen zur Ratenbegrenzung

HubSpotlegt der HubSpot API Ratenbegrenzungen fest. Weitere Informationen zu den HubSpot API-Ratenbegrenzungen, einschließlich der Beschränkungen für Apps, die OAuth verwenden, finden Sie auf der Website unter Ratenbegrenzungen. HubSpot Wenn die Kombination aus AppFabric und Ihre vorhandenen HubSpot API-Anwendungen die Grenzwerte überschreiten, AppFabric kann HubSpot es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem HubSpot Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit HubSpot autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung HubSpot erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die HubSpot Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in HubSpot zu erstellen:

1. Folgen Sie den Anweisungen im Abschnitt Öffentliche App erstellen in der HubSpot Anleitung auf der HubSpot Website.
2. Fügen Sie auf der Registerkarte Auth die drei Bereiche hinzu, die unter aufgeführt sind. Erforderliche Bereiche
3. Verwenden Sie unter Umleitungs-URL eine Umleitungs-URL mit dem folgenden Format.

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

   In dieser URL <region>befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
4. Wählen Sie App erstellen.

Erforderliche Bereiche

Sie müssen Ihrer HubSpot OAuth-Anwendung die folgenden Bereiche hinzufügen:

- `settings.users.read`
- `crm.objects.owners.read`

- `account-info.security.read`

App-Autorisierungen

Tenant-ID

Geben Sie eine ID ein, die diese eindeutige HubSpot Organisation identifiziert. Geben Sie beispielsweise Ihre HubSpot Konto-ID ein.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige HubSpot Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle aus der App-Autorisierung erstellten Dateneingaben zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vorHubSpot, um Ihre Kunden-ID in zu finden:

1. Navigieren Sie zur HubSpotAnmeldeseite und melden Sie sich mit den Anmeldeinformationen Ihres Entwicklerkontos an.
2. Wählen Sie im Apps-Menü Ihre App aus.
3. Suchen Sie auf der Registerkarte Auth nach dem Client-ID-Wert.

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Gehen Sie wie folgt vorHubSpot, um Ihr Kundengeheimnis in zu finden:

1. Gehen Sie zur HubSpotAnmeldeseite und melden Sie sich mit den Anmeldeinformationen Ihres Entwicklerkontos an.
2. Wählen Sie im Apps-Menü Ihre App aus.
3. Suchen Sie auf der Registerkarte Auth nach dem Wert Client Secret.

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen HubSpot können. Melden Sie sich mit den

Anmeldeinformationen Ihres Unternehmenskontos (nicht mit Ihrem Entwicklerkonto) bei Ihrem Konto an, um die AppFabric Autorisierung zu genehmigen. Wählen Sie „Zulassen“.

IBM Security® Verify

Die IBM Security® Verify Produktreihe bietet automatisierte, cloudbasierte und lokale Funktionen zur Verwaltung der Identitätsverwaltung, zur Verwaltung der Identität und des Zugriffs von Mitarbeitern und Verbrauchern sowie zur Kontrolle privilegierter Konten. Ganz gleich, ob Sie eine Cloud- oder eine On-Premises-Lösung einsetzen müssen, sie IBM Security® Verify hilft Ihnen dabei, Vertrauen aufzubauen und sich vor Insiderbedrohungen für Ihre Belegschaft und Verbraucher zu schützen.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenIBM Security® Verify, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für IBM Security® Verify
- Verbindung AppFabric zu Ihrem IBM Security® Verify Konto herstellen

AppFabric Unterstützung für IBM Security® Verify

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonIBM Security® Verify.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von IBM Security® Verify zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Um auf die Audit-Logs zugreifen zu können, benötigen Sie ein IBM Security® VerifySaaS-Konto.
- Um auf die Audit-Logs zugreifen zu können, benötigen Sie eine Administratorrolle in Ihrem IBM Security® Verify SaaS-Konto.

Überlegungen zur Ratenbegrenzung

IBM Security® Verifylegt der IBM Security® Verify API Ratenbegrenzungen fest. Weitere Informationen zu den IBM Security® Verify API-Ratenbegrenzungen finden Sie in den IBM

Nutzungsbedingungen. Wenn die Kombination aus AppFabric und Ihre vorhandenen IBM Security® Verify API-Anwendungen die IBM Security® Verify Grenzwerte überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihren Bestimmungsort geliefert wird. Dies ist auf Verzögerungen bei den Prüfungsereignissen zurückzuführen, die von der Anwendung bereitgestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an AWS Support.

Verbindung AppFabric zu Ihrem IBM Security® Verify Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit IBM Security® Verify autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung IBM Security® Verify erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die IBM Security® Verify Verwendung von OAuth. Informationen zum Erstellen einer OAuth-Anwendung finden Sie unter Erstellen eines API-Clients auf der IBM Dokumentationswebsite. IBM Security® Verify

1. Verwenden Sie für die Erstanmeldung die Anmelde-URL und die Anmeldeinformationen, die an Ihre registrierte E-Mail-Adresse gesendet wurden.
2. Greifen Sie auf die Verwaltungskonsole unter zu. `https://<hostname>.verify.ibm.com/ui/admin/` Weitere Informationen finden Sie unter Zugriff auf IBM Security® Verify.
3. Wählen Sie in der Verwaltungskonsole unter Sicherheit < API-Zugriff < API-Client die Option Hinzufügen aus.
4. Wählen Sie die folgenden Optionen aus. Diese sind für das Lesen des Auditprotokolls und der Benutzerdetails erforderlich.

   - Berichte lesen
   - Lesen Sie Benutzer und Gruppen
5. Behalten Sie die Standardoption in der Client-Authentifizierungsmethode bei.

   Bearbeiten Sie das Feld Benutzerdefinierte Bereiche nicht.
6. Wählen Sie Weiter aus.

7. Bearbeiten Sie das IP-Filterfeld nicht.
8. Wählen Sie Weiter aus.
9. Bearbeiten Sie das Feld Zusätzliche Eigenschaften nicht.
10. Wählen Sie Weiter aus.
11. Geben Sie einen Namen und eine Beschreibung an. Die Beschreibung ist optional.
12. Wählen Sie „API-Client erstellen“.

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Sie finden die Mandanten-ID in der IBM Security® Verify Standard-URL. In der `https://hostname.verify.ibm.com/` URL ist die Mandanten-ID beispielsweise der *`Hostname`*, der zuvor gefunden wurde `.verify.ibm.com` (oder davor, `ice.ibmcloud.com` wenn Sie einen früheren Hostnamen verwenden). Wenn Sie eine Vanity-URL verwenden, wenden Sie sich an Ihr IBM Security® Verify Support-Team, um Ihre Standard-URL zu erhalten.

Name des Mandanten

Geben Sie einen Namen ein, der diesen eindeutigen IBM Security® Verify Mandanten identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Daten zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vorIBM Security® Verify, um Ihre Kunden-ID in zu finden:

1. Verwenden Sie für die erste Anmeldung die Anmelde-URL und die Anmeldeinformationen, die an Ihre registrierte E-Mail-Adresse gesendet wurden.
2. Greifen Sie auf die Verwaltungskonsole unter zu. `https://<hostname>.verify.ibm.com/ui/admin/` Weitere Informationen finden Sie unter Zugriff auf IBM Security® Verify.
3. Wählen Sie in der Verwaltungskonsole unter Sicherheit < API-Zugriff < API-Client die Auslassungszeichen () neben der jeweiligen OAuth-App aus.
4. Wählen Sie Verbindungsdetails aus.

5. Suchen Sie die Client-ID unter den API-Anmeldeinformationen.

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Gehen Sie wie folgt vorIBM Security® Verify, um Ihr Kundengeheimnis in zu finden:

1. Verwenden Sie für die erste Anmeldung die Anmelde-URL und die Anmeldeinformationen, die an Ihre registrierte E-Mail-Adresse gesendet wurden.
2. Greifen Sie auf die Verwaltungskonsole unter zu. `https://<hostname>.verify.ibm.com/ui/admin/` Weitere Informationen finden Sie unter Zugriff auf IBM Security® Verify.
3. Wählen Sie in der Verwaltungskonsole unter Sicherheit < API-Zugriff < API-Client die Auslassungszeichen () neben der jeweiligen OAuth-App aus.
4. Wählen Sie Verbindungsdetails aus.
5. Suchen Sie unter API-Anmeldeinformationen nach Client Secret.

JumpCloud

JumpCloud Inc. ist ein amerikanisches Unternehmen für Unternehmenssoftware, das eine cloudbasierte Verzeichnisplattform für das Identitätsmanagement anbietet. Es zentralisiert und vereinfacht das Identitätsmanagement und ermöglicht Benutzern den sicheren Zugriff auf ihre Systeme, Apps, Netzwerke und Dateiserver mit einem einzigen Satz von Anmeldeinformationen, unabhängig von Plattform, Protokoll, Anbieter oder Standort.

Sie können AWS verwenden, AppFabric um Auditprotokolle und Benutzerdaten zu empfangen JumpCloud, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format zu normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Kinesis Data Firehose auszugeben.

Themen

- AppFabric Unterstützung für JumpCloud
- Verbindung AppFabric zu Ihrem JumpCloud Konto herstellen

AppFabric Unterstützung für JumpCloud

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonJumpCloud.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von JumpCloud zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über ein aktives kostenpflichtiges JumpCloud Abonnement verfügen. Weitere Informationen finden Sie Select a package that's right for youauf der JumpCloud Website.
- Sie müssen die Rolle „Admins with Billing“ haben.

Überlegungen zur Ratenbegrenzung

JumpCloudveröffentlicht keine Ratenlimits. Sie müssen einen Support-Fall erstellen oder sich an Ihr JumpCloud Kundenteam wenden. Wenn die Kombination aus AppFabric und Ihre vorhandenen JumpCloud API-Anwendungen die JumpCloud's Grenzwerte überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei Prüfereignissen zurückzuführen, die von der Anwendung bereitgestellt werden, und auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem JumpCloud Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit JumpCloud autorisieren. Folgen Sie den Schritten im nächsten Abschnitt AppFabric, um die für die Autorisierung JumpCloud erforderlichen Informationen zu finden.

Erstellen Sie aus dem Konto ein Organisationstoken JumpCloud

AppFabric verwendet einen API-Schlüssel zur Integration mit JumpCloud Um einen API-Schlüssel zu erstellen JumpCloud, gehen Sie wie folgt vor:.

1. Melden Sie sich als Administrator JumpCloud bei Ihrem Konto an.
2. Wählen Sie im Admin-Portal oben rechts Ihre Kontoinitialen aus und wählen Sie im Menü die Option Mein API-Schlüssel aus.
3. Wählen Sie „Neuen API-Schlüssel generieren“ oder wählen Sie einen vorhandenen Schlüssel aus.

> **Note**
>
> JumpClouderlaubt nur einen aktiven API-Schlüssel. Durch das Generieren eines neuen API-Schlüssels wird der Zugriff auf den aktuellen API-Schlüssel widerrufen. Dadurch kann auf alle Aufrufe, die den vorherigen API-Schlüssel verwenden, nicht mehr zugegriffen werden. Sie müssen alle vorhandenen Integrationen, die den vorherigen API-Schlüssel verwenden, mit dem neuen Schlüsselwert aktualisieren.

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Hier wird „Organisations-ID“ die Mandanten-ID sein. Gehen Sie folgendermaßen vor, um die „Organisations-ID“ zu finden.

1. Melden Sie sich bei Ihrem JumpCloud-Konto an.
2. Wählen Sie im Navigationsbereich Einstellungen, dann Organisationsprofil und dann Allgemein aus.
3. Wählen Sie das „Auge“ -Symbol, um die verdeckte Ansicht zu entfernen.
4. Wählen Sie das Symbol „Doppelseite“, um die ID zu kopieren.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige JumpCloud Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Dienstkonto-Token

AppFabric fordert Ihr Dienstkonto-Token an. In AppFabric, das ist das Organisations-API-Token, das Sie weiter oben in Erstellen Sie aus dem Konto ein Organisationstoken JumpCloud diesem Thema erstellt haben.

Microsoft365

Microsoft365 ist eine Produktfamilie von Produktivitätssoftware, Kollaborations- und Cloud-basierten Diensten im Besitz vonMicrosoft.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von Microsoft 365 empfangen, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für 365 Microsoft

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen von Microsoft 365.

Voraussetzungen

Damit Sie AppFabric Prüfprotokolle von Microsoft 365 an unterstützte Ziele übertragen können, müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen einen Microsoft 365 Enterprise-Plan abonnieren. Weitere Informationen zur Erstellung eines 365 Enterprise-Plans oder zum Upgrade auf einen Microsoft 365 Enterprise-Plan finden Sie auf der Microsoft Website unter Microsoft365 Enterprise-Pläne.
- In Ihrem Microsoft 365-Konto muss ein Benutzer mit Administratorrechten vorhanden sein.
- Sie müssen die Auditprotokollierung für Ihre Organisation aktivieren. Weitere Informationen finden Sie unter Auditing auf der Microsoft Website ein- oder ausschalten.

Überlegungen zur Ratenbegrenzung

Microsoft365 legt Ratenbegrenzungen für die Microsoft 365-API fest. Weitere Informationen zu Microsoft 365-API-Ratenbegrenzungen finden Sie unter dienstspezifische Drosselungsgrenzen Microsoft für Graph in der Microsoft Graph-Dokumentation auf der Website. Microsoft Wenn die Kombination aus AppFabric und Ihren vorhandenen Microsoft 365-API-Anwendungen das Limit überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der

Anwendung bereitgestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Microsoft 365-Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie es AppFabric bei Microsoft 365 autorisieren. Gehen Sie wie folgt vor, um die Informationen zu finden AppFabric, die für die Autorisierung von Microsoft 365 erforderlich sind.

Erstellen Sie eine OAuth-Anwendung

AppFabric lässt sich mithilfe von OAuth in Microsoft 365 integrieren. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Microsoft 365 zu erstellen:

1. Folgen Sie den Anweisungen im Abschnitt Eine Anwendung registrieren im Azure Active Directory-Entwicklerhandbuch auf der Microsoft Website.

   Wählen Sie in der Konfiguration Unterstützte Kontotypen die Option Nur Konten in diesem Organisationsverzeichnis aus.
2. Folgen Sie den Anweisungen im Abschnitt Umleitungs-URI hinzufügen im Azure Active Directory-Entwicklerhandbuch.

   Wählen Sie die Webplattform aus.

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

   In dieser URL *<region>* befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

   Sie können die anderen Eingabefelder für die Webplattform überspringen.
3. Folgen Sie den Anweisungen im Abschnitt Einen geheimen Clientschlüssel hinzufügen im Azure Active Directory-Entwicklerhandbuch.

Erforderliche Berechtigungen

Sie müssen Ihrer OAuth-Anwendung die folgenden Berechtigungen hinzufügen. Folgen Sie zum Hinzufügen von Berechtigungen den Anweisungen im Abschnitt Hinzufügen von Berechtigungen für den Zugriff auf Ihre Web-API im Azure Active Directory-Entwicklerhandbuch.

- `Microsoft Graph API>` `User.Read` (automatisch hinzugefügt)
- `Office 365 Management APIs>` `ActivityFeed.Read` (Wählen Sie den delegierten Typ aus)
- `Office 365 Management APIs>` `ActivityFeed.ReadDlp` (Wählen Sie den delegierten Typ aus)
- `Office 365 Management APIs>` `ServiceHealth.Read` (Wählen Sie den delegierten Typ aus)

Nachdem Sie die Berechtigungen hinzugefügt haben, folgen Sie den Anweisungen im Abschnitt Admin-Zustimmungsschaltfläche im Azure Active Directory-Entwicklerhandbuch, um die Zustimmung des Administrators für die Berechtigungen zu erteilen.

App-Autorisierungen

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen von Ihrem Microsoft 365-Konto. Um sowohl Auditprotokolle als auch Benutzerdaten von Microsoft 365 zu erhalten, müssen Sie zwei App-Autorisierungen erstellen, eine mit dem Namen Microsoft365 in der Dropdownliste für die App-Autorisierung und eine weitere mit dem Namen Microsoft365 Audit Log in der Dropdownliste für die App-Autorisierung. Sie können dieselbe Mandanten-ID, Client-ID und denselben geheimen Clientschlüssel für beide App-Autorisierungen verwenden. Um Audit-Logs von Microsoft 365 zu erhalten, benötigen Sie sowohl die Microsoft365- als auch die Microsoft 365 Audit Log-App-Autorisierungen. Um das Benutzerzugriffstool allein zu verwenden, ist nur die Microsoft365-App-Autorisierung erforderlich.

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die angegebene Mandanten-ID AppFabric ist Ihre Azure Active Directory-Mandanten-ID. Informationen zu Ihrer Azure Active Directory-Mandanten-ID finden Sie in der Azure-Produktdokumentation auf der Microsoft Website unter So finden Sie Ihre Azure Active Directory-Mandanten-ID.

Name des Mandanten

Geben Sie einen Namen ein, der dieses eindeutige Microsoft 365-Konto identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert Ihre Kunden-ID an. Die angegebene Client-ID AppFabric ist die Microsoft 365-Anwendungs-ID (Client). Gehen Sie wie folgt vor, um Ihre Microsoft 365-Anwendungs-ID (Client) zu ermitteln:

1. Öffnen Sie die Übersichtsseite für die OAuth-Anwendung, die Sie mit verwenden. AppFabric
2. Die Anwendungs-ID (Client) wird unter Essentials angezeigt.
3. Geben Sie die Anwendungs- (Client-) ID für Ihren OAuth-Client in das Feld Client-ID unter ein. AppFabric

Clientschlüssel

AppFabric fordert Ihr Client-Geheimnis an. Microsoft365 stellt diesen Wert nur bereit, wenn Sie das Client-Geheimnis für Ihre OAuth-Anwendung zunächst erstellen. Gehen Sie wie folgt vor, um ein neues Client-Geheimnis zu generieren, falls Sie noch keines haben:

1. Folgen Sie den Anweisungen im Abschnitt Hinzufügen eines geheimen Client-Schlüssels im Azure Active Directory-Entwicklerhandbuch, um einen geheimen Clientschlüssel zu erstellen.
2. Geben Sie den Inhalt des Wertefeldes in das Feld Clientgeheimnis unter ein AppFabric.

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie von Microsoft 365 ein Popup-Fenster, in dem Sie die Autorisierung genehmigen können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen.

Miro

Miroist ein Online-Arbeitsbereich für Innovation, der es verteilten Teams jeder Größe ermöglicht, das nächste große Ding zu entwickeln. Die unendliche Vielfalt der Plattform ermöglicht es Teams, ansprechende Workshops und Besprechungen abzuhalten, Produkte zu entwerfen, Ideen zu sammeln und vieles mehr. Miro, mit Hauptsitz in San Francisco und Amsterdam, bedient weltweit

mehr als 50 Millionen Nutzer, darunter 99% der Fortune-100-Unternehmen. Mirowurde 2011 gegründet und beschäftigt derzeit mehr als 1.500 Mitarbeiter an 12 Standorten auf der ganzen Welt. Um mehr zu erfahren, besuchen Sie Miro.

Miroumfasst eine umfassende Palette von Funktionen für die Zusammenarbeit, die auf Innovation ausgelegt sind, darunter Diagrammerstellung, Wireframing, Datenvisualisierung in Echtzeit, Moderation von Workshops und integrierte Unterstützung für agile Praktiken, Workshops und interaktive Präsentationen. Mirovor Kurzem wurde Miro KI angekündigt, die die Funktionen Miro um KI-gestützte Kartierung und Diagrammerstellung, Clustering und Zusammenfassung sowie Inhaltsgenerierung erweitert. Miroermöglicht es Unternehmen, die Anzahl der eigenständigen Tools zu reduzieren, wodurch Informationsfragmentierung und Kosten reduziert werden.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenMiro, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für Miro

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonMiro.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Miro zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über einen Miro Enterprise-Plan verfügen. Weitere Informationen zu den Miro-Tarifen finden Sie auf der Seite mit den MiroPreisen auf der Miro Website.
- Sie müssen einen Benutzer mit der Rolle Unternehmensadministrator in Ihrem Miro Konto haben. Weitere Informationen zu Rollen finden Sie im Abschnitt Rollen in Miro auf Unternehmensebene auf der Miro Help Center-Website.
- Ihr Konto muss über ein Enterprise Developer-Team verfügen. Miro Informationen zur Erstellung von Entwicklerteams finden Sie unter Enterprise Developer Teams auf der Miro Help Center-Website.

Überlegungen zur Ratenbegrenzung

Mirolegt der Miro API Ratenbegrenzungen fest. Weitere Informationen zu den Miro API-Ratenbegrenzungen finden Sie unter Ratenbegrenzung im MiroEntwicklerhandbuch auf der Miro Website. Wenn die Kombination aus AppFabric und Ihre vorhandenen Miro API-Anwendungen das Limit überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung bereitgestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Miro Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Miro autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Miro erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Miro Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Miro zu erstellen:

1. Um eine OAuth-Anwendung zu erstellen, folgen Sie den Anweisungen im Abschnitt Apps erstellen und installieren des Artikels Enterprise Developer Teams auf der Miro Help Center-Website.
2. Aktivieren Sie im Dialogfeld zur App-Erstellung das Kontrollkästchen Benutzerautorisierungstoken ablaufen, nachdem Sie ein Entwicklerteam für die Unternehmensorganisation ausgewählt haben.

   > **Note**
   >
   > Sie müssen dies tun, bevor Sie die App erstellen, da Sie diese Option nach dem Erstellen der App nicht mehr ändern können.

3. Geben Sie auf der App-Seite im Abschnitt Umleitungs-URI für OAuth 2.0 eine URL mit dem folgenden Format ein.

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

In dieser URL <region>befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

4. Kopieren und speichern Sie Ihre Client-ID und Ihr Client-Geheimnis, um sie bei der AppFabric App-Autorisierung zu verwenden.

Erforderliche Bereiche

Sie müssen die folgenden Bereiche im `Permissions` Abschnitt Ihrer Miro OAuth-App-Seite hinzufügen:

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

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die angegebene Mandanten-ID AppFabric ist Ihre Miro Team-ID. Informationen darüber, wie Sie Ihre Miro-Team-ID finden, finden Sie im Abschnitt Häufig gestellte Fragen von Ich bin ein neuer Miro Administrator. Wo soll ich anfangen? auf der MiroHelp-Center-Website.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Miro Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert Ihre Kunden-ID an. Gehen Sie wie folgt vor, um Ihre Kunden-ID zu finden:

1. Navigieren Sie zu Ihren Miro Profileinstellungen.

2. Wählen Sie den Tab Deine Apps aus.
3. Wählen Sie die App aus, mit der Sie eine Verbindung herstellen AppFabric.
4. Geben Sie die Client-ID aus dem Abschnitt App-Anmeldeinformationen in das Feld Client-ID unter ein AppFabric.

Clientschlüssel

AppFabric fordert Ihr Kundengeheimnis an. Gehen Sie wie folgt vor, um Ihr Kundengeheimnis herauszufinden:

1. Navigiere zu deinen Miro Profileinstellungen.
2. Wählen Sie den Tab Deine Apps aus.
3. Wählen Sie die App aus, mit der Sie eine Verbindung herstellen AppFabric.
4. Geben Sie den geheimen Client-Schlüssel aus dem Abschnitt App-Anmeldeinformationen in das Feld Client-Geheimnis unter ein AppFabric.

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Miro können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen.

Okta

Oktaist das World's Identity Company. Als führender unabhängiger Identity-Partner gibt Okta es jedem die Möglichkeit, jede Technologie sicher zu nutzen — überall, auf jedem Gerät oder in jeder App. Die vertrauenswürdigsten Marken vertrauen daraufOkta, sicheren Zugriff, Authentifizierung und Automatisierung zu ermöglichen. Da Flexibilität und Neutralität im Mittelpunkt der Okta Workforce Identity und Customer Identity Clouds stehen, können sich Führungskräfte und Entwickler dank anpassbarer Lösungen und mehr als 7.000 vorgefertigter Integrationen auf Innovationen konzentrieren und die digitale Transformation beschleunigen. Oktabaut eine Welt auf, in der Identität Ihnen gehört. Erfahren Sie mehr auf okta .com.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenOkta, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für Okta

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonOkta.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Okta zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie können es AppFabric mit jedem beliebigen Okta Abotyp verwenden.
- Sie müssen einen Benutzer mit der Super-Admin-Rolle in Ihrem Okta Konto haben.
- Der Benutzer, der die App-Autorisierung genehmigt, AppFabric muss auch die Super-Admin-Rolle in Ihrem Okta Konto haben.

Überlegungen zur Ratenbegrenzung

Oktalegt der Okta API Ratenbegrenzungen fest. Weitere Informationen zu den Okta API-Ratenbegrenzungen finden Sie im OktaEntwicklerhandbuch auf der Okta Website unter Ratenlimits. Wenn die Kombination aus AppFabric und Ihre vorhandenen Okta API-Anwendungen die Grenzwerte überschreiten, AppFabric kann Okta es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung bereitgestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Okta Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Okta autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Okta erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Okta Verwendung von OAuth. Um eine OAuth-Anwendung zu erstellen AppFabric, mit der Sie eine Verbindung herstellen können, folgen Sie den Anweisungen unter OIDC-App-Integrationen erstellen auf der Help-Center-Website. Okta Im Folgenden finden Sie Überlegungen zur Konfiguration für: AppFabric

1. Wählen Sie als Anwendungstyp die Option Webanwendung aus.
2. Wählen Sie als Grant-Typ die Optionen Authorization Code und Refresh Token aus.
3. Verwenden Sie eine Umleitungs-URL mit dem folgenden Format als Anmelde-Umleitungs-URI und Abmelde-Umleitungs-URI.

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

   In dieser URL <region>befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
4. Sie können die Trusted Origins-Konfiguration überspringen.
5. Gewähren Sie in der Konfiguration „Kontrollierter Zugriff“ allen Mitgliedern Ihrer Okta Organisation Zugriff.

   > **Note**
   >
   > Wenn Sie diesen Schritt bei der ersten Erstellung der OAuth-Anwendung überspringen, können Sie mithilfe der Registerkarte Zuweisungen auf der Anwendungskonfigurationsseite alle Personen in Ihrer Organisation als Gruppe zuweisen.
6. Sie können alle anderen Optionen mit ihren Standardwerten belassen.

Erforderliche Bereiche

Sie müssen Ihrer Okta OAuth-Anwendung die folgenden Bereiche hinzufügen:

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

App-Autorisierungen

Tenant-ID

AppFabric fordert eine Mandanten-ID an. Die Mandanten-ID in AppFabric ist Ihre Okta Domain. Weitere Informationen zur Suche nach Ihrer Okta Domain finden Sie unter Suchen Sie Ihre Okta Domain im OktaEntwicklerhandbuch auf der Okta Website.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Okta Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle aus der App-Autorisierung erstellten Dateneingaben zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vorOkta, um Ihre Kunden-ID in zu finden:

1. Navigieren Sie zur Okta Entwicklerkonsole.
2. Wählen Sie die Registerkarte Anwendungen.
3. Wählen Sie Ihre Anwendung und dann die Registerkarte Allgemein aus.
4. Scrollen Sie zum Abschnitt Kundenanmeldedaten.
5. Geben Sie die Client-ID Ihres OAuth-Clients in das Feld Client-ID unter ein. AppFabric

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Gehen Sie wie folgt vorOkta, um Ihr Kundengeheimnis in zu finden:

1. Navigieren Sie zur Okta Entwicklerkonsole.
2. Wählen Sie die Registerkarte Anwendungen.
3. Wählen Sie Ihre Anwendung und dann die Registerkarte Allgemein aus.
4. Scrollen Sie zum Abschnitt Kundenanmeldedaten.
5. Geben Sie den geheimen Clientschlüssel aus Ihrer OAuth-Anwendung in das Feld Client Secret unter ein. AppFabric

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Okta können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen. Der Benutzer, der die Okta Autorisierung genehmigt, muss über Super-Admin-Rechte verfügen. Okta

OneLogin by One Identity

OneLogin by One Identityist eine moderne, cloudbasierte Access-Management-Lösung, die alle digitalen Identitäten für Ihre Belegschaft, Kunden und Partner nahtlos verwaltet. OneLoginbietet sicheres Single Sign-On (SSO), Multi-Faktor-Authentifizierung (MFA), adaptive Authentifizierung, MFA auf Desktop-Ebene, Verzeichnisintegration mit AD, LDAP, G Suite und anderen externen Verzeichnissen, Identity Lifecycle Management und vieles mehr. Mit können Sie Ihr Unternehmen vor den häufigsten Angriffen schützenOneLogin, was zu mehr Sicherheit, reibungslosem Benutzererlebnis und der Einhaltung gesetzlicher Anforderungen führt. Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenOneLogin, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für OneLogin by One Identity

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonOneLogin by One Identity.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von OneLogin by One Identity zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über ein OneLogin Advanced- oder Professional-Konto verfügen.
- Sie müssen über einen Benutzer mit Administrator-/Delegierten Administratorrechten verfügen.

Überlegungen zur Ratenbegrenzung

OneLogin by One Identitylegt der OneLogin API Ratenbegrenzungen fest. Weitere Informationen zu den OneLogin API-Ratenlimits finden Sie unter Get Rate Limit in der OneLoginAPI-Referenz. Wenn die Kombination aus AppFabric und Ihre vorhandenen OneLogin API-Anwendungen die Grenzwerte überschreiten, AppFabric kann OneLogin es zu Verzögerungen bei der Anzeige von Audit-Logs kommen. Das OneLogin Ratenlimit kann jedoch erhöht werden. Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren OneLogin by One Identity Account Manager oder wenden Sie sich an One Identity.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem OneLogin by One Identity Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit OneLogin by One Identity autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung OneLogin erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die OneLogin by One Identity Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in OneLogin zu erstellen:

1. Navigieren Sie zur OneLoginAnmeldeseite und melden Sie sich an.
2. Wählen Sie im Menü Entwickler die Option API-Anmeldeinformationen aus.
3. Wählen Sie Neue Anmeldeinformationen, geben Sie einen Namen für Ihre neuen Anmeldeinformationen ein und wählen Sie dann Alle lesen aus.
4. Wählen Sie „Speichern“. OneLoginerstellt eine Client-ID und einen geheimen Clientschlüssel.

Erforderliche Bereiche

Sie müssen Ihrer OneLogin by One Identity OAuth-Anwendung die folgenden Bereiche hinzufügen:

- Lesen Sie alles. Weitere Informationen zu Bereichen und Client-Anmeldeinformationen finden Sie unter Arbeiten mit API-Anmeldeinformationen in der OneLoginAPI-Referenz.

App-Autorisierungen

Tenant-ID

AppFabric fordert eine Mandanten-ID an. Die darin angegebene Mandanten-ID AppFabric ist Ihre Instanz-Subdomain. Sie finden Ihre Mandanten-ID in der Adressleiste Ihres Browsers. Zum Beispiel `subdomain` ist die Mandanten-ID in der folgenden URL enthaltenhttps://*subdomain*.onelogin.com.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige OneLogin by One Identity Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vorOneLogin by One Identity, um Ihre Kunden-ID in zu finden:

1. Navigieren Sie zur OneLoginAnmeldeseite und melden Sie sich an.
2. Wählen Sie im Menü Entwickler die Option API-Anmeldeinformationen aus.
3. Wählen Sie die API-Anmeldeinformationen aus, um die Client-ID zu erhalten.

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Gehen Sie wie folgt vorOneLogin by One Identity, um Ihr Kundengeheimnis in zu finden:

1. Navigieren Sie zur OneLoginAnmeldeseite und melden Sie sich an.
2. Wählen Sie im Menü Entwickler die Option API-Anmeldeinformationen aus.
3. Wählen Sie die API-Anmeldeinformationen aus, um das Client Secret abzurufen.

Autorisierung der Client-App

Erstellen Sie in AppFabric eine App-Autorisierung mit Ihrer Mandanten-ID und Ihrem Namen sowie Ihrer Kunden-ID und Ihrem Namen. Wählen Sie Verbinden, um die Autorisierung zu aktivieren.

PagerDuty

PagerDutyist eine digitale Operationsmanagement-Plattform, die Teams dabei unterstützt, Probleme zu minimieren, die sich auf Kunden auswirken, indem sie jedes Signal in Maßnahmen umsetzen, sodass Sie Probleme schneller lösen und effizienter arbeiten können. Integriert inCloudWatch,GuardDuty, CloudTrail und. Personal Health Dashboard Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenPagerDuty, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für PagerDuty

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonPagerDuty.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von PagerDuty zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Um auf die Audit-Logs zugreifen zu können, benötigen Sie einen PagerDuty Business - oder Digital Operations-Plan.
- Sie sollten ein globaler Administrator oder Kontoinhaber des PagerDuty Kontos sein.

Überlegungen zur Ratenbegrenzung

PagerDutylegt der PagerDuty API Ratenbegrenzungen fest. Weitere Informationen zu den PagerDuty API-Ratenbegrenzungen finden Sie unter REST-API-Ratenlimits auf der PagerDuty Entwicklerplattform. Wenn die Kombination aus AppFabric und Ihre vorhandenen PagerDuty API-Anwendungen die Grenzwerte überschreiten, AppFabric kann PagerDuty es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem PagerDuty Konto herstellen

Die PagerDuty Plattform unterstützt API-Zugriffsschlüssel. Gehen Sie wie folgt vor, um einen API-Zugriffsschlüssel zu generieren.

Erstellen Sie einen API-Zugriffsschlüssel

AppFabric lässt sich in PagerDuty die Verwendung eines API-Zugriffsschlüssels für öffentliche Kunden integrieren. Gehen Sie wie folgt vorPagerDuty, um einen API-Zugriffsschlüssel in zu erstellen:

1. Navigieren Sie zur PagerDutyAnmeldeseite und melden Sie sich an.
2. Wählen Sie Integrationen, API-Zugriffsschlüssel.
3. Wählen Sie Neuen API-Schlüssel erstellen.
4. Geben Sie eine Beschreibung ein und wählen Sie dann Read-Only API Key aus.
5. Klicken Sie auf Create key (Schlüssel erstellen).
6. Kopieren und speichern Sie den API-Schlüssel. Sie werden ihn später benötigen AppFabric. Wenn Sie die Seite schließen, bevor Sie den API-Schlüssel speichern, müssen Sie einen neuen API-Schlüssel generieren und speichern. Dieser Schlüssel sollte dafür vorgesehen sein, um AppFabric zu verhindern, dass das PagerDuty API-Ratenlimit mit Ihren anderen Integrationen geteilt wird.

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die Mandanten-ID für Ihr PagerDuty Konto ist die Basis-URL Ihres Kontos. Sie finden diese, indem Sie sich in die Adressleiste Ihres Webbrowsers einloggen PagerDuty und sie aus der Adressleiste kopieren. Die Mandanten-ID sollte einem der folgenden Formate entsprechen:

- Für US-Konten *subdomain*.pagerduty.com
- Für EU-Konten *subdomain*.eu.pagerduty.com

Name des Mieters

Geben Sie einen Namen ein, der diese eindeutige PagerDuty Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Dienstkonto-Token

AppFabric fordert Ihr Dienstkonto-Token an. Das Dienstkonto-Token in AppFabric ist der API-Zugriffsschlüssel, in dem Sie erstellt habenErstellen Sie einen API-Zugriffsschlüssel.

Ping Identity

Wir bei glauben daranPing Identity, digitale Erlebnisse für alle Benutzer sowohl sicher als auch nahtlos zu gestalten, ohne Kompromisse einzugehen. Aus diesem Grund entscheiden sich mehr als die Hälfte der Fortune-100-Unternehmen dafür, digitale Interaktionen für ihre Nutzer Ping Identity zu schützen und gleichzeitig für reibungslose Erlebnisse zu sorgen. Am 23. August 2023 haben sie ForgeRock sich zusammengeschlossen, um Kunden Ping Identity und Partnern mehr Auswahl, tieferes Fachwissen und eine umfassendere Identitätslösung zu bieten. Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenPing Identity, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für Ping Identity
- Verbindung AppFabric zu Ihrem Ping Identity Konto herstellen

AppFabric Unterstützung für Ping Identity

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonPing Identity.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Ping Identity zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über ein Essential-, Plus- oder Ping Identity Premium-Konto verfügen. Weitere Informationen zur Erstellung oder zum Upgrade des entsprechenden Ping Identity Plantyps finden Sie auf der Ping Identity Website unter Ping IdentityPreise für alle Funktionen.
- In Ihrem Ping Identity Konto müssen Sie die Rolle „Nur Lesen“ für Identitätsdaten haben. Sie können Ihrem Konto Rollen hinzufügen, indem Sie Rollen für Ihre Anwendung zuweisen. Weitere Informationen zu Rollen finden Sie auf der Ping Identity Support-Website unter Rollen.

Überlegungen zur Ratenbegrenzung

Ping Identityveröffentlicht keine Ratenlimits. Sie müssen einen Support-Fall erstellen oder sich an Ihr Ping Identity Kundenerfolgsteam wenden. Wenn die Kombination aus AppFabric und Ihre vorhandenen Ping Identity API-Anwendungen die Grenzwerte überschreiten, AppFabric kann Ping Identity es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Ping Identity Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Ping Identity autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Ping Identity erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Ping Identity Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Ping Identity zu erstellen:

1. Folgen Sie den Anweisungen im Abschnitt Anwendungsverbindung erstellen im Handbuch PingOnefür Entwickler auf der Ping Identity Website.
2. Nachdem Sie den Antrag erstellt haben, passen Sie die Zuschussarten an.

    a. Wenn Sie bei der Anwendung angemeldet sind, wählen Sie die Registerkarte Konfiguration und klicken Sie auf das Stiftsymbol, um Änderungen an der vorhandenen Konfiguration vorzunehmen.

b. Wählen Sie unter Art der Gewährung die Option Autorisierungscode aus. Behalten Sie die PKCE-Durchsetzung als OPTIONAL bei.

c. Wählen Sie Refresh Token und wählen Sie Ihre Aktualisierungsdauer aus.

3. Verwenden Sie unter Umleitungs-URL/Rückruf-URL eine Umleitungs-URL mit dem folgenden Format.

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

In dieser URL <region>befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die angegebene Mandanten-ID AppFabric ist Ihr Ping Identity Instanzname. Sie finden Ihre Mandanten-ID in der Adressleiste Ihres Browsers. z. B. *API_PATH*`/v1/environments/`*environmentID*. Where *API_PATH* steht für die regionale Domäne des PingOne Servers, z. B.`api.pingone.com`, und *environmentID* steht für Ihre Umgebungs-ID, die in den Eigenschaften Ihrer Anwendungsumgebung angegeben ist. Weitere Informationen zu Umgebungseigenschaften finden Sie auf der Ping Identity Website unter Umgebungseigenschaften.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Ping Identity Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vorPing Identity, um Ihre Kunden-ID in zu finden:

1. Melden Sie sich bei der PingOne Admin-Konsole an und wählen Sie Anwendungen.
2. Wählen Sie die Anwendung aus der Liste aus.

3. Wählen Sie die Registerkarte Übersicht und suchen Sie dann nach dem Client-ID-Wert.

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Gehen Sie wie folgt vorPing Identity, um Ihr Kundengeheimnis in zu finden:

1. Melden Sie sich bei der PingOne Admin-Konsole an und wählen Sie Anwendungen.
2. Wählen Sie die Anwendung aus der Liste aus.
3. Wählen Sie die Registerkarte Overview und suchen Sie dann nach dem Wert Client Secret.

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Ping Identity können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen.

Salesforce

Salesforcestellt cloudbasierte Software her, die Unternehmen dabei unterstützt, mehr Interessenten zu finden, mehr Geschäfte abzuschließen und Kunden mit fantastischem Service zu begeistern. Salesforce's Customer 360 bietet eine komplette Produktsuite, vereint Vertriebs-, Service-, Marketing-, Handels- und IT-Teams mit einer einzigen, gemeinsamen Ansicht von Kundeninformationen und hilft Unternehmen dabei, die Beziehungen zu Kunden und Mitarbeitern gleichermaßen auszubauen. Sie können AWS AppFabric damit Auditprotokolle und Benutzerdaten empfangenSalesforce, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für Salesforce
- Verbindung AppFabric zu Ihrem Salesforce Konto herstellen

AppFabric Unterstützung für Salesforce

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonSalesforce.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Salesforce zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie benötigen eine Performance-, Enterprise- oder Unlimited-Edition vonSalesforce. Wenden Sie sich Salesforce an, um auf eine dieser Editionen zu aktualisieren.
- Wenn Sie stündlich Ereignisprotokolldateien mit einem vollständigen Satz von Protokollereignissen AppFabric übertragen möchtenSalesforce, müssen Sie Event Monitoring als Teil der Shield-Funktionen von abonnierenSalesforce. Andernfalls AppFabric werden begrenzte Ereignisse (d. h. Anmeldung, Abmeldung, API Gesamtnutzung InsecureExternalAssets, CORS Verletzung und HostnameRedirects ELF Ereignisse) aus der täglichen Salesforce's Standardprotokolldatei übertragen. Sie können überprüfen, ob Ihr Salesforce Konto bereits Shield-Funktionen abonniert hat, indem Sie zu Setup > Event Manager gehen. Wenn Sie 19 oder mehr Ereignisse aufgelistet sehen, hat Ihr Konto die Ereignisüberwachung abonniert. Wenn Sie Event Monitoring nicht haben, können Sie ein Abonnement für dieses Add-on erwerben, indem Sie sich an uns wendenSalesforce.
- Sie müssen sich in den Salesforce Einstellungen für die Generierung von Ereignisprotokolldateien anmelden.
- Sie sollten das Systemadministratorprofil verwenden, um eine OAuth Anwendung zu erstellen und sich mit denselben Anmeldeinformationen für AppFabric anzumelden.

> **Note**
>
> Die Ereignisse API Total UsageCORS, Violation Record, Hostnamen-Weiterleitungen, Unsichere externe Ressourcen, Anmeldung und Abmeldung sind in den unterstützten Editionen von ohne zusätzliche Kosten verfügbar. Salesforce Wenden Sie sich anSalesforce, um die übrigen Ereignistypen zu erwerben. Weitere Informationen zu Salesforce Ereignistypen finden Sie auf der Salesforce Website unter EventLogFile Unterstützte Ereignistypen.
>
> AppFabric kann bis zu 100.000 Ereignisse pro Ereignistyp und Protokolldatei-Instanz unterstützen (täglich oder stündlich, abhängig vom Event Monitoring-Add-On-Abonnement). Eine Protokolldatei, die den Schwellenwert überschreitet, kann dazu führen, dass die gesamte Protokolldatei von der Aufnahme ausgeschlossen wird.

Überlegungen zur Ratenbegrenzung

Salesforcelegt Ratenbegrenzungen für die Salesforce API fest. Weitere Informationen zu den Salesforce API Ratenlimits finden Sie auf der Website unter APIAnforderungslimits und Zuteilungen. Salesforce Wenn die Kombination aus AppFabric und Ihre vorhandenen Salesforce API Anwendungen die Salesforce's Grenzwerte überschreiten, AppFabric kann es sein, dass die Audit-Logs verzögert angezeigt werden.

Überlegungen zur Datenverzögerung

Möglicherweise kommt es bei der täglichen Protokolldatei zu einer Verzögerung von bis zu 6 Stunden oder zu einer Verzögerung von bis zu 29 Stunden bei der stündlichen Protokolldatei, wenn ein Prüfereignis an Ihr Ziel übermittelt wird. Dies ist auf Verzögerungen bei den von der Anwendung bereitgestellten Prüfereignissen sowie auf Vorkehrungen zur Reduzierung von Datenverlusten zurückzuführen. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Salesforce Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Salesforce autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Salesforce erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine Anwendung OAuth

AppFabric integriert sich in die Salesforce VerwendungOAuth. Gehen Sie wie folgt vorSalesforce, um eine OAuth Anwendung in zu erstellen:

1. Loggen Sie sich in Ihr Salesforce Konto ein.
2. Gehen Sie zur Einrichtungsseite, wie in der SalesforceDokumentation beschrieben.
3. Suchen Sie in der Schnellsuche nach App Manager.
4. Wählen Sie „Neue verbundene App“.
5. Geben Sie die erforderlichen Informationen in die Formularfelder ein.
6. Wählen Sie OAuthEinstellungen aktivieren.
7. Stellen Sie sicher, dass Sie die folgenden Optionen ausschalten:
    - Proof Key für die Erweiterung Code Exchange (PKCE) für unterstützte Autorisierungsabläufe erforderlich

- Für den Webserver-Flow ist ein geheimer Schlüssel erforderlich
- Für Refresh Token Flow ist ein geheimer Schlüssel erforderlich

8. Geben Sie in das URLCallback-Textfeld einen Wert URL mit dem folgenden Format ein und wählen Sie Änderungen speichern aus.

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

Darin URL *<region>* ist der Code für den, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region URL lautet die Umleitung`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

9. Füllen Sie die Bereiche nach Bedarf aus (im folgenden Erforderliche Bereiche Abschnitt beschrieben). Alle anderen Felder können mit ihren Standardwerten belassen werden.
10. Wählen Sie Save (Speichern) aus.
11. Gehen Sie wie folgt vor, um die Aktualisierungstoken-Richtlinie für die neue OAuth App zu überprüfen:

    a. Geben Sie auf der Einrichtungsseite im Textfeld „Schnellsuche“ den Text Verbundene Apps ein und wählen Sie dann Verbundene Apps verwalten aus.

    b. Wählen Sie neben der neu erstellten App die Option Bearbeiten aus.

    c. Stellen Sie sicher, dass das Aktualisierungstoken gültig ist, bis die Option „Widerruf“ ausgewählt ist.

    d. Speichern Sie Ihre Änderungen.

12. Gehen Sie wie folgt vor, um sicherzustellen, dass Audit-Logs generiert werden:

    a. Geben Sie auf der Setup-Seite in das Textfeld „Schnellsuche“ den Text Event Log File ein und wählen Sie dann Event Log File Browser aus.

    b. Vergewissern Sie sich, dass die Ereignisprotokolle im Browser für die Ereignisprotokolldatei aufgeführt sind.

13. Navigieren Sie zu der erstellten App und wählen Sie im Drop-down-Menü die Option Ansicht aus.
14. Wählen Sie Verbraucherdaten verwalten aus.

    Sie werden zu einem neuen Tab weitergeleitet, auf dem Sie Ihre Identität überprüfen müssen. Notieren Sie sich auf dieser Registerkarte die Werte für Consumer Key und Consumer Secret. Sie benötigen diese später, um sich anzumelden.

Erforderliche Bereiche

Sie müssen Ihrer Anwendung die folgenden Bereiche hinzufügen SalesforceOAuth:

- Benutzerdaten verwalten über APIs (`API`).
- Anfrage jederzeit ausführen (`refresh_token`und`offline_access`).

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die Mieter-ID in AppFabric ist die Subdomain Ihrer Salesforce My Domain. Sie finden Ihre My Domain-Subdomain in der Adressleiste Ihres Browsers zwischen und`https://`. `.my.salesforce.com`

Verwenden Sie die folgenden Anweisungen auf dem Salesforce Startbildschirm, um Ihre Salesforce Meine Domain zu finden.

1. Gehen Sie wie in der SalesforceDokumentation beschrieben zur Einrichtungsseite.
2. Suchen Sie in der Schnellsuche nach Unternehmenseinstellungen und wählen Sie in den Ergebnissen Meine Domain aus.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Salesforce Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vorSalesforce, um Ihre Kunden-ID in zu finden:

1. Navigieren Sie zur Einrichtungsseite.
2. Wählen Sie „Setup“ und anschließend „App Manager“.
3. Wählen Sie die erstellte App aus und wählen Sie im Dropdownmenü die Option „Anzeigen“.
4. Wählen Sie Verbraucherdaten verwalten aus. Sie werden zu einem neuen Tab weitergeleitet.
5. Überprüfen Sie Ihre Identität und suchen Sie dann nach dem Wert für den Consumer Key.

6. Geben Sie den Verbraucherschlüssel in das Feld für die Client-ID unter ein AppFabric.

Clientschlüssel

AppFabric fordert Ihr Kundengeheimnis an. Das Kundengeheimnis in AppFabric ist das Kundengeheimnis inSalesforce. Gehen Sie wie folgt vorSalesforce, um Ihr Secret in zu finden:

1. Navigiere zur Einrichtungsseite.
2. Wählen Sie „Setup“ und anschließend „App Manager“.
3. Wählen Sie die erstellte App aus und wählen Sie im Dropdownmenü die Option „Anzeigen“.
4. Wählen Sie Verbraucherdaten verwalten aus. Sie werden zu einem neuen Tab weitergeleitet.
5. Überprüfen Sie Ihre Identität und suchen Sie dann nach dem Wert „Consumer Secret“.
6. Geben Sie den Consumer Secret in das Feld für den geheimen Kundenschlüssel unter ein AppFabric.

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Salesforce können. Stellen Sie auf der Genehmigungsseite sicher, dass Sie bei der Autorisierung die Rolle Salesforce Systemadministrator oder einen Salesforce Benutzer mit den Benutzerberechtigungen „Ereignisprotokolldateien anzeigenAPI“ und „Aktiviert“ verwenden. Wählen Sie Zulassen, um die AppFabric Autorisierung zu genehmigen.

ServiceNow

ServiceNowist ein führender Anbieter von Cloud-basierten Diensten, die den IT-Betrieb von Unternehmen automatisieren. ServiceNowITOM bietet Unternehmen vollständige Transparenz und Kontrolle über ihre gesamte IT-Umgebung — einschließlich virtualisierter Infrastruktur und Cloud-Infrastruktur. Es vereinfacht die Zuordnung, Bereitstellung und Sicherung von Services und konsolidiert IT-Service- und Infrastrukturdaten in einem einzigen Aufzeichnungssystem. Darüber hinaus automatisiert und optimiert es wichtige Prozesse — einschließlich Ereignis-, Vorfall-, Problem-, Konfiguration- und Änderungsmanagement. Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenServiceNow, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für ServiceNow

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonServiceNow.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von ServiceNow zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie können es AppFabric mit jedem beliebigen ServiceNow Plantyp verwenden.
- Sie müssen einen Benutzer mit der Administratorrolle in Ihrem ServiceNow Konto haben.
- Sie müssen eine ServiceNow Instanz haben.

Überlegungen zur Ratenbegrenzung

ServiceNowlegt der ServiceNow API Ratenbegrenzungen fest. Weitere Informationen zu den ServiceNow API-Ratenbegrenzungen finden Sie auf der Website unter Ratenbegrenzung für eingehende REST-APIs. ServiceNow Wenn die Kombination aus AppFabric und Ihre vorhandenen ServiceNow API-Anwendungen die Grenzwerte überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung bereitgestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem ServiceNow Konto herstellen

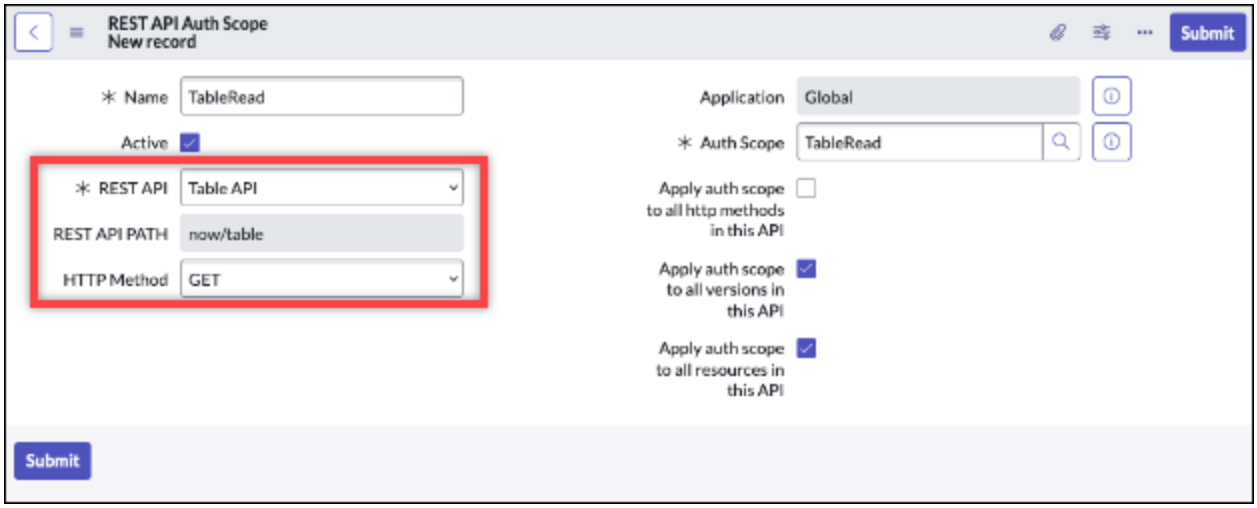
Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit ServiceNow autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung ServiceNow erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

Der Typ Now Platform unterstützt OAuth 2.0 — Authorization Grant für öffentliche Clients zur Generierung eines Zugriffstokens.

1. Registrieren Sie Ihre OAuth-Anwendung. Dazu sind die folgenden drei Schritte erforderlich. Weitere Informationen zum Ausführen dieser Schritte finden Sie unter Registrieren Sie Ihre Bewerbung bei ServiceNow auf der ServiceNowWebsite.

   a. Registrieren Sie die App und stellen Sie sicher, dass der Auth Scope Zugriff auf die Tabellen-API hat, mit dem REST-API-PATH now/table und der HTTP-Methode GET, wie im folgenden Beispiel gezeigt.



   b. Generieren Sie einen Autorisierungscode.

   c. Generieren Sie mithilfe des Autorisierungscodes ein Trägertoken.

2. Verwenden Sie eine Weiterleitungs-URL mit dem folgenden Format.

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

   In dieser URL <region>befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

App-Autorisierungen

Tenant-ID

AppFabric fordert eine Mandanten-ID an. Die darin angegebene Mandanten-ID AppFabric ist Ihr Instanzname. Sie finden Ihre Mandanten-ID in der Adressleiste Ihres Browsers. Zum Beispiel *example* ist die Mandanten-ID in der folgenden URL enthaltenhttps://*example*.service-now.com.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige ServiceNow Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Gehen Sie wie folgt vor, um Ihre Kunden-ID in zu findenServiceNow.

1. Navigieren Sie zur ServiceNow Konsole.
2. Wählen Sie System OAuth und dann die Registerkarte Anwendungsregistrierung.
3. Wählen Sie Ihre Anwendung.
4. Geben Sie die Client-ID Ihres OAuth-Clients in das Feld Client-ID unter ein. AppFabric

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Gehen Sie wie folgt vor, um Ihr Kundengeheimnis in zu findenServiceNow.

1. Navigieren Sie zur ServiceNow Konsole.
2. Wählen Sie System OAuth und dann die Registerkarte Anwendungsregistrierung.
3. Wählen Sie Ihre Anwendung.
4. Geben Sie den geheimen Clientschlüssel aus Ihrer OAuth-Anwendung in das Feld Client Secret unter ein. AppFabric

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen ServiceNow können. Wählen Sie Zulassen, um die AppFabric Autorisierung zu genehmigen.

Singularity Cloud

Die Singularity Cloud Plattform schützt Ihr Unternehmen in allen Phasen vor Bedrohungen aller Kategorien. Die patentierte künstliche Intelligenz erweitert die Sicherheit von bekannten Signaturen und Mustern bis hin zu ausgeklügeltsten Angriffen wie Zero-Day und Ransomware.

Sie können AWS AppFabric damit Auditprotokolle und Benutzerdaten empfangenSingularity Cloud, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

> **Note**
>
> Singularity CloudAuf die Dokumentation kann erst zugegriffen werden, nachdem Sie sich bei Ihrem Singularity Cloud Konto angemeldet haben. Daher können wir in diesem Dokument nicht direkt auf die Singularity Cloud Dokumentation verweisen.

Themen

- AppFabric Unterstützung für Singularity Cloud
- Verbindung AppFabric zu Ihrem Singularity Cloud Konto herstellen

AppFabric Unterstützung für Singularity Cloud

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonSingularity Cloud.

Voraussetzungen

Um Prüfprotokolle von unterstützten Zielen Singularity Cloud zu übertragen, müssen Sie über eine Administratorrolle in Ihrem Singularity Cloud Konto verfügen. AppFabric Für weitere Informationen zu den Singularity Cloud API-Ratenbegrenzungen melden Sie sich bei Ihrem Singularity Cloud-Konto an, durchsuchen Sie den Dokumentationsbereich und suchen Sie nach Rollen.

Überlegungen zur Ratenbegrenzung

Singularity Cloudlegt der Singularity Cloud API Ratenbegrenzungen fest. Für weitere Informationen zu den Singularity Cloud API-Ratenbegrenzungen melden Sie sich bei Ihrem Singularity Cloud-Konto an, durchsuchen Sie den Dokumentationsbereich und suchen Sie nach API-Ratenbegrenzungen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel übermittelt wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung bereitgestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Singularity Cloud Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Singularity Cloud autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Singularity Cloud erforderlichen Informationen zu finden. AppFabric

Erstellen Sie ein API-Token für Singularity Cloud

Gehen Sie wie folgt vor, um ein API-Token zu erstellen, das einem Dienstbenutzer zugeordnet ist. Das API-Token wird nicht mit einem bestimmten Konsolenbenutzer oder einer bestimmten E-Mail-Adresse verknüpft.

> **Note**
>
> Erstellen Sie einen neuen Benutzer oder kopieren Sie den Dienstbenutzer, um vor oder nach Ablauf eines Dienstbenutzer-API-Tokens ein neues API-Token zu erhalten.

1. Melden Sie sich bei Ihrem Singularity Cloud-Konto an.
2. Wählen Sie in der Einstellungssymbolleiste Benutzer und dann Dienstbenutzer aus.
3. Wählen Sie Aktionen und dann Neuen Dienstbenutzer erstellen aus.
4. Geben Sie auf der Seite Neuen Dienstbenutzer erstellen einen Namen, eine Beschreibung und ein Ablaufdatum für den Dienstbenutzer ein.
5. Wählen Sie Weiter aus.

6. Wählen Sie im Abschnitt „Zugriffsbereich auswählen“ den Bereich aus.
   - Wählen Sie Account als Zugriffsebene aus.
   - Wählen Sie das Konto aus, für das Sie Auditprotokolle abrufen möchten.
7. Wählen Sie Create User.

   Das API-Token wird generiert. Ein Fenster wird geöffnet und zeigt die Token-Zeichenfolge mit einer Meldung an, dass Sie das Token zum letzten Mal anzeigen können.
8. (Optional) Wählen Sie „API-Token kopieren“ und speichern Sie es an einem sicheren Ort.
9. Klicken Sie auf Schließen.

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die eingegebene Mandanten-ID ist AppFabric die Subdomain der Sentinel One Website-Adresse, unter der Sie sich für den Service anmelden. Wenn Sie sich beispielsweise unter der `example-company-1.sentinelone.net` Adresse in Ihrem Singularity Cloud Konto anmelden, lautet Ihre Mandanten-ID. `example-company-1`

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Singularity Cloud Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Dienstkonto-Token

Verwenden Sie das Token, das Sie mithilfe der Schritte im Erstellen Sie ein API-Token für Singularity Cloud Abschnitt dieses Handbuchs generiert haben. Wenn Sie das Token verlegen oder nicht finden können, können Sie ein neues generieren, indem Sie dieselben Schritte erneut ausführen.

> **Note**
>
> Wenn während der Erfassung der Audit-Logs ein neues API-Token in der Singularity Cloud-Konsole generiert AppFabric wird, werden die Datenerfassungen gestoppt. In diesem Fall müssen Sie die App-Autorisierung mit einem neuen API-Token aktualisieren, um die Erfassung des Audit-Logs fortzusetzen.

Slack

Slackhat es sich zur Aufgabe gemacht, das Arbeitsleben der Menschen einfacher, angenehmer und produktiver zu gestalten. Es ist die Produktivitätsplattform für Kundenunternehmen, die die Leistung verbessert, indem sie allen eine Automatisierung ohne Programmierkenntnisse ermöglicht, die Suche und den Wissensaustausch reibungslos ermöglicht und dafür sorgt, dass Teams miteinander verbunden und engagiert bleiben, während sie gemeinsam ihre Arbeit vorantreiben. Als Teil von Salesforce Slack ist sie tief in Salesforce Customer 360 integriert und steigert so die Produktivität aller Vertriebs-, Service- und Marketingteams. Besuchen Sie slack.com, um mehr zu erfahren und Slack kostenlos loszulegen.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenSlack, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für Slack
- Verbindung AppFabric zu Ihrem Slack Konto herstellen

AppFabric Unterstützung für Slack

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonSlack.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Slack zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie benötigen einen Enterprise Grid-Plan mitSlack. Weitere Informationen finden Sie auf der Slack Website unter Eine Einführung in Slack Enterprise Grid.
- Sie müssen einen Benutzer mit der Rolle „Organisationsinhaber“ in Ihrem Slack Konto haben. Weitere Informationen zu Rollen findest du unter Rollentypen Slack im Slack Help Center auf der Slack Website.

Überlegungen zur Ratenbegrenzung

Slacklegt der Slack API Ratenbegrenzungen fest. Weitere Informationen zu Slack API-Ratenbegrenzungen finden Sie unter Ratenlimits im SlackAPI-Nutzungshandbuch auf der Slack

Website. Wenn die Kombination aus AppFabric und Ihre vorhandenen Slack API-Anwendungen das Limit überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Slack Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Slack autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Slack erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Slack Verwendung von OAuth. Es gibt zwei Möglichkeiten, eine OAuth-App zu erstellen: mithilfe eines App-Manifests oder von Grund auf neu. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Slack zu erstellen.

Using an app manifest

1. Navigieren Sie in Ihrem SlackBrowser zur App Management-Benutzeroberfläche.
2. Wählen Sie Neue App erstellen.
3. Wählen Sie Aus einem App-Manifest.
4. Wähle den Workspace aus, für den du dich autorisieren AppFabric möchtest.
5. Wählen Sie im Feld App-Manifest unten eingeben die Option JSON aus und ersetzen Sie das vorhandene JSON durch das Folgende. <region>Ersetzen Sie es durch das entsprechende AWS-Region (z. B. *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. Kopieren und speichern Sie die Client-ID und den geheimen Client-Schlüssel von der Seite mit den Basisinformationen.
7. Für den `auditLogs:read` Geltungsbereich müssen Sie die öffentliche Verteilung Ihrer App aktivieren. Weitere Informationen findest du unter Öffentliche Verteilung aktivieren auf der Slack-Website.

From scratch

1. Wähle auf dem Bildschirm „App erstellen“ die Option Von Grund auf neu.
2. Benennen Sie Ihre App und wählen Sie einen Workspace aus.
3. Kopiere und speichere die Client-ID und den geheimen Client-Schlüssel von der Seite mit den Basisinformationen.
4. Wählen Sie auf der Seite OAuth & Permissions die Option Erweiterte Tokensicherheit über Token-Rotation.
5. Fügen Sie im Abschnitt Umleitungs-URLs der Seite OAuth & Permissions eine URL mit dem folgenden Format hinzu.

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

   In dieser URL *<region>* befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-

Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

6. Für diesen `auditLogs:read` Geltungsbereich müssen Sie die öffentliche Verteilung Ihrer App aktivieren. Weitere Informationen findest du unter Öffentliche Verteilung aktivieren auf der Slack-Website.

Erforderliche Bereiche

> **Note**
>
> Dieser Abschnitt ist nur relevant, wenn Sie die OAuth-App von Grund auf neu erstellen möchten. Überspringen Sie diesen Abschnitt, wenn Sie das App-Manifest verwenden möchten, um eine Anwendungsautorisierung zu erstellen.

Sie müssen auf der Seite „OAuth & Permissions“ Ihrer Slack OAuth-Anwendung die folgenden Bereiche für Benutzer-Tokens hinzufügen:

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

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die angegebene Mandanten-ID AppFabric ist Ihre Slack Workspace-ID. Um deine Mandanten-ID zu erhalten, befolge die Anweisungen unter Finde deine Slack URL im SlackHelp Center auf der Slack Website. Deine Slack Workspace-URL hat ein ähnliches Format wie `examplecorp.slack.com` oder`examplecorp.enterprise.slack.com`. Die Mandanten-ID, die du benötigst, ist `examplecorp` ohne `.slack.com` oder`.enterprise.slack.com`.

Name des Mandanten

Geben Sie einen Namen ein, der Ihre Slack Workspace-ID identifiziert. AppFabricverwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen

Client-ID

AppFabric fordert die Client-ID von Ihrer Slack OAuth-Anwendung an. Gehen Sie wie folgt vor, um die Client-ID zu finden:

1. Navigieren Sie in Ihrem Browser zur SlackApp Management-Benutzeroberfläche.
2. Wählen Sie die OAuth-Anwendung aus, mit der Sie arbeiten. AppFabric
3. Geben Sie die Client-ID von der Seite mit den Basisinformationen in das Feld Client-ID unter ein. AppFabric

Clientschlüssel

AppFabric fordert das Client-Geheimnis von Ihrer Slack OAuth-Anwendung an. Gehen Sie wie folgt vor, um den geheimen Clientschlüssel zu ermitteln:

1. Navigieren Sie in Ihrem Browser zur SlackApp Management-Benutzeroberfläche.
2. Wählen Sie die OAuth-Anwendung aus, mit der Sie arbeiten. AppFabric
3. Geben Sie den geheimen Client-Schlüssel von der Seite mit den Basisinformationen in das Feld Client-Geheimnis unter ein. AppFabric

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Slack können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen.

Smartsheet

Smartsheetist eine Work-Management-Plattform, mit der Sie Arbeit, Mitarbeiter und Technologie unternehmensweit aufeinander abstimmen können. Smartsheetbietet eine Reihe robuster Funktionen für Unternehmen, mit denen jeder Projekte verwalten, Workflows automatisieren und schnell skalierbare Lösungen entwickeln kann. Dadurch wird ein Umfeld für Innovationen geschaffen und gleichzeitig Sicherheit und Compliance gewährleistet.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenSmartsheet, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für Smartsheet

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonSmartsheet.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Smartsheet zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über ein Smartsheet Business-, Enterprise- oder Advance-Konto verfügen. Weitere Informationen zur Erstellung oder zum Upgrade Ihres Smartsheet Kontos finden Sie entweder unter SmartsheetPreise oder SmartsheetAdvance auf der Smartsheet Website.
- Sie müssen den Registrierungsprozess für Smartsheet Entwickler abschließen.

Überlegungen zur Ratenbegrenzung

Smartsheetlegt der Smartsheet API Ratenbegrenzungen fest. Weitere Informationen zu den Smartsheet API-Ratenbegrenzungen finden Sie unter Ratenbegrenzung in der Smartsheet-API-Referenz auf der Smartsheet-Website.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung bereitgestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Smartsheet Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Smartsheet autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Smartsheet erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Smartsheet Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Smartsheet zu erstellen:

1. Navigieren Sie zu den Entwicklertools in Ihrem Smartsheet Konto.
2. Wählen Sie auf dem Bildschirm mit den Entwicklertools die Option Neue App erstellen aus.
3. Füllen Sie alle Eingabefelder auf dem Bildschirm „Neue App erstellen“ aus.
4. Verwenden Sie einen beliebigen eindeutigen Wert für App-URL und App-Kontakt/Support.
5. Verwenden Sie eine Umleitungs-URL mit dem folgenden Format als App-Umleitungs-URL.

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

   In dieser URL *<region>* befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2`.
6. Wählen Sie Speichern.
7. Kopieren und speichern Sie die App-Client-ID und den App-Secret.

Erforderliche Bereiche

Smartsheeterfordert nicht, dass Sie Ihrer OAuth-Konfiguration explizit Bereiche hinzufügen. AppFabric fordert in der Autorisierungsanfrage für Ihr Konto die folgenden Bereiche an: Smartsheet

- `READ_EVENTS`
- `READ_USERS`

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die angegebene Mieter-ID AppFabric ist Ihre Smartsheet Konto-ID.

Name des Mandanten

AppFabric fordert Ihre Mieter-ID an. Geben Sie einen beliebigen Wert ein, der Ihr Smartsheet Konto eindeutig identifiziert.

Client-ID

AppFabric fordert Ihre Kunden-ID an. Die angegebene Client-ID AppFabric ist Ihre Smartsheet App-Client-ID. Gehen Sie wie folgt vorSmartsheet, um Ihre App-Client-ID in zu finden:

1. Navigieren Sie zu den Entwicklertools in Ihrem Smartsheet Konto.
2. Wählen Sie die OAuth-Anwendung aus, mit der Sie eine Verbindung herstellen. AppFabric
3. Geben Sie die App-Client-ID aus dem App-Profilbildschirm in das Feld Client-ID unter ein. AppFabric

Clientschlüssel

AppFabric fordert Ihr Kundengeheimnis an. Das Client-Geheimnis in AppFabric ist Ihr Smartsheet App-Secret. Gehen Sie wie folgt vorSmartsheet, um Ihren geheimen App-Schlüssel zu finden:

1. Navigieren Sie zu den Entwicklertools in Ihrem Smartsheet Konto.
2. Wählen Sie die OAuth-Anwendung aus, mit der Sie eine Verbindung herstellen. AppFabric
3. Geben Sie den geheimen Schlüssel der App auf dem Bildschirm „App-Profil“ in das Feld Client Secret ein. AppFabric

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Smartsheet können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen.

Terraform Cloud

HashiCorp Terraform Cloudist das weltweit am häufigsten verwendete Multi-Cloud-Provisioning-Produkt. Das Terraform Ökosystem umfasst mehr als 3.000 Anbieter, 14.000 Module und 250 Millionen Downloads. Terraform Cloudist der schnellste Weg zur Einführung und bietet allesTerraform, was Praktiker, Teams und globale Unternehmen benötigen, um Infrastruktur aufzubauen und zusammenzuarbeiten und Risiken in Bezug auf Sicherheit, Compliance und

betriebliche Einschränkungen zu bewältigen. Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenTerraform Cloud, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für Terraform Cloud
- Verbindung AppFabric zu Ihrem Terraform Cloud Konto herstellen

AppFabric Unterstützung für Terraform Cloud

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonTerraform Cloud.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Terraform Cloud zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Um auf die Auditprotokolle zugreifen zu können, müssen Sie über einen Terraform Cloud Plus Edition-Plan verfügen und Eigentümer der Organisation sein. Weitere Informationen zu den Terraform Cloud Plänen finden Sie auf der HashiCorp Terraform Website unter TerraformPreise.
- TBD-Auditprotokolle sind für Organisationen verfügbar, die über das Terraform Cloud Konto erstellt werden können.

Überlegungen zur Ratenbegrenzung

Terraform Cloudlegt der Terraform Cloud API Ratenbegrenzungen fest. Weitere Informationen zu den Terraform Cloud API-Ratenbegrenzungen finden Sie unter API-Ratenbegrenzung in den allgemeinen Einstellungen der Terraform Cloud Entwickleradministration auf der Terraform Cloud Website. Wenn die Kombination aus AppFabric und Ihre vorhandenen Terraform Cloud API-Anwendungen die Grenzwerte überschreiten, AppFabric kann Terraform Cloud es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der

Anwendung bereitgestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Terraform Cloud Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Terraform Cloud autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Terraform Cloud erforderlichen Informationen zu finden. AppFabric

Erstellen Sie ein API-Token für eine Organisation

AppFabric integriert sich in Terraform Cloud die Verwendung eines Organisations-API-Tokens. Weitere Informationen zu den API-Token der Terraform Cloud Organisation finden Sie unter API-Token für Organisationen. Um eine Organisation zu erstellen, folgen Sie den Anweisungen unter Organizations erstellen. Gehen Sie wie folgt vorTerraform Cloud, um ein Organisations-API-Token in zu erstellen.

1. Navigieren Sie zur Terraform CloudAnmeldeseite und melden Sie sich an.
2. Wählen Sie im linken Bereich Organisation, Einstellungen und dann API-Token aus.
3. Wählen Sie unter Organisationstoken die Option Organisationstoken erstellen und dann Token generieren aus.
4. (Optional) Geben Sie das Ablaufdatum oder die Uhrzeit des Tokens ein, oder erstellen Sie ein Token, das nie abläuft.
5. Kopieren und speichern Sie das Token. Das wirst du später brauchen AppFabric. Wenn Sie die Seite schließen, bevor Sie das Token speichern, müssen Sie das alte Token widerrufen und ein neues erstellen.

App-Autorisierungen

Tenant-ID

AppFabric fordert eine Mandanten-ID an. Die Mandanten-ID für Ihr Terraform Cloud Konto ist die aktuelle Organisations-URL Ihres Kontos. Sie finden diese, indem Sie sich bei Ihrer Terraform Cloud Organisation anmelden und die aktuelle Organisations-URL kopieren. Die Mandanten-ID sollte einem der folgenden Formate entsprechen:

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

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Terraform Cloud Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Dienstkonto-Token

AppFabric fordert Ihr Dienstkonto-Token an. Das Dienstkonto-Token in AppFabric ist das Organisations-API-Token, in dem Sie es erstellt habenErstellen Sie ein API-Token für eine Organisation.

Webex by Cisco

Ciscoist ein weltweit führendes Technologieunternehmen, das das Internet unterstützt. Ciscoeröffnet neue Möglichkeiten, indem es Ihre Anwendungen neu konzipiert, Ihre Daten schützt, Ihre Infrastruktur transformiert und Ihre Teams für eine globale und integrative future befähigt.

Über Webex by Cisco

Webexist ein führender Anbieter von Cloud-basierten Kollaborationslösungen, zu denen Videokonferenzen, Telefonate, Nachrichten, Veranstaltungen, Kundenerlebnislösungen wie Contact Center und speziell entwickelte Geräte für die Zusammenarbeit gehören. WebexDer Fokus auf die Bereitstellung inklusiver Kollaborationserlebnisse fördert Innovationen, bei denen KI und Machine Learning genutzt werden, um die Barrieren in Bezug auf geografische, sprachliche, persönliche und technologische Vertrautheit zu beseitigen. Die Lösungen des Unternehmens sind von Haus aus auf Sicherheit und Datenschutz ausgelegt. Webexfunktioniert mit den weltweit führenden Geschäfts- und Produktivitäts-Apps — bereitgestellt über eine einzige Anwendung und Oberfläche. Weitere Informationen finden Sie unter webex.com.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenWebex, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für Webex
- Verbindung AppFabric zu Ihrem Webex Konto herstellen

AppFabric Unterstützung für Webex

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonWebex.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Webex zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über einen Collaboration Flex-Plan, Meet Plan, Call Plan oder höher verfügen. Weitere Informationen zur Erstellung oder zum Upgrade auf den jeweiligen Webex Plantyp finden Sie auf der Webex Website unter WebexPreise für alle Funktionen.
- Ihr Konto muss über die Pro Pack-Lizenz verfügen, um auf Security Audit Events zugreifen zu können, die von einer der Cisco AuditLog APIs bereitgestellt werden.
- Sie benötigen einen Benutzer mit der Rolle Organisationsadministrator > Volladministrator.
- In der Konfiguration der Administratorrollen für Ihren Volladministrator muss die Option Compliance Officer aktiviert sein.

Überlegungen zur Ratenbegrenzung

Webexlegt der Webex API Ratenbegrenzungen fest. Weitere Informationen zu den Webex API-Ratenbegrenzungen finden Sie im WebexEntwicklerhandbuch auf der Webex Website unter Ratenbegrenzungen. Wenn die Kombination aus AppFabric und Ihre vorhandenen Webex API-Anwendungen das Limit überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Webex Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Webex autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Webex erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Webex Verwendung von OAuth. Gehen Sie wie folgt vor, um eine OAuth-Anwendung in Webex zu erstellen:

1. Folgen Sie den Anweisungen im Abschnitt Registrierung Ihrer Integration auf der Seite Integrationen und Autorisierung des Webex Entwicklerhandbuchs.
2. Verwenden Sie eine Weiterleitungs-URL mit dem folgenden Format.

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

   In dieser URL *<region>* befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Erforderliche Bereiche

Sie müssen Ihrer Webex OAuth-Anwendung die folgenden Bereiche hinzufügen:

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

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die angegebene Mandanten-ID AppFabric ist Ihre Webex Organisations-ID. Informationen dazu, wie Sie Ihre Webex Organisations-ID finden, finden Sie auf der WebexHelp-Center-Website unter Suchen Sie Ihre Organisations-ID in CiscoWebex Control Hub.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Webex Instanz identifiziert. AppFabricverwendet den Namen des Mandanten, um die App-Autorisierungen und alle aus der App-Autorisierung erstellten Dateneingaben zu kennzeichnen.

Client-ID

AppFabric fordert Ihre Webex Kunden-ID an. Gehen Sie wie folgt vor, um Ihre Webex Kunden-ID zu finden:

1. Melden Sie sich unter https://developer.webex.com in Ihrem Webex Konto an.
2. Wähle oben rechts deinen Avatar aus.
3. Wählen Sie Meine Webex-Apps.
4. Wählen Sie die OAuth2-Anwendung, für die Sie verwenden. AppFabric
5. Geben Sie die Client-ID auf dieser Seite in das Feld Client-ID unter ein. AppFabric

Clientschlüssel

AppFabric fordert Ihr Webex Kundengeheimnis an. Webexpräsentiert Ihr Client-Geheimnis nur einmal, wenn Sie Ihre OAuth-Anwendung zum ersten Mal erstellen. Gehen Sie wie folgt vor, um ein neues Client-Geheimnis zu generieren, wenn Sie das ursprüngliche Client-Geheimnis nicht gespeichert haben:

1. Melden Sie sich unter https://developer.webex.com in Ihrem Webex Konto an.
2. Wähle oben rechts deinen Avatar aus.
3. Wählen Sie Meine Webex-Apps.
4. Wählen Sie die OAuth2-Anwendung, für die Sie verwenden. AppFabric
5. Generieren Sie auf dieser Seite einen neuen geheimen Clientschlüssel.
6. Geben Sie das neue Kundengeheimnis in das Feld Kundengeheimnis unter ein AppFabric.

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung erstellt haben, erhalten AppFabric Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Webex können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Akzeptieren.

Zendesk

Zendeskhat 2007 die Revolution des Kundenerlebnisses ins Leben gerufen, indem es jedem Unternehmen auf der ganzen Welt ermöglicht hat, seinen Kundenservice online anzubieten. Heute Zendesk ist der Champion für großartigen Service überall für alle, unterstützt Milliarden von Konversationen und verbindet mehr als 100.000 Marken mit Hunderten von Millionen von Kunden

über Telefonie, Chat, E-Mail, Messaging, soziale Kanäle, Communitys, Bewertungsseiten und Helpcenter. ZendeskProdukte werden mit Liebe gebaut, um geliebt zu werden. Das Unternehmen wurde in Kopenhagen, Dänemark, gegründet, in Kalifornien gebaut und ausgebaut und beschäftigt heute mehr als 6.000 Mitarbeiter auf der ganzen Welt.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenZendesk, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

AppFabric Unterstützung für Zendesk

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonZendesk.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Zendesk zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über ein Zendesk Suite Enterprise- oder Enterprise Plus-Konto oder ein Zendesk Support Enterprise-Konto verfügen. Weitere Informationen zur Erstellung oder zum Upgrade auf ein Zendesk Enterprise-Konto finden Sie Zendesk auf der Zendesk Website unter Überprüfen Ihres Plantyps.
- Sie müssen einen Benutzer mit der Administratorrolle in Ihrem Zendesk Konto haben. Weitere Informationen zu Rollen finden Sie auf der Zendesk Website unter Grundlegendes zu Zendesk Support-Benutzerrollen.

Überlegungen zur Ratenbegrenzung

Zendesklegt der Zendesk API Ratenbegrenzungen fest. Weitere Informationen zu den Zendesk API-Ratenbegrenzungen finden Sie im ZendeskEntwicklerhandbuch auf der Zendesk Website unter Ratenbegrenzungen. Wenn die Kombination aus AppFabric und Ihre vorhandenen Zendesk API-Anwendungen das Limit überschreiten, AppFabric kann es zu Verzögerungen bei der Anzeige von Audit-Logs kommen.

Überlegungen zur Datenverzögerung

Es kann zu einer Verzögerung von bis zu 30 Minuten kommen, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung zur Verfügung gestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten. Dies kann jedoch auf Kontoebene anpassbar sein. Wenn Sie Hilfe benötigen, wenden Sie sich an. AWS Support

Verbindung AppFabric zu Ihrem Zendesk Konto herstellen

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Zendesk autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Zendesk erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine OAuth-Anwendung

AppFabric integriert sich in die Zendesk Verwendung von OAuth. In Zendesk müssen Sie eine OAuth-Anwendung mit den folgenden Einstellungen erstellen:

1. Folgen Sie den Anweisungen im Abschnitt Registrierung Ihrer Anwendung bei Zendesk des Artikels Verwenden der OAuth-Authentifizierung mit Ihrer Anwendung auf der Zendesk Support-Website.
2. Verwenden Sie eine Weiterleitungs-URL mit dem folgenden Format.

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

   In dieser URL *<region>* befindet sich der Code für das, AWS-Region in dem Sie Ihr AppFabric App-Bundle konfiguriert haben. Der Code für die Region USA Ost (Nord-Virginia) lautet beispielsweise`us-east-1`. Für diese Region lautet die Weiterleitungs-URL`https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2`.

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die Tenant-ID in AppFabric ist Ihre Zendesk Subdomain. Weitere Informationen zur Suche nach Ihrer Zendesk Subdomain finden Sie unter Wo finde ich meine Zendesk Subdomain auf der Zendesk Support-Website.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Zendesk Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert eine Client-ID an. Die angegebene Client-ID AppFabric ist Ihre eindeutige Zendesk API-ID. Gehen Sie wie folgt vor, um Ihre eindeutige Zendesk-ID zu finden:

1. Navigieren Sie in Ihrem Zendesk Konto zum Admin Center.
2. Wählen Sie Apps und Integrationen aus.
3. Wählen Sie APIs, ZendeskAPIs.
4. Wählen Sie die Registerkarte OAuth-Clients.
5. Wählen Sie die OAuth-Anwendung aus, für die Sie sie erstellt haben. AppFabric
6. Geben Sie die eindeutige Kennung für Ihren OAuth-Client in das Feld Client-ID unter ein. AppFabric

Clientschlüssel

AppFabric fordert einen geheimen Client-Schlüssel an. Das darin enthaltene Client-Geheimnis AppFabric ist Ihr Zendesk geheimes Token. Zendeskpräsentiert Ihr geheimes Token nur einmal, wenn Sie Ihre Zendesk OAuth-Anwendung zum ersten Mal erstellen. Gehen Sie wie folgt vor, um ein neues geheimes Token zu generieren, wenn Sie das ursprüngliche geheime Token nicht gespeichert haben:

1. Navigieren Sie in Ihrem Zendesk Konto zum Admin Center.
2. Wählen Sie Apps und Integrationen aus.
3. Wählen Sie APIs, ZendeskAPIs.
4. Wählen Sie die Registerkarte OAuth-Clients.
5. Wählen Sie die OAuth-Anwendung aus, für die Sie sie erstellt haben. AppFabric
6. Wählen Sie neben dem Feld Geheimes Token die Schaltfläche Regenerieren aus.
7. Geben Sie das neue geheime Token in das Feld Kundengeheimnis unter ein. AppFabric

Autorisierung genehmigen

Nachdem Sie die App-Autorisierung in erstellt haben AppFabric, erhalten Sie ein Popup-Fenster von, in dem Sie die Autorisierung genehmigen Zendesk können. Um die AppFabric Autorisierung zu genehmigen, wählen Sie Zulassen.

Zoom

Zoomist eine all-in-one intelligente Kollaborationsplattform, die für Unternehmen und Privatpersonen einfacher, immersiver und dynamischer Verbindungen macht. ZoomTechnologie stellt den Menschen in den Mittelpunkt, ermöglicht sinnvolle Verbindungen, erleichtert moderne Zusammenarbeit und fördert menschliche Innovation durch Lösungen wie Team-Chat, Telefon, Besprechungen, Omnichannel-Cloud-Kontaktzentrum, intelligente Aufzeichnungen, Whiteboard und mehr in einem einzigen Angebot.

Aus AWS AppFabric Sicherheitsgründen können Sie Auditprotokolle und Benutzerdaten von empfangenZoom, die Daten in das Open Cybersecurity Schema Framework (OCSF) -Format normalisieren und die Daten in einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Stream ausgeben.

Themen

- AppFabric Unterstützung für Zoom
- Stellen Sie AppFabric eine Verbindung zu Ihrem Zoom Konto her

AppFabric Unterstützung für Zoom

AppFabric unterstützt den Empfang von Benutzerinformationen und Auditprotokollen vonZoom.

Voraussetzungen

Für AppFabric die Übertragung von Audit-Logs von Zoom zu unterstützten Zielen müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über einen Zoom Pro-, Business-, Education- oder Enterprise-Plan verfügen.
- Ihre Zoom Administratorrolle muss über die Berechtigung zum Erstellen von server-to-server OAuth Anwendungen verfügen. Informationen zur Aktivierung von server-to-server OAuth Anwendungen finden Sie im Abschnitt Berechtigungen aktivieren auf der OAuth Seite Server-to-Server im ZoomEntwicklerhandbuch auf der Zoom Website.

- Ihre Zoom Administratorrolle muss berechtigt sein, Administratoraktivitätsprotokolle einzusehen und Auditaktivitäten an- und abzumelden. Weitere Informationen zum Aktivieren der Berechtigung zum Anzeigen von Auditaktivitäten finden Sie unter Verwenden der Rollenverwaltung und Verwenden von Administratoraktivitätsprotokollen auf der Zoom Support-Website.

Überlegungen zur Ratenbegrenzung

Zoomlegt Ratenbegrenzungen für die Zoom API fest. Weitere Informationen zu Zoom API Ratenlimits finden Sie unter Ratenlimits im ZoomEntwicklerhandbuch. Wenn die Kombination aus AppFabric und Ihre vorhandenen Zoom Anwendungen das Limit überschreiten, werden die Auditprotokolle AppFabric möglicherweise verzögert angezeigt.

Überlegungen zur Datenverzögerung

Möglicherweise kommt es zu einer Verzögerung von etwa 24 Stunden, bis ein Prüfereignis an Ihr Ziel gesendet wird. Dies ist auf Verzögerungen bei den Prüfereignissen zurückzuführen, die von der Anwendung bereitgestellt werden, sowie auf Vorkehrungen zur Reduzierung von Datenverlusten.

Stellen Sie AppFabric eine Verbindung zu Ihrem Zoom Konto her

Nachdem Sie Ihr App-Bundle innerhalb des AppFabric Dienstes erstellt haben, müssen Sie sich AppFabric mit Zoom autorisieren. Gehen Sie wie folgt vor, um die für die Autorisierung Zoom erforderlichen Informationen zu finden. AppFabric

Erstellen Sie eine Anwendung server-to-server OAuth

AppFabric verwendet server-to-server OAuth mit App-Anmeldeinformationen für die IntegrationZoom. Um eine server-to-server OAuth Anwendung in zu erstellenZoom, folgen Sie den Anweisungen unter Erstellen einer OAuth Server-to-Server-App im ZoomEntwicklerhandbuch. AppFabric unterstützt keine Zoom Webhooks, und Sie können den Abschnitt zum Hinzufügen von Webhook-Abonnements überspringen.

Erforderliche Bereiche

Zoombietet zwei Arten von Bereichen: detaillierte Bereiche (für neu erstellte Anwendungen) und klassische Bereiche (für zuvor erstellte Anwendungen).

Sie müssen Ihrer Anwendung die folgenden detaillierten Bereiche hinzufügen: Zoom server-to-server OAuth

- `report:read:user_activities:admin`

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

Wenn Sie eine zuvor erstellte Anwendung verwenden, müssen Sie die folgenden klassischen Bereiche hinzufügen:

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

App-Autorisierungen

Tenant-ID

AppFabric fordert Ihre Mandanten-ID an. Die angegebene Mandanten-ID AppFabric ist die Zoom Konto-ID. Gehen Sie wie folgt vor, um Ihre Zoom Konto-ID zu ermitteln:

1. Navigieren Sie zum Zoom Marketplace.
2. Wählen Sie Manage (Verwalten).
3. Wählen Sie die server-to-server OAuth Anwendung, für die Sie verwenden AppFabric.
4. Geben Sie die Konto-ID von der Seite mit den App-Anmeldeinformationen in das Feld Mandanten-ID unter ein AppFabric.

Name des Mandanten

Geben Sie einen Namen ein, der diese eindeutige Zoom Organisation identifiziert. AppFabric verwendet den Namen des Mandanten, um die App-Autorisierungen und alle im Rahmen der App-Autorisierung erstellten Eingaben zu kennzeichnen.

Client-ID

AppFabric fordert Ihre Kunden-ID an. Gehen Sie wie folgt vor, um Ihre Zoom Kunden-ID zu finden:

1. Navigieren Sie zum Zoom Marketplace.
2. Wählen Sie Manage (Verwalten).
3. Wählen Sie die server-to-server OAuth Anwendung, für die Sie verwenden AppFabric.

4. Geben Sie die Client-ID von der Seite mit den App-Anmeldeinformationen in das Feld Client-ID unter ein AppFabric.

Clientschlüssel

AppFabric fordert Ihr Kundengeheimnis an. Gehen Sie wie folgt vor, um Ihr Zoom Kundengeheimnis herauszufinden:

1. Navigieren Sie zum Zoom Marketplace.
2. Wählen Sie Manage (Verwalten).
3. Wählen Sie die server-to-server OAuth Anwendung, für die Sie verwenden AppFabric.
4. Geben Sie den geheimen Client-Schlüssel von der Seite mit den App-Anmeldeinformationen in das Feld Client-Geheimnis unter ein AppFabric.

Übermittlung des Auditprotokolls

Zoomstellt Auditprotokolle zur Verfügung, indem API alle 24 Stunden auf sie zugegriffen wird. Wenn Sie Auditprotokolle mit anzeigen AppFabric, beziehen Zoom sich die angezeigten Daten auf die Aktivitäten des Vortages.

Kompatible Sicherheitstools und -dienste

AWS AppFabric for Security unterstützt die Integration mit den folgenden Sicherheitstools und -diensten. Wählen Sie den Namen eines Dienstes aus, um weitere Informationen darüber zu erhalten, wie Sie die AppFabric Sicherheitseinstellungen für die Verbindung zu diesem Dienst einrichten.

Themen

- Barracuda XDR
- Dynatrace
- Logz.io
- Netskope
- NetWitness
- Amazon QuickSight
- Rapid7
- Amazon Security Lake

- Singularity Cloud
- Splunk

Barracuda XDR

Barracuda Networksist ein vertrauenswürdiger Partner und führender Anbieter von Cloud-First-Sicherheitslösungen, der E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen schützt, die wachsen und sich an die Entwicklung der Unternehmen anpassen. Barracuda XDRist eine offene, erweiterte Erkennungs- und Reaktionslösung, die hochentwickelte Technologien mit einem Team von Sicherheitsanalysten in unserem Security Operations Center (SOC) kombiniert. Die Barracuda XDR Plattform analysiert täglich Milliarden von Rohereignissen aus über 40 integrierten Datenquellen. Zusammen mit umfangreichen Regeln zur Bedrohungserkennung, die dem MITRE ATT&CK® -Framework zugeordnet sind, können Bedrohungen schneller erkannt und die Reaktionszeit verkürzt werden.

AWS AppFabric Überlegungen zur Erfassung von Auditprotokollen

In den folgenden Abschnitten werden das AppFabric Ausgabeschema, die Ausgabeformate und die Ausgabeziele beschrieben, mit denen Sie arbeiten können. Barracuda XDR

Schema und Format

Barracuda XDRunterstützt das folgende AppFabric Ausgabeschema und die folgenden Formate:

- OCSF - JSON: AppFabric normalisiert die Daten mithilfe des Open Cybersecurity Schema Framework (OCSF) und gibt die Daten im JSON-Format aus.

Speicherorte für die Ausgabe

Barracuda XDRunterstützt den Empfang von Audit-Protokollen von Amazon Security Lake. Gehen Sie wie folgt vorBarracuda XDR, AppFabric um Daten von an zu senden:

1. Daten an Amazon Security Lake senden: Konfigurieren Sie AppFabric das Senden von Daten an Amazon Security Lake über eine Amazon Data Firehose. Weitere Informationen finden Sie unter Amazon Security Lake.
2. Daten senden anBarracuda XDR: Konfigurieren Sie Barracuda XDR den Empfang von Auditprotokollen von Amazon Security Lake. Weitere Informationen finden Sie unter Amazon Security Lake einrichten und verwenden.

Dynatrace

Das Dynatrace® Platform kombiniert umfassende und umfassende Beobachtbarkeit und kontinuierliche Runtime-Anwendungssicherheit mit fortschrittlichen AIOps, um Antworten und intelligente Automatisierung auf der Grundlage von Daten zu bieten. Dies ermöglicht es Innovatoren, den Cloud-Betrieb zu modernisieren und zu automatisieren, Software schneller und sicherer bereitzustellen und makellose digitale Erlebnisse zu gewährleisten.

AWS AppFabric Überlegungen zur Erfassung von Auditprotokollen

In den folgenden Abschnitten werden das AppFabric Ausgabeschema, die Ausgabeformate und die Ausgabeziele beschrieben, die mit dem verwendet werden können. Dynatrace Platform

Schema und Format

Das Dynatrace Platform unterstützt das folgende AppFabric Ausgabeschema und die folgenden Formate:

- OCSF — JSON: AppFabric normalisiert die Daten mithilfe des Open Cybersecurity Schema Framework (OCSF) und gibt die Daten im JSON-Format aus.

Speicherorte für die Ausgabe

Das Dynatrace Platform unterstützt den Empfang von Auditprotokollen von den folgenden AppFabric Ausgabespeicherorten.

- Amazon-Simple-Storage-Service (Amazon-S3)
  - Um den für den Dynatrace Platform Empfang von Daten aus dem Amazon S3 S3-Bucket, der Ihre Audit-Logs enthält, zu konfigurieren, folgen Sie den Anweisungen im S3 Log Forwarder-Projekt von Dynatrace unter. GitHub

Logz.io

Logz.iohilft Cloud-nativen Unternehmen dabei, ihre Umgebungen über die Logz.ioOpen 360 Platform zu überwachen und zu sichern. So werden Observability und Sicherheit von einer kostenintensiven Belastung mit geringem Wert zu einem hochwertigen, kosteneffizienten Instrument für bessere Geschäftsergebnisse.

Logz.ioCloud-SIEM geht direkt auf die wichtigsten Sicherheitsherausforderungen von heute ein — von der Datenüberflutung bis hin zu den allgegenwärtigen Qualifikationslücken im

Cyberbereich — durch schnelle Abfragen, mehrdimensionale Erkennung und umfassend anpassbare Sicherheitsinhalte, mit denen Sie Ihre gesamte Cloud-Umgebung überwachen und untersuchen können — ohne Leistungseinbußen, unabhängig vom Datenvolumen.

Die Logz.io Lösung wurde speziell für fortschrittliche Bedrohungsanalysen und -untersuchungen mit geringerer Komplexität und geringeren Kosten entwickelt. Kunden werden von engagierten Sicherheitsanalysten, Threat Content as a Service und KI-gestützten Funktionen unterstützt, die speziell darauf ausgelegt sind, Datenrauschen zu reduzieren und sich auf die Informationen zu konzentrieren, die es Ihrem Team ermöglichen, reale Bedrohungen schnell zu priorisieren.

AWS AppFabric Überlegungen zur Erfassung von Auditprotokollen

In den folgenden Abschnitten werden das AppFabric Ausgabeschema, die Ausgabeformate und die Ausgabeziele beschrieben, mit denen Sie arbeiten können. Logz.io

Schema und Format

Logz.iounterstützt das folgende AppFabric Ausgabeschema und die folgenden Formate:

- Raw — JSON
  - AppFabric gibt Daten im ursprünglichen Schema aus, das von der Quellanwendung verwendet wurde, im JSON-Format.
- OCSF - JSON
  - AppFabric normalisiert die Daten mithilfe des Open Cybersecurity Schema Framework (OCSF) und gibt die Daten im JSON-Format aus.

Speicherorte für die Ausgabe

Logz.iounterstützt die folgenden AppFabric Ausgabespeicherorte:

- Amazon Data Firehose
  - Um Ihren Firehose-Lieferstream so zu konfigurieren, dass Daten gesendet werdenLogz.io, folgen Sie den Anweisungen unter Wählen Sie Logz.io Ihr Ziel im Amazon Data Firehose Developer Guide.
- Amazon-Simple-Storage-Service (Amazon-S3)
  - Um den Empfang von Daten aus dem Amazon S3 S3-Bucket Logz.io zu konfigurieren, der Ihre Audit-Logs enthält, folgen Sie den Anweisungen unter Amazon S3 S3-Bucket konfigurieren auf der Logz.io Website.

Netskope

Netskope, ein weltweit führendes Unternehmen im Bereich Cybersicherheit, definiert Cloud-, Daten- und Netzwerksicherheit neu, um Unternehmen dabei zu unterstützen, Zero-Trust-Prinzipien zum Schutz von Daten anzuwenden. Die Netskope Plattform ist schnell und einfach zu bedienen und bietet optimierten Zugriff und Zero-Trust-Sicherheit für Menschen, Geräte und Daten, egal wo sie sich befinden. Netskopehilft Kunden dabei, Risiken zu reduzieren, die Leistung zu steigern und einen unvergleichlichen Einblick in alle Cloud-, Web- und privaten Anwendungsaktivitäten zu erhalten. Tausende von Kunden, darunter mehr als 25 der Fortune-100-Unternehmen, vertrauen Netskope auf sein leistungsstarkes NewEdge Netzwerk, um neuen Bedrohungen, neuen Risiken, technologischen Veränderungen, organisatorischen und Netzwerkänderungen sowie neuen regulatorischen Anforderungen zu begegnen. Besuchen Sie netskope.com Netskope, um zu erfahren, wie Kunden auf ihrer SASE-Reise auf alles vorbereitet sind.

AWS AppFabric Überlegungen zur Erfassung von Auditprotokollen

In den folgenden Abschnitten werden das AppFabric Ausgabeschema, die Ausgabeformate und die Ausgabeziele beschrieben, mit denen Sie arbeiten können. Netskope

Schema und Format

Netskopeunterstützt das folgende AppFabric Ausgabeschema und die folgenden Formate:

- Raw — JSON
  - AppFabric gibt Daten im ursprünglichen Schema aus, das von der Quellanwendung verwendet wurde, im JSON-Format.
- OCSF - JSON
  - AppFabric normalisiert die Daten mithilfe des Open Cybersecurity Schema Framework (OCSF) und gibt die Daten im JSON-Format aus.

Speicherorte für die Ausgabe

Netskopeunterstützt den folgenden AppFabric Ausgabespeicherort:

- Amazon-Simple-Storage-Service (Amazon-S3)
  - Um den Empfang von Daten aus dem Amazon S3 S3-Bucket Netskope zu konfigurieren, der Ihre Audit-Logs enthält, folgen Sie den Anweisungen unter Datenschutz für Amazon Web Services S3 auf der Netskope Website.

NetWitness

NetWitnessist ein führender Entwickler von XDR-Software (Extended Detection and Response). Ihr weltweiter Kundenstamm mit hohem Sicherheitsbewusstsein vertraut auf NetWitness XDR, um sich vor raffinierten und aggressiven Gegnern zu schützen. Mit der branchenweit umfassendsten, integriertesten und ausgereiftesten Plattform zur Erkennung, Untersuchung und Abwehr digitaler Angriffe bildet NetWitness XDR die einheitliche Grundlage für ein modernes und effektives SOC.

Aufgrund seiner hochmodularen Architektur erkennt NetWitness XDR Bedrohungen überall dort, wo sie auftreten — in der Cloud, vor Ort, bei mobilen und externen Mitarbeitern oder irgendwo dazwischen. Die NetWitness Platform XDR bietet umfassende Transparenz in Kombination mit angewandten Bedrohungsinformationen und Analysen des Benutzerverhaltens, um Bedrohungen zu erkennen, Aktivitäten zu priorisieren, zu untersuchen und Reaktionen zu automatisieren. All dies ermöglicht Sicherheitsanalysten eine bessere und schnellere Effizienz, sodass Sicherheitsoperationen den geschäftsschädigenden Bedrohungen immer einen Schritt voraus sind.

AWS AppFabric Überlegungen zur Erfassung von Audit-Logs

In den folgenden Abschnitten werden das AppFabric Ausgabeschema, die Ausgabeformate und die Ausgabeziele beschrieben, mit denen Sie arbeiten können. NetWitness

Schema und Format

NetWitness unterstützt das folgende AppFabric Ausgabeschema und die folgenden Formate:

- Raw — JSON
  - AppFabric gibt Daten im ursprünglichen Schema aus, das von der Quellanwendung verwendet wurde, im JSON-Format.
- OCSF - JSON
  - AppFabric normalisiert die Daten mithilfe des Open Cybersecurity Schema Framework (OCSF) und gibt die Daten im JSON-Format aus.

Speicherorte für die Ausgabe

NetWitnessunterstützt den folgenden AppFabric Ausgabespeicherort:

- Amazon-Simple-Storage-Service (Amazon-S3)

- Um den Empfang von Daten aus dem Amazon S3 S3-Bucket NetWitness zu konfigurieren, der Ihre Audit-Logs enthält, folgen Sie den Anweisungen im S3 Universal Connector Event Source Log Configuration Guide auf der Seite NetWitnessPlatform Integrations auf der NetWitness Website.

Amazon QuickSight

Amazon QuickSight unterstützt datengesteuerte Unternehmen mit einheitlicher Business Intelligence (BI) auf höchstem Niveau. Dank moderner interaktiver Dashboards QuickSight, paginierter Berichte, eingebetteter Analysen und Abfragen in natürlicher Sprache können alle Benutzer unterschiedliche Analyseanforderungen von derselben Informationsquelle aus erfüllen. Sie können AWS AppFabric Audit-Protokolldaten analysieren QuickSight, indem Sie Ihren Amazon Simple Storage Service (Amazon S3) -Bucket, in dem Ihre AppFabric vier Sicherheitsprotokolle gespeichert werden, als Quelle auswählen.

AppFabric Überlegungen zur Erfassung von Audit-Logs

In den folgenden Abschnitten werden das AppFabric Ausgabeschema, die Ausgabeformate und die Ausgabeziele beschrieben, die mit Amazon verwendet werden können QuickSight.

Schema und Formate

QuickSight unterstützt das folgende AppFabric Ausgabeschema und die folgenden Formate:

- Raw — JSON
  - AppFabric gibt Daten im ursprünglichen Schema aus, das von der Quellanwendung verwendet wurde, im JSON-Format.
- OCSF - JSON
  - AppFabric normalisiert die Daten mithilfe des Open Cybersecurity Schema Framework (OCSF) und gibt die Daten im JSON-Format aus.

Speicherorte für die Ausgabe

QuickSight unterstützt die folgenden AppFabric Ausgabespeicherorte:

- Amazon S3
  - Sie können Daten aus Amazon S3 direkt in Amazon S3 aufnehmen, QuickSight indem Sie einen Datensatz mit Amazon S3-Dateien erstellen. Wie Sie überprüfen können, ob Ihr

Zieldateisatz die QuickSight Datenquellenkontingente nicht überschreitet, finden Sie unter Datenquellenkontingente im QuickSight Amazon-Benutzerhandbuch.

- Wenn Ihr Dateisatz die QuickSight Kontingente für eine Amazon S3-Datenquelle überschreitet, können Sie Ihre Daten mithilfe von Amazon Athena und AWS Glue Tabellen in Amazon S3 aufnehmen. Wenn Sie Athena in Ihrem QuickSight Datensatz verwenden, fallen zusätzliche Kosten an. Weitere Informationen zu den Athena-Preisen finden Sie auf der Athena-Preisseite.

  Um Athena zu verwenden:

  1. Folgen Sie den Anweisungen unter Verwenden AWS Glue , um eine Verbindung zu Datenquellen in Amazon S3 herzustellen im Athena-Benutzerhandbuch.
  2. Folgen Sie den Anweisungen unter Erstellen eines Datensatzes mit Athena-Daten im QuickSight Amazon-Benutzerhandbuch.

Rapid7

Rapid7, Inc. hat es sich zur Aufgabe gemacht, eine sicherere digitale Welt zu schaffen, indem Cybersicherheit einfacher und zugänglicher gemacht wird. Rapid7versetzt Sicherheitsexperten in die Lage, eine moderne Angriffsfläche mithilfe von best-in-class Technologie, Spitzenforschung und umfassendem strategischem Fachwissen zu verwalten. Rapid7Die umfassenden Sicherheitslösungen helfen mehr als 10.000 Kunden weltweit dabei, Cloud-Risikomanagement und Bedrohungserkennung zu vereinen, um Angriffsflächen zu reduzieren und Bedrohungen schnell und präzise zu beseitigen.

AWS AppFabric Überlegungen zur Erfassung von Auditprotokollen

In den folgenden Abschnitten werden das AppFabric Ausgabeschema, das Ausgabeformat und die Ausgabeziele beschrieben, mit denen Sie arbeiten können. Rapid7

Schema und Format

Rapid7unterstützt das folgende AppFabric Ausgabeschema und die folgenden Formate:

- Raw — JSON
  - AppFabric gibt Daten im ursprünglichen Schema aus, das von der Quellanwendung verwendet wurde, im JSON-Format.
- OCSF - JSON
  - AppFabric normalisiert die Daten mithilfe des Open Cybersecurity Schema Framework (OCSF) und gibt die Daten im JSON-Format aus.

Speicherorte für die Ausgabe

Rapid7unterstützt den folgenden AppFabric Ausgabespeicherort:

- Amazon-Simple-Storage-Service (Amazon-S3)
  - Um Rapid7 so zu konfigurieren, dass es Daten aus dem Amazon S3-Bucket empfängt, der Ihre Audit-Logs enthält, folgen Sie den Anweisungen im Blogbeitrag How to Monitor Your Amazon S3 Activity with InsightIDR auf der Blog-Website. Rapid7

Amazon Security Lake

Amazon Security Lake zentralisiert automatisch Sicherheitsdaten aus AWS Umgebungen, SaaS-Anbietern (Software as a Service), lokalen Standorten und Cloud-Quellen in einem speziell entwickelten Data Lake, der in Ihrem gespeichert ist. AWS-Konto Mit Security Lake erhalten Sie ein umfassenderes Verständnis Ihrer Sicherheitsdaten in Ihrem gesamten Unternehmen. Security Lake hat das Open Cybersecurity Schema Framework (OCSF) eingeführt, ein Open-Source-Schema für Sicherheitsereignisse. Mit OCSF Unterstützung normalisiert und kombiniert der Service Sicherheitsdaten aus AWS und einer Vielzahl von Sicherheitsdatenquellen für Unternehmen.

AppFabric Überlegungen zur Erfassung von Auditprotokollen

Sie können Ihre SaaS-Auditprotokolle in Amazon Security Lake in Ihrem abrufen, AWS-Konto indem Sie eine benutzerdefinierte Quelle zu Security Lake hinzufügen. In den folgenden Abschnitten werden das AppFabric Ausgabeschema, das Ausgabeformat und die Ausgabeziele beschrieben, die mit Security Lake verwendet werden sollen.

Schema und Format

Security Lake unterstützt das folgende AppFabric Ausgabeschema und -format:

- OCSF - JSON
  - AppFabric normalisiert die Daten mithilfe des Open Cybersecurity Schema Framework (OCSF) und gibt die Daten im JSON Format aus.

Speicherorte für die Ausgabe

Security Lake unterstützt AppFabric als benutzerdefinierte Quelle die Verwendung eines Amazon Data Firehose-Lieferdatenstroms als Speicherort für die AppFabric Aufnahme und Ausgabe. Gehen

Sie wie folgt vor, um die AWS Glue Tabelle und den Firehose-Lieferstream zu konfigurieren und eine benutzerdefinierte Quelle in Security Lake einzurichten.

Erstellen Sie eine Tabelle AWS Glue

1. Navigieren Sie zu Amazon Simple Storage Service (Amazon S3) und erstellen Sie einen Bucket mit einem Namen Ihrer Wahl.
2. Navigieren Sie zur AWS Glue Konsole.
3. Gehen Sie für Datenkatalog zum Abschnitt Tabellen und wählen Sie Tabelle hinzufügen aus.
4. Geben Sie einen Namen Ihrer Wahl für diese Tabelle ein.
5. Wählen Sie den Amazon S3 S3-Bucket aus, den Sie in Schritt 1 erstellt haben.
6. Wählen Sie für das Datenformat JSONdie Option Weiter aus.
7. Wählen Sie auf der Seite Schema auswählen oder definieren die Option Schema bearbeiten als ausJSON.
8. Geben Sie das folgende Schema ein und schließen Sie die AWS Glue Tabellenerstellung ab.

```
[
    {
        "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
    }
]
```

Erstellen Sie eine benutzerdefinierte Quelle in Security Lake

1. Navigieren Sie zur Amazon Security Lake-Konsole.
2. Wählen Sie im Navigationsbereich Benutzerdefinierte Quellen aus.
3. Wählen Sie Benutzerdefinierte Quelle erstellen aus.
4. Geben Sie einen Namen für Ihre benutzerdefinierte Quelle ein und wählen Sie eine entsprechende OCSF Ereignisklasse aus.

> **Note**
>
> AppFabric verwendet die Ereignisklassen Kontoänderung, Authentifizierung, Benutzerzugriffsverwaltung, Gruppenverwaltung, Webressourcenaktivität und Webressourcenzugriffsaktivität.

5. Geben Sie sowohl für die AWS-Konto ID als auch für die externe AWS-Konto ID Ihre ID ein. Wählen Sie dann die Option Erstellen.
6. Speichern Sie den Amazon S3 S3-Speicherort der benutzerdefinierten Quelle. Sie werden es verwenden, um einen Amazon Data Firehose-Lieferstream einzurichten.

Erstellen Sie einen Lieferstream in Firehose

1. Navigieren Sie zur Amazon Data Firehose-Konsole.
2. Wählen Sie Create a Delivery Stream aus.
3. Wählen Sie als Quelle die Option Direkt ausPUT.
4. Wählen Sie als Ziel die Option S3 aus.
5. Wählen Sie im Abschnitt Datensätze transformieren und konvertieren die Option Konvertierung des Datensatzformats aktivieren und wählen Sie Apache Parquetals Ausgabeformat aus.
6. Wählen Sie für AWS Glue Tabelle die AWS Glue Tabelle aus, die Sie im vorherigen Verfahren erstellt haben, und wählen Sie die neueste Version aus.
7. Wählen Sie für Zieleinstellungen den Amazon S3 S3-Bucket aus, den Sie mit der benutzerdefinierten Security Lake-Quelle erstellt haben.
8. Wählen Sie für Dynamische Partitionierung die Option Aktiviert.
9. Wählen Sie für Inline-Parsing für die Option JSON Aktiviert.
   - Geben Sie als Schlüsselname ein. `eventDayValue`
   - Geben Sie für JQ Expression ein. `(.time/1000)|strftime("%Y%m%d")`
10. Geben Sie für das S3-Bucket-Präfix den folgenden Wert ein.

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

    Ersetzen *<custom source name>*, *<region>* and *<account_id>* mit Ihrem benutzerdefinierten Security Lake-Quellnamen AWS-Region und Ihrer AWS-Konto ID.
11. Geben Sie für das Ausgabepräfix für den S3-Bucket-Fehler den folgenden Wert ein.

    ```
    ext/AppFabric/error/
    ```
12. Wählen Sie für die Dauer des Wiederholversuchs 300 aus.
13. Wählen Sie für die Puffergröße 128 MiB aus.
14. Wählen Sie für das Pufferintervall 60s aus.
15. Schließen Sie den Erstellungsprozess für den Firehose-Lieferstream ab.

Ingestions erstellen AppFabric

Um Daten an Amazon Security Lake zu senden, müssen Sie in der AppFabric Konsole eine Aufnahme erstellen, die den Firehose-Lieferstream, den Sie zuvor erstellt haben, als Ausgabespeicherort verwendet. Weitere Informationen zur Konfiguration von AppFabric Ingestions für die Verwendung von Firehose als Ausgabespeicherort finden Sie unter Erstellen eines Ausgabespeicherorts.

Singularity Cloud

Die Singularity Cloud Plattform schützt Ihr Unternehmen in allen Phasen vor Bedrohungen aller Kategorien. Die patentierte KI (künstliche Intelligenz) erweitert die Sicherheit von bekannten Signaturen und Mustern bis hin zu ausgeklügeltsten Angriffen wie Zero-Day und Ransomware.

AWS AppFabric Überlegungen zur Erfassung von Auditprotokollen

In den folgenden Abschnitten werden das AppFabric Ausgabeschema, die Ausgabeformate und die Ausgabeziele beschrieben, mit denen Sie arbeiten können. Singularity Cloud

Schema und Format

Singularity Cloudunterstützt das folgende AppFabric Ausgabeschema und die folgenden Formate:

OCSF - JSON: AppFabric normalisiert die Daten mithilfe des Open Cybersecurity Schema Framework (OCSF) und gibt die Daten im JSON-Format aus.

Speicherorte für die Ausgabe

Singularity Cloudunterstützt den Empfang von Auditprotokollen von den folgenden AppFabric Ausgabespeicherorten.

- Amazon-Simple-Storage-Service (Amazon-S3)
  - Folgen Sie den Anweisungen in der Singularity Cloud’s Dokumentation, Singularity Cloud um den Empfang von Daten aus dem Amazon S3 S3-Bucket zu konfigurieren, der Ihre Audit-Logs enthält.

Splunk

Splunkträgt dazu bei, Unternehmen widerstandsfähiger zu machen. Führende Unternehmen nutzen Splunk die einheitliche Sicherheits- und Beobachtungsplattform, um ihre digitalen Systeme sicher

und zuverlässig zu halten. Organizations vertrauen darauf, Splunk zu verhindern, dass Sicherheits-, Infrastruktur- und Anwendungsprobleme zu größeren Zwischenfällen werden, Schocks aufgrund digitaler Störungen abfangen und die digitale Transformation beschleunigen.

AWS AppFabric Überlegungen zur Erfassung von Auditprotokollen

In den folgenden Abschnitten werden das AppFabric Ausgabeschema, die Ausgabeformate und die Ausgabeziele beschrieben, mit denen Sie arbeiten können. Splunk

Schema und Format

Splunk unterstützt die folgenden AppFabric Ausgabeschemas und -formate:

- Raw — JSON
  - AppFabric gibt Daten im ursprünglichen Schema aus, das von der Quellanwendung verwendet wurde, im JSON-Format.
- OCSF - JSON
  - AppFabric normalisiert die Daten mithilfe des Open Cybersecurity Schema Framework (OCSF) und gibt die Daten im JSON-Format aus.
- OCSF - Parquet
  - AppFabric normalisiert die Daten mithilfe des Open Cybersecurity Schema Framework (OCSF) und gibt die Daten im folgenden Format aus. Apache Parquet

Speicherorte für die Ausgabe

Splunkunterstützt die folgenden AppFabric Ausgabespeicherorte:

- Amazon Data Firehose
  - Um den Empfang von Audit-Logs aus dem Firehose-Stream Splunk zu konfigurieren, der Ihre Audit-Logs enthält, folgen Sie den Anweisungen im SplunkAdd-on für Amazon Data Firehose auf der Splunk Website.
- Amazon-Simple-Storage-Service (Amazon-S3)
  - Um den Empfang von Daten aus dem Amazon S3 S3-Bucket Splunk zu konfigurieren, der Ihre Audit-Logs enthält, folgen Sie den Anweisungen unter SQS-basierte S3-Eingaben für das Splunk Add-on konfigurieren für AWS auf der Splunk Website.

Aus AWS AppFabric Sicherheitsgründen löschen

Wenn Sie die Nutzung aus AWS AppFabric Sicherheitsgründen nicht fortsetzen möchten, löschen Sie unbedingt die Daten in den Ausgabeverzeichnissen, die Sie während der Installation erstellt haben, und Ihre AppFabric Sicherheitsressourcen, um zusätzliche Gebühren zu vermeiden.
Um Ihre AppFabric Ressourcen zu bereinigen, müssen Sie die Ressourcen in der umgekehrten Reihenfolge löschen, in der Sie sie für jede SaaS-Anwendung (Software as a Service) erstellt haben: Aufnahmeziele > Ingestions > App-Autorisierung > App-Bundles

Nachdem Sie Ihre endgültige App-Autorisierung gelöscht haben, können Sie das App-Bundle löschen.

Themen

Löschen Sie ein Aufnahmeziel

Wenn Sie bei der Erstellung einer Aufnahme einen Ausgabespeicherort auswählen, werden aus AppFabric Sicherheitsgründen Aufnahmeziele in Ihrem Namen erstellt. Gehen Sie wie folgt vor, um ein Aufnahmeziel zu löschen:

1. Öffnen Sie die AppFabric Konsole unter https://console.aws.amazon.com/appfabric/.
2. Erweitern Sie auf der Seite Erste Schritte das Menü auf der linken Seite.
3. Wählen Sie Ingestions.
4. Wählen Sie eine App-Autorisierung aus.
5. Wählen Sie das Optionsfeld neben dem Ziel aus, das Sie löschen möchten, und wählen Sie Löschen.
6. Wählen Sie zur Bestätigung im Dialogfeld „Ziel löschen“ die Option Löschen aus.
7. Wiederholen Sie die obigen Schritte für alle Ihre Ziele.

Löschen Sie eine Aufnahme

Gehen Sie wie folgt vor, um eine Aufnahme zu löschen:

1. Erweitern Sie auf der Seite Erste Schritte das Menü auf der linken Seite.
2. Wählen Sie Ingestions.
3. Wählen Sie das Optionsfeld neben Ihrer App-Autorisierung aus.
4. Gehen Sie zum Drop-down-Menü Aktionen.
5. Wählen Sie Löschen aus.
6. Wählen Sie zur Bestätigung im Dialogfeld „Datenerfassung löschen“ die Option Löschen aus.

Löschen Sie eine App-Autorisierung

Gehen Sie wie folgt vor, um eine App-Autorisierung zu löschen:

1. Erweitern Sie auf der Seite Erste Schritte das Menü auf der linken Seite.
2. Wählen Sie App-Autorisierungen aus.
3. Wählen Sie das Optionsfeld neben der App-Autorisierung aus, die Sie löschen möchten.
4. Gehen Sie zum Drop-down-Menü Aktionen.
5. Wählen Sie Löschen aus.
6. Wählen Sie zur Bestätigung im Dialogfeld „Datenerfassung löschen“ die Option Löschen aus.

Löschen Sie ein App-Bundle

Gehen Sie wie folgt vor, um Ihr App-Bundle zu löschen:

1. Erweitern Sie auf der Seite Erste Schritte das Menü auf der linken Seite.
2. Wählen Sie App-Bundle.
3. Wählen Sie die Schaltfläche Löschen.
4. Geben Sie `delete` zur Bestätigung ein und wählen Sie dann Löschen aus.

Was ist AWS AppFabric für die Produktivität?

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

> **Note**
>
> Bereitgestellt von Amazon Bedrock: AWS implementiert automatisierte Missbrauchserkennung. Da AWS AppFabric For Productivity auf Amazon Bedrock basiert, übernehmen die Benutzer die in Amazon Bedrock implementierten Kontrollen zur Durchsetzung von Sicherheit und verantwortungsvollem Umgang mit KI.

AWS AppFabric for Productivity (Vorversion) hilft dabei, die Produktivität von Endbenutzern in Drittanbieteranwendungen neu zu definieren, indem Erkenntnisse und Aktionen im Kontext mehrerer Anwendungen generiert werden. App-Entwickler wissen, dass der Zugriff auf Benutzerdaten aus anderen Apps wichtig ist, um ein produktiveres App-Erlebnis zu schaffen, möchten aber nicht Integrationen für jede Anwendung erstellen und verwalten. AppFabric Aus Produktivitätsgründen erhalten Anwendungsentwickler Zugriff auf generative KI-gestützte APIs, die anwendungsübergreifende Dateneinblicke und Aktionen generieren, sodass sie mithilfe neuer oder vorhandener generativer KI-Assistenten umfassendere Endbenutzererlebnisse bieten können. AppFabric for productivity integriert Daten aus mehreren Anwendungen, sodass Entwickler keine Integrationen erstellen oder verwalten müssen. point-to-point Anwendungsentwickler können aus AppFabric Produktivitätsgründen direkt in die Benutzeroberfläche ihrer Anwendung einbetten und so für ein einheitliches Benutzererlebnis sorgen und gleichzeitig relevanten Kontext aus anderen Anwendungen abrufen.

AppFabric for Productivity verbindet Daten aus häufig verwendeten Anwendungen wieAsana,Atlassian Jira Suite,Google Workspace,Microsoft 365,Miro, SlackSmartsheet, und mehr. AppFabric for productivity bietet App-Entwicklern eine einfachere Möglichkeit, personalisiertere App-Erlebnisse zu entwickeln, die die Akzeptanz, Zufriedenheit und Loyalität der Nutzer verbessern. In der Zwischenzeit profitieren Endbenutzer vom Zugriff auf Erkenntnisse, die sie benötigen, aus allen ihren Anwendungen, ohne ihren Arbeitsablauf zu unterbrechen.

Themen

- Datenverarbeitung

Vorteile

AppFabric Aus Produktivitätsgründen erhalten Anwendungsentwickler Zugriff auf APIs, die anwendungsübergreifende Dateneinblicke und Aktionen generieren, sodass sie mithilfe neuer oder vorhandener generativer KI-Assistenten umfassendere Endbenutzererlebnisse bieten können.

- Eine einzige Quelle für anwendungsübergreifende Benutzerdaten: AppFabric for Productivity integriert Daten aus mehreren Anwendungen, sodass Entwickler keine Integrationen erstellen oder verwalten müssen. point-to-point SaaS-App-Daten werden für die Verwendung in anderen Anwendungen verarbeitet, indem unterschiedliche Datentypen automatisch in ein für jede Anwendung verständliches Format normalisiert werden, sodass App-Entwickler mehr Daten integrieren können, was die Produktivität der Endbenutzer tatsächlich verbessert.
- Vollständige Kontrolle über die Benutzererfahrung: Entwickler integrieren sie aus AppFabric Produktivitätsgründen direkt in die Benutzeroberfläche ihrer Anwendung, behalten so die volle Kontrolle über die Benutzererfahrung und bieten Endbenutzern personalisierte Einblicke und Handlungsempfehlungen mit Kontext aus ihren Anwendungen. Dadurch ist AppFabric die Produktivität in der bevorzugten SaaS-Anwendung der Endbenutzer verfügbar und sie ist in der App verfügbar, die sie für die Ausführung ihrer Aufgaben bevorzugen. Endbenutzer verbringen weniger Zeit damit, zwischen Apps zu wechseln, und können im Fluss ihrer Arbeit bleiben.
- Verkürzen Sie die Markteinführungszeit: Mit einem einzigen API-Aufruf können App-Entwickler Einblicke in die generierten Benutzerdaten erhalten, ohne ein Modell feinabstimmen, eine benutzerdefinierte Aufforderung schreiben oder Integrationen für mehrere Anwendungen erstellen zu müssen. AppFabric abstrahiert diese Komplexität, sodass App-Entwickler generative KI-Funktionen schneller entwickeln, einbetten oder erweitern können. Auf diese Weise können sich App-Entwickler auf ihre Ressourcen auf die wichtigsten Aufgaben konzentrieren.
- Artefaktreferenzen zum Aufbau von Benutzervertrauen: Als Teil der Ausgabe werden aus Produktivitätsgründen relevante Artefakte oder Quelldateien angezeigt, die AppFabric zur Generierung der Erkenntnisse verwendet werden, um das Vertrauen der Endbenutzer in die LLM-Ergebnisse aufzubauen.
- Vereinfachte Benutzerberechtigungen: Benutzerartefakte, die zur Generierung von Erkenntnissen verwendet werden, basieren darauf, worauf ein Benutzer Zugriff hat. AppFabric nutzt aus Produktivitätsgründen die Berechtigungs- und Zugriffskontrolle eines ISVs als Informationsquelle.

Anwendungsfälle

App-Entwickler können For Productivity nutzen AppFabric , um die Produktivität in ihren Anwendungen neu zu definieren. AppFabric for productivity bietet zwei APIs, die sich auf die folgenden Anwendungsfälle konzentrieren, um Endbenutzern zu helfen, produktiver zu arbeiten:

- Priorisieren Sie Ihren Tag
  - Die API für umsetzbare Einblicke hilft Benutzern dabei, ihren Tag optimal zu verwalten, indem sie zeitnahe Erkenntnisse aus allen ihren Anwendungen wie E-Mails, Kalendern, Nachrichten, Aufgaben und mehr bereitstellt. Darüber hinaus können Benutzer von ihrer bevorzugten Anwendung aus anwendungsübergreifende Aktionen wie das Erstellen von E-Mails, das Planen von Besprechungen und das Erstellen von Aktionselementen ausführen. Beispielsweise sieht ein Mitarbeiter, der über Nacht eine Kundeneskalation erlebt hat, nicht nur eine Zusammenfassung der nächtlichen Konversationen, sondern kann auch eine empfohlene Maßnahme zur Planung eines Treffens mit dem Kundenbetreuer einsehen. Aktionen sind mit Pflichtfeldern (wie Name und Besitzer der Aufgabe oder E-Mail-Absender/Empfänger) vorab gefüllt, sodass bereits ausgefüllte Inhalte bearbeitet werden können, bevor die Aktion ausgeführt wird.
- Bereiten Sie sich auf bevorstehende Besprechungen vor
  - Die API zur Vorbereitung von Besprechungen hilft Benutzern dabei, sich optimal auf Besprechungen vorzubereiten, indem sie den Zweck der Besprechung zusammenfasst und relevante anwendungsübergreifende Artefakte wie E-Mails, Nachrichten und mehr anzeigt. Benutzer können sich jetzt schnell auf Besprechungen vorbereiten und müssen keine Zeit damit verschwenden, zwischen Apps zu wechseln, um nach Inhalten zu suchen.

Zugriff aus AppFabric Produktivitätsgründen

AppFabric for Productivity wird derzeit als Vorversion eingeführt und ist im Osten der USA (Nord-Virginia) erhältlich AWS-Region. Weitere Informationen zu finden Sie AWS-Regionen unter AWS AppFabric Endpunkte und Kontingente im Allgemeine AWS-Referenz.

In jeder Region können Sie aus AppFabric Produktivitätsgründen auf eine der folgenden Arten zugreifen:

- Als App-Entwickler
  - Erste Schritte mit AppFabric Produktivitätssteigerung (Vorschau) für Anwendungsentwickler
- Als Endnutzer

- Erste Schritte mit AppFabric Produktivitätssteigerung (Vorschau) für Endbenutzer

Erste Schritte mit AppFabric Produktivitätssteigerung (Vorschau) für Anwendungsentwickler

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Dieser Abschnitt unterstützt App-Entwickler bei der Integration von „ AWS AppFabric For Productivity“ (Vorschauversion) in ihre Anwendungen. AWS AppFabric For Productivity ermöglicht es Entwicklern, ihren Benutzern umfassendere App-Erlebnisse zu bieten, indem sie KI-gestützte Erkenntnisse und Aktionen aus E-Mails, Kalenderereignissen, Aufgaben, Nachrichten und mehr für mehrere Anwendungen generieren. Eine Liste der unterstützten Anwendungen finden Sie unter AWS AppFabric Unterstützte Anwendungen.

AppFabric For Productivity bietet Entwicklern die Möglichkeit, Apps in einer sicheren und kontrollierten Umgebung zu entwickeln und zu experimentieren. Wenn Sie For Productivity AppFabric zum ersten Mal verwenden, erstellen Sie einen einzelnen Testbenutzer AppClient und registrieren ihn. Dieser Ansatz soll Ihnen helfen, den Authentifizierungs- und Kommunikationsfluss zwischen Ihrer Anwendung und zu testen und zu testen AppFabric. Nachdem Sie den Test mit einem einzelnen Benutzer durchgeführt haben, können Sie Ihre Anwendung AppFabric zur Überprüfung einreichen, bevor Sie den Zugriff auf weitere Benutzer ausweiten (siheSchritt 5. Bitte AppFabric um Überprüfung Ihrer Bewerbung). AppFabric überprüft die Anwendungsinformationen, bevor eine breite Akzeptanz ermöglicht wird, um Anwendungsentwickler, Endbenutzer und deren Daten zu schützen und so den Weg für eine verantwortungsvolle Ausweitung der Benutzerakzeptanz zu ebnen.

Themen

- Voraussetzungen
- Schritt 1. Erstellen Sie einen AppFabric für mehr Produktivität AppClient
- Schritt 2. Authentifizieren und autorisieren Sie Ihre Anwendung
- Schritt 3. Fügen Sie die URL des AppFabric Benutzerportals zu Ihrer Anwendung hinzu
- Schritt 4. Wird verwendet AppFabric , um anwendungsübergreifende Einblicke und Aktionen zu erhalten
- Schritt 5. Bitte AppFabric um Überprüfung Ihrer Bewerbung

- Verwaltung im AppFabric Hinblick auf Produktivität AppClients
- Fehlerbehebung

Voraussetzungen

Bevor Sie beginnen, müssen Sie eine AWS-Konto erstellen. Weitere Informationen finden Sie unter Melden Sie sich an für ein AWS-Konto. Sie müssen außerdem mindestens einen Benutzer mit Zugriff auf die unten aufgeführte `"appfabric:CreateAppClient"` IAM-Richtlinie erstellen, mit AppFabric der der Benutzer Ihre Anwendung registrieren kann. Weitere Informationen zur Gewährung von Berechtigungen AppFabric für die Produktivitätsfunktionen finden Sie unterAppFabric für Beispiele für Produktivitätspolitik IAM. Ein Administratorbenutzer ist zwar von Vorteil, aber für die Ersteinrichtung nicht zwingend erforderlich. Weitere Informationen finden Sie unter Erstellen Sie einen Benutzer mit Administratorzugriff.

AppFabric zur Produktivitätssteigerung ist während der Vorschauphase nur in der Region USA Ost (Nord-Virginia) verfügbar. Stellen Sie sicher, dass Sie sich in dieser Region befinden, bevor Sie mit den folgenden Schritten beginnen.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Schritt 1. Erstellen Sie einen AppFabric für mehr Produktivität AppClient

Bevor Sie mit der Suche nach Erkenntnissen AppFabric zur Produktivität in Ihrer Anwendung beginnen können, müssen Sie eine AppFabric AppClient erstellen. Ein AppClient ist im Grunde Ihr Tor zu mehr AppFabric Produktivität. Er fungiert als sicherer OAuth-Anwendungsclient, der eine sichere Kommunikation zwischen Ihrer Anwendung und ermöglicht. AppFabric Wenn Sie einen erstellen AppClient, erhalten Sie eine AppClient ID, eine eindeutige Kennung, die entscheidend dafür ist, dass dieser AppFabric weiß, ob er mit Ihrer und Ihrer Anwendung funktioniert. AWS-Konto

AppFabric For Productivity bietet Entwicklern die Möglichkeit, Apps in einer sicheren und kontrollierten Umgebung zu entwickeln und zu experimentieren. Wenn Sie For Productivity AppFabric zum ersten Mal verwenden, erstellen Sie einen einzelnen Testbenutzer AppClient und registrieren ihn. Dieser Ansatz soll Ihnen helfen, den Authentifizierungs- und Kommunikationsfluss zwischen Ihrer Anwendung und zu testen und zu testen AppFabric. Nachdem Sie den Test mit einem einzelnen Benutzer durchgeführt haben, können Sie Ihre Anwendung AppFabric zur Überprüfung einreichen, bevor Sie den Zugriff auf weitere Benutzer ausweiten (sieheSchritt 5. Bitte AppFabric um Überprüfung Ihrer Bewerbung). AppFabric überprüft die Anwendungsinformationen, bevor eine breite Akzeptanz ermöglicht wird, um Anwendungsentwickler, Endbenutzer und deren Daten zu schützen und so den Weg für eine verantwortungsvolle Ausweitung der Benutzerakzeptanz zu ebnen.

Verwenden Sie die AWS AppFabric `CreateAppClient` API-Operation AppClient, um eine zu erstellen. Wenn Sie AppClient danach aktualisieren müssen, können Sie den `UpdateAppClient` API-Vorgang verwenden, um nur die RedirectUrls zu ändern. Wenn Sie einen der anderen mit Ihnen verknüpften Parameter AppClient wie AppName oder Beschreibung ändern müssen, müssen Sie den löschen AppClient und einen neuen erstellen. Weitere Informationen finden Sie unter CreateAppClient.

Sie können Ihre Anwendung mithilfe der `CreateAppClient` API bei AWS Diensten registrieren, indem Sie verschiedene Programmiersprachen verwenden, darunter Python, Node.js, Java, C#, Go und Rust. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Beispiele für Anforderungssignaturen. Um diesen API-Vorgang durchzuführen, müssen Sie Ihre Kontosignaturdaten der Version 4 verwenden. Weitere Informationen zur Signaturversion 4 finden Sie im IAM-Benutzerhandbuch unter Signieren von AWS API-Anfragen.

Felder anfordern

- `appName`- Der Name der Anwendung, der den Benutzern auf der Zustimmungsseite des AppFabric Benutzerportals angezeigt wird. Auf der Einwilligungsseite werden Endbenutzer um Erlaubnis gebeten, AppFabric Einblicke in Ihre Anwendung anzuzeigen. Einzelheiten zur Einwilligungsseite finden Sie unterSchritt 2. Erteilen Sie Ihre Zustimmung zur Anzeige von Erkenntnissen durch die App.
- `description`- Eine Beschreibung der Anwendung.
- `redirectUrls`— Der URI, zu dem Endbenutzer nach der Autorisierung weitergeleitet werden sollen. Sie können bis zu 5 Weiterleitungs-URLs hinzufügen. z. B. `https://localhost:8080`.
- `starterUserEmails`- Eine Benutzer-E-Mail-Adresse, der Zugriff auf die Erkenntnisse gewährt wird, bis die Anwendung verifiziert ist. Es ist nur eine E-Mail-Adresse zulässig. Beispiel: `anyuser@example.com`

- `customerManagedKeyIdentifier`(optional) — Der ARN des vom Kunden verwalteten Schlüssels (generiert von KMS), der zur Verschlüsselung der Daten verwendet werden soll. Wenn nicht angegeben, wird der AWS AppFabric verwaltete Schlüssel verwendet. Weitere Informationen zu AWS-eigene Schlüssel und vom Kunden verwalteten Schlüsseln finden Sie unter Kundenschlüssel und AWS Schlüssel im AWS Key Management Service Entwicklerhandbuch.

Felder für Antworten

- `appClientArn`- Der Amazon-Ressourcenname (ARN), der die AppClient ID enthält. Die AppClient ID lautet beispielsweise`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `verificationStatus`- Der AppClient Bestätigungsstatus.
  - `pending_verification`- Die Überprüfung von AppClient ist noch im Gange AppFabric. Bis zur AppClient Überprüfung von kann nur ein Benutzer (angegeben unter`starterUserEmails`) den verwenden AppClient. Dem Benutzer wird im AppFabric Benutzerportal eine Benachrichtigung angezeigt, die in eingeführt wurde und darauf hinweistSchritt 3. Fügen Sie die URL des AppFabric Benutzerportals zu Ihrer Anwendung hinzu, dass die Anwendung nicht verifiziert wurde.
  - `verified`- Der Überprüfungsprozess wurde erfolgreich abgeschlossen AppFabric und AppClient ist nun vollständig verifiziert.
  - `rejected`- Der Überprüfungsprozess für AppClient wurde von abgelehnt AppFabric. Der AppClient kann erst dann von weiteren Benutzern verwendet werden, wenn der Überprüfungsprozess erneut initiiert und erfolgreich abgeschlossen wurde.

```
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>"
}'
```

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

```
{
    "appClientConfigSummary": {
        "appClientArn": "arn:aws:appfabric:<region>:<account>:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "verificationStatus": "pending_verification"
    }
}
```

Schritt 2. Authentifizieren und autorisieren Sie Ihre Anwendung

Ermöglichen Sie Ihrer Anwendung die sichere Integration von AppFabric Erkenntnissen, indem Sie einen OAuth 2.0-Autorisierungsablauf einrichten. Zunächst müssen Sie einen Autorisierungscode erstellen, der Ihre Anwendungsidentität verifiziert. Weitere Informationen finden Sie unter Autorisieren. Anschließend tauschen Sie diesen Autorisierungscode gegen ein Zugriffstoken aus, das Ihrer Anwendung die Berechtigungen zum Abrufen und Anzeigen von AppFabric Erkenntnissen innerhalb Ihrer Anwendung gewährt. Weitere Informationen finden Sie unter Token.

Weitere Informationen zur Erteilung der Genehmigung zur Autorisierung einer Anwendung finden Sie unter. Erlauben Sie den Zugriff, um Anwendungen zu autorisieren

1. Verwenden Sie den AWS AppFabric `oauth2/authorize` API-Vorgang, um einen Autorisierungscode zu erstellen.

   Felder anfordern

   - `app_client_id`(erforderlich) — Die AppClient ID für die in Schritt 1 AWS-Konto erstellte. Erstellen Sie eine AppClient. z. B. `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
   - `redirect_uri`(erforderlich) — Der URI, zu dem Endbenutzer nach der Autorisierung, die Sie in Schritt 1 verwendet haben, umgeleitet werden sollen. Erstellen Sie eine AppClient. z. B. `https://localhost:8080`.
   - `state`(erforderlich) — Ein eindeutiger Wert, um den Status zwischen der Anfrage und dem Rückruf beizubehalten. z. B. `a8904edc-890c-1005-1996-29a757272a44`.

   ```
   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. Nach der Authentifizierung werden Sie mit einem Autorisierungscode, der als Abfrageparameter zurückgegeben wird, zur angegebenen URI weitergeleitet. Zum Beispiel wocode=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc.

```
https://localhost:8080/?code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-
sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-
oampc&state=a8904edc-890c-1005-1996-29a757272a44
```

3. Tauschen Sie diesen Autorisierungscode mithilfe der AppFabric `oauth2/token` API-Operation gegen ein Zugriffstoken aus.

   Dieses Token wird für API-Anfragen verwendet und ist zunächst gültig, `starterUserEmails` bis das verifiziert AppClient ist. Nach AppClient der Überprüfung kann dieses Token für jeden Benutzer verwendet werden. Sie müssen die Anmeldeinformationen für Version 4 Ihrer Kontosignatur verwenden, um diesen API-Vorgang auszuführen. Weitere Informationen zur Signaturversion 4 finden Sie im IAM-Benutzerhandbuch unter Signieren von AWS API-Anfragen.

   Felder anfordern

   - `code`(erforderlich) — Der Autorisierungscode, den Sie nach der Authentifizierung im letzten Schritt erhalten haben. z. B. `mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`.
   - `app_client_id`(erforderlich) — Die in Schritt 1 AWS-Konto erstellte AppClient ID. Erstellen Sie eine AppClient. z. B. `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
   - `grant_type`(erforderlich) — Der Wert muss sein`authorization_code`.
   - `redirect_uri`(erforderlich) — Der URI, zu dem Benutzer nach der Autorisierung weitergeleitet werden sollen, die Sie in Schritt 1 verwendet haben. Erstellen Sie eine AppClient. Dies muss derselbe Umleitungs-URI sein, der zum Erstellen eines Autorisierungscodes verwendet wurde. z. B. `https://localhost:8080`.

   Antwortfelder

   - `expires_in`- Wie lange dauert es, bis das Token abläuft. Die Standardablaufzeit beträgt 12 Stunden.
   - `refresh_token`— Das Aktualisierungstoken, das von der ersten /token-Anforderung empfangen wurde.

- `token`— Das Token, das von der ersten /token-Anforderung empfangen wurde.
- `token_type`- Der Wert wird sein. `Bearer`
- `appfabric_user_id`- Die AppFabric Benutzer-ID. Dies wird nur für Anfragen zurückgegeben, die den `authorization_code` Grant-Typ verwenden.

```
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\"
}"
```

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

```
{
    "expires_in": 43200,
    "refresh_token": "apkaeibaerjr2example",
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "<userId>"
}
```

Schritt 3. Fügen Sie die URL des AppFabric Benutzerportals zu Ihrer Anwendung hinzu

Endbenutzer müssen autorisiert werden, AppFabric auf Daten aus ihren Anwendungen zuzugreifen, die zur Generierung von Erkenntnissen verwendet werden. AppFabric beseitigt die Komplexität für App-Entwickler, diesen Prozess selbst in die Hand zu nehmen, indem ein spezielles Benutzerportal (ein Popup-Bildschirm) eingerichtet wird, über das Endbenutzer ihre Apps autorisieren können. Wenn Benutzer bereit sind, produktiver zu AppFabric arbeiten, werden sie zum Benutzerportal weitergeleitet, über das sie Anwendungen verbinden und verwalten können, die zur Generierung von

Erkenntnissen und anwendungsübergreifenden Aktionen verwendet werden. Wenn sie angemeldet sind, können Benutzer aus AppFabric Produktivitätsgründen eine Verbindung zu Anwendungen herstellen und dann zu Ihrer Anwendung zurückkehren, um die Erkenntnisse und Aktionen zu erkunden. Um Ihre Anwendung in AppFabric for productivity zu integrieren, müssen Sie Ihrer Anwendung eine bestimmte AppFabric URL hinzufügen. Dieser Schritt ist entscheidend, damit Benutzer direkt von Ihrer Anwendung aus auf das AppFabric Benutzerportal zugreifen können.

1. Navigieren Sie zu den Einstellungen Ihrer Anwendung und suchen Sie den Abschnitt zum Hinzufügen von Weiterleitungs-URLs.
2. Nachdem Sie den entsprechenden Bereich gefunden haben, fügen Sie Ihrer Anwendung die folgende AppFabric URL als Weiterleitungs-URL hinzu:

```
https://userportal.appfabric.<region>.amazonaws.com/eup_login
```

Nachdem Sie die URL hinzugefügt haben, wird Ihre Anwendung so eingerichtet, dass sie Benutzer zum AppFabric Benutzerportal weiterleitet. Hier können sich Benutzer anmelden, eine Verbindung herstellen und ihre Anwendungen verwalten, die AppFabric zur Generierung von Produktivitätseinblicken verwendet werden.

Schritt 4. Wird verwendet AppFabric , um anwendungsübergreifende Einblicke und Aktionen zu erhalten

Nachdem Benutzer ihre Anwendungen miteinander verbunden haben, können Sie die Erkenntnisse Ihrer Benutzer nutzen, um deren Produktivität zu verbessern, indem Sie dazu beitragen, das Wechseln zwischen Anwendungen und Kontexten zu reduzieren. AppFabric generiert nur Erkenntnisse für einen Benutzer auf der Grundlage dessen, wofür der Benutzer Zugriffsrechte besitzt. AppFabric speichert Benutzerdaten in einem AWS-Konto Eigentum von AppFabric. Informationen darüber, wie Ihre Daten AppFabric verwendet werden, finden Sie unterDatenverarbeitung.

Sie können die folgenden KI-gestützten APIs verwenden, um Erkenntnisse und Aktionen auf Benutzerebene in Ihren Apps zu generieren und aufzudecken:

- `ListActionableInsights`— Weitere Informationen finden Sie weiter unten im Abschnitt „Umsetzbare Erkenntnisse“.
- `ListMeetingInsights`— Weitere Informationen finden Sie im Abschnitt zur Vorbereitung von Besprechungen weiter unten in diesem Handbuch.

Umsetzbare Erkenntnisse () **`ListActionableInsights`**

Die `ListActionableInsights` API hilft Benutzern dabei, ihren Tag am besten zu verwalten und liefert umsetzbare Erkenntnisse auf der Grundlage der Aktivitäten in ihren Anwendungen, einschließlich E-Mails, Kalendern, Nachrichten, Aufgaben und mehr. Bei zurückgegebenen Erkenntnissen werden auch eingebettete Links zu Artefakten angezeigt, die zur Generierung der Erkenntnisse verwendet wurden. So können Benutzer schnell erkennen, welche Daten zur Generierung der Erkenntnisse verwendet wurden. Darüber hinaus kann die API basierend auf den Erkenntnissen vorgeschlagene Aktionen zurückgeben und es Benutzern ermöglichen, anwendungsübergreifende Aktionen von Ihrer Anwendung aus auszuführen. Insbesondere lässt sich die API in Plattformen wieAsana,, und integrieren Google WorkspaceMicrosoft 365, Smartsheet um Benutzern das Senden von E-Mails, das Erstellen von Kalendereereignissen und das Erstellen von Aufgaben zu ermöglichen. Die Large Language Models (LLMs) können Details im Rahmen einer empfohlenen Aktion (wie E-Mail-Text oder Aufgabenname) vorab ausfüllen, die Benutzer vor der Ausführung anpassen können, was die Entscheidungsfindung vereinfacht und die Produktivität steigert. Ähnlich wie bei der Autorisierung von Anwendungen durch Endbenutzer wird dasselbe spezielle Portal AppFabric verwendet, über das Benutzer anwendungsübergreifende Aktionen anzeigen, bearbeiten und ausführen können. Für die Ausführung von Aktionen AppFabric müssen ISVs Benutzer zu einem AppFabric Benutzerportal weiterleiten, wo sie die Aktionsdetails einsehen und diese ausführen können. Jede von generierte Aktion AppFabric hat eine eindeutige URL. Diese URL ist in der Antwort auf die `ListActionableInsights` API-Antwort verfügbar.

Im Folgenden finden Sie eine Zusammenfassung der unterstützten anwendungsübergreifenden Aktionen und der Apps, in denen:

- E-Mail senden (Google Workspace,Microsoft 365)
- Kalendereereignis erstellen (Google Workspace,Microsoft 365)
- Aufgabe erstellen (Asana,Smartsheet)

Felder anfordern

- `nextToken`(optional) — Das Paginierungstoken zum Abrufen der nächsten Reihe von Erkenntnissen.
- `includeActionExecutionStatus`— Ein Filter, der eine Liste von Statusangaben bei der Ausführung von Aktionen akzeptiert. Die Aktionen werden auf der Grundlage der übergebenen Statuswerte gefiltert. Mögliche Werte: `NOT_EXECUTED` | `EXECUTED`

Header der Anfrage

- Der Autorisierungsheader muss zusammen mit dem `Bearer Token` Wert übergeben werden.

Antwortfelder

- `insightId`- Die eindeutige ID für den generierten Einblick.
- `insightContent`- Dies gibt eine Zusammenfassung der Erkenntnisse und eingebettete Links zu Artefakten zurück, die zur Generierung der Erkenntnisse verwendet wurden. Hinweis: Dies wäre ein HTML-Inhalt, der eingebettete Links (<a>Tags) enthält.
- `insightTitle`- Der Titel des generierten Einblicks.
- `createdAt`- Wann der Insight generiert wurde.
- `actions`- Eine Liste von Aktionen, die für den generierten Einblick empfohlen werden. Aktionsobjekt:
  - `actionId`- Die eindeutige ID für die generierte Aktion.
  - `actionIconUrl`- Die Symbol-URL für die App, in der die Aktion ausgeführt werden soll.
  - `actionTitle`- Der Titel der generierten Aktion.
  - `actionUrl`- Die eindeutige URL, über die der Endbenutzer die Aktion im AppFabric Benutzerportal anzeigen und ausführen kann. Hinweis: Für die Ausführung von Aktionen leiten ISV-Apps Benutzer mithilfe dieser URL zum AppFabric Benutzerportal (Popup-Bildschirm) weiter.
  - `actionExecutionStatus`- Eine Aufzählung, die den Status der Aktion angibt. Die möglichen Werte sind: | `EXECUTED` `NOT_EXECUTED`
- `nextToken`(optional) — Das Paginierungstoken zum Abrufen der nächsten Reihe von Erkenntnissen. Es ist ein optionales Feld, das, wenn es Null zurückgegeben wird, bedeutet, dass keine weiteren Erkenntnisse geladen werden müssen.

Weitere Informationen finden Sie unter ActionableInsights.

```
curl -v --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/actionableInsights" \
  --header "Authorization: Bearer <token>"
```

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

```
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
```

```
}
```

Vorbereitung des Treffens (**`ListMeetingInsights`**)

Die `ListMeetingInsights` API hilft Benutzern dabei, sich optimal auf bevorstehende Besprechungen vorzubereiten, indem sie den Zweck der Besprechung zusammenfasst und relevante anwendungsübergreifende Artefakte wie E-Mails, Nachrichten und mehr anzeigt. Benutzer können sich jetzt schnell auf Besprechungen vorbereiten und müssen keine Zeit damit verschwenden, zwischen Apps zu wechseln, um Inhalte zu finden.

Felder anfordern

- `nextToken`(optional) — Das Paginierungstoken zum Abrufen der nächsten Reihe von Erkenntnissen.

Header anfordern

- Der Autorisierungsheader muss zusammen mit dem `Bearer Token` Wert übergeben werden.

Antwortfelder

- `insightId`- Die eindeutige ID für den generierten Einblick.
- `insightContent`- Die Beschreibung der Einsicht, in der die Details in einem Zeichenkettenformat hervorgehoben werden. Zum Beispiel, warum diese Einsicht wichtig ist.
- `insightTitle`- Der Titel des generierten Einblicks.
- `createdAt`- Wann der Insight generiert wurde.
- `calendarEvent`- Das wichtige Kalenderereignis oder die wichtige Besprechung, auf die sich der Benutzer konzentrieren sollte. Objekt „Kalenderereignis“:
  - `startTime`- Die Startzeit des Ereignisses.
  - `endTime`- Die Endzeit der Veranstaltung.
  - `eventUrl`— Die URL für das Kalenderereignis in der ISV-App.
- `resources`- Die Liste mit den anderen Ressourcen, die sich auf die Generierung der Erkenntnisse beziehen. Ressourcenobjekt:
  - `appName`- Der Name der App, zu der die Ressource gehört.
  - `resourceTitle`- Der Titel der Ressource.

  - `resourceType`- Der Typ der Ressource. Die möglichen Werte sind: `EMAIL` | `EVENT` | `MESSAGE` | `TASK`
  - `resourceUrl`- Die Ressourcen-URL in der App.
  - `appIconUrl`- Die Bild-URL der App, zu der die Ressource gehört.
- `nextToken`(optional) — Das Paginierungstoken zum Abrufen der nächsten Reihe von Erkenntnissen. Es ist ein optionales Feld, das, wenn es Null zurückgegeben wird, bedeutet, dass keine weiteren Erkenntnisse geladen werden müssen.

Weitere Informationen finden Sie unter MeetingInsights.

```
curl --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/meetingContexts" \
  --header "Authorization: Bearer <token>"
```

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP-201-Antwort zurück.

```
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
}
```

Geben Sie Feedback zu Ihren Erkenntnissen oder Aktionen

Verwenden Sie den AppFabric `PutFeedback` API-Vorgang, um Feedback zu den generierten Erkenntnissen und Aktionen zu geben. Sie können diese Funktion in Ihre Apps einbetten, um die

Möglichkeit zu bieten, eine Feedback-Bewertung (1 bis 5, wobei je höher die Bewertung desto besser) für ein bestimmtes InsightId oder abzugeben ActionId.

Felder anfordern

- `id`- Die Kennung des Objekts, für das Feedback eingereicht wird. Dies kann entweder der InsightId oder der sein ActionId.
- `feedbackFor`- Der Ressourcentyp, für den Feedback eingereicht wird. Mögliche Werte: `ACTIONABLE_INSIGHT` | `MEETING_INSIGHT` | `ACTION`
- `feedbackRating`- Feedback-Bewertung von `1` bis`5`. Je höher die Bewertung, desto besser.

Antwortfelder

- Es gibt keine Antwortfelder.

Weitere Informationen finden Sie unter PutFeedback.

```
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
}'
```

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP-201-Antwort mit leerem HTTP-Textinhalt zurück.

Schritt 5. Bitte AppFabric um Überprüfung Ihrer Bewerbung

Bis jetzt haben Sie die Benutzeroberfläche Ihrer Anwendung aktualisiert, um AppFabric anwendungsübergreifende Einblicke und Aktionen einzubetten, und Sie haben Erkenntnisse für einen einzelnen Benutzer erhalten. Wenn Sie mit den Tests zufrieden sind und Ihr AppFabric erweitertes Nutzererlebnis auf weitere Nutzer ausweiten möchten, können Sie Ihren Antrag AppFabric zur Prüfung und Überprüfung bei uns einreichen. AppFabric überprüft die Anwendungsinformationen, bevor eine breite Akzeptanz ermöglicht wird, um Anwendungsentwickler, Endbenutzer und deren

Daten zu schützen und so den Weg für eine verantwortungsvolle Ausweitung der Benutzerakzeptanz zu ebnen.

Leitet den Überprüfungsprozess ein

Beginnen Sie den Überprüfungsprozess, indem Sie eine E-Mail an appfabric-appverification@amazon.com senden und darum bitten, dass Ihre App verifiziert wird.

Geben Sie in Ihrer E-Mail die folgenden Informationen an:

- Deine AWS-Konto ID
- Der Name der Anwendung, für die Sie eine Bestätigung beantragen
- Ihr AppClient Ausweis
- Deine Kontaktinformationen

Geben Sie außerdem, falls verfügbar, die folgenden Informationen an, damit wir Prioritäten und Auswirkungen beurteilen können:

- Eine geschätzte Anzahl von Benutzern, denen Sie Zugriff gewähren möchten
- Ihr angestrebter Starttermin

> **Note**
>
> Wenn Sie einen AWS-Konto Manager oder AWS Partner Development Manager haben, kopieren Sie ihn bitte in Ihre E-Mail. Die Angabe dieser Kontakte kann dazu beitragen, den Überprüfungsprozess zu beschleunigen.

Kriterien für die Überprüfung

Bevor Sie den Überprüfungsprozess einleiten können, müssen Sie die folgenden Kriterien erfüllen:

- Aus Produktivitätsgründen müssen Sie ein gültiges AWS-Konto Passwort verwenden AppFabric

Darüber hinaus erfüllen Sie mindestens eines der folgenden Kriterien:

- Ihre Organisation ist ein AWS Partner auf der Stufe AWS Partner Network mit mindestens der Stufe „AWS Select“. Weitere Informationen finden Sie unter Stufen der AWS Partnerservices.

- Ihr Unternehmen sollte in den letzten drei Jahren mindestens 10.000$ für AppFabric Dienstleistungen ausgegeben haben.
- Ihre Bewerbung sollte auf der AWS Marketplace aufgeführt sein. Weitere Informationen finden Sie im AWS Marketplace.

Warten Sie auf die Aktualisierung des Bestätigungsstatus

Nachdem Ihre Bewerbung geprüft wurde, antworten wir per E-Mail und der Status Ihrer Bewerbung AppClient ändert sich von `pending_verification` zu`verified`. Wenn Ihre Bewerbung abgelehnt wird, müssen Sie den Überprüfungsprozess erneut einleiten.

Verwaltung im AppFabric Hinblick auf Produktivität AppClients

> Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Sie können Ihre AppFabric Produktivität verwalten, AppClients um den reibungslosen Betrieb und die Aufrechterhaltung der Authentifizierungs- und Autorisierungsprozesse sicherzustellen.

Erfahren Sie mehr über ein AppClient

Verwenden Sie den AppFabric `GetAppClient` API-Vorgang, um Details zu Ihrem anzuzeigen AppClient, einschließlich der Überprüfung des AppClient Status. Weitere Informationen finden Sie unter GetAppClient.

Um Details zu einem zu erhalten AppClient, müssen Sie mindestens über die `"appfabric:GetAppClient"` IAM-Richtlinienberechtigungen verfügen. Weitere Informationen finden Sie unter Erlauben Sie den Zugriff, um Details zu erhalten AppClients.

Felder anfordern

- `appClientId`- Die AppClient ID.

Antwortfelder

- `appName`- Der Name der Anwendung, die den Benutzern auf der Zustimmungsseite des AppFabric Benutzerportals angezeigt wird.

- `customerManagedKeyIdentifier`(optional) — Der ARN des vom Kunden verwalteten Schlüssels (generiert von KMS), der zur Verschlüsselung der Daten verwendet werden soll. Wenn nicht angegeben, wird der AWS AppFabric verwaltete Schlüssel verwendet.
- `description`- Eine Beschreibung der Anwendung.
- `redirectUrls`— Der URI, zu dem Endbenutzer nach der Autorisierung weitergeleitet werden sollen. Sie können bis zu 5 Weiterleitungs-URLs hinzufügen. z. B. `https://localhost:8080`.
- `starterUserEmails`- Eine Benutzer-E-Mail-Adresse, der Zugriff auf die Erkenntnisse gewährt wird, bis die Anwendung verifiziert ist. Es ist nur eine E-Mail-Adresse zulässig. z. B. `anyuser@example.com`.
- `verificationStatus`- Der AppClient Bestätigungsstatus.
  - `pending_verification`- Die Überprüfung von AppClient ist noch im Gange AppFabric. Bis zur AppClient Überprüfung von kann nur ein Benutzer (angegeben unter`starterUserEmails`) den verwenden AppClient.
  - `verified`- Der Überprüfungsprozess wurde erfolgreich abgeschlossen AppFabric und AppClient ist nun vollständig verifiziert.
  - `rejected`- Der Überprüfungsprozess für AppClient wurde von abgelehnt AppFabric. Der AppClient kann erst dann von weiteren Benutzern verwendet werden, wenn der Überprüfungsprozess erneut initiiert und erfolgreich abgeschlossen wurde.

```
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
```

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

```
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"
        }
    }
}
```

Liste AppClients

Verwenden Sie den AppFabric `ListAppClients` API-Vorgang, um eine Liste Ihrer anzuzeigen AppClients. AppFabric erlaubt nur einen AppClient pro AWS-Konto. Dies kann sich in future ändern. Weitere Informationen finden Sie unter ListAppClients.

Um die Liste auflisten AppClients zu können, müssen Sie mindestens über die `"appfabric:ListAppClients"` IAM-Richtlinienberechtigungen verfügen. Weitere Informationen finden Sie unter Erlauben Sie den Zugriff auf die Liste AppClients.

Felder anfordern

- Es gibt keine Pflichtfelder.

Felder für Antworten

- `appClientARN`- Der Amazon-Ressourcenname (ARN), der die AppClient ID enthält. Die AppClient ID lautet beispielsweise`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `verificationStatus`- Der AppClient Bestätigungsstatus.
  - `pending_verification`- Die Überprüfung von AppClient ist noch im Gange AppFabric. Bis zur AppClient Überprüfung von kann nur ein Benutzer (angegeben unter`starterUserEmails`) den verwenden AppClient.
  - `verified`- Der Überprüfungsprozess wurde erfolgreich abgeschlossen AppFabric und AppClient ist nun vollständig verifiziert.

- `rejected`- Der Überprüfungsprozess für AppClient wurde von abgelehnt AppFabric. Der AppClient kann erst dann von weiteren Benutzern verwendet werden, wenn der Überprüfungsprozess erneut initiiert und erfolgreich abgeschlossen wurde.

```
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
```

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

```
200 OK

{
    "appClientList": [
        {
            "appClientArn": "arn:aws:appfabric:<region>:111122223333:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "verificationStatus": "pending_verification"
        }
    ]
}
```

Aktualisieren Sie ein AppClient

Verwenden Sie den AppFabric `UpdateAppClient` API-Vorgang, um die Ihren zugewiesenen Redirect-URLs zu aktualisieren. AppClient Wenn Sie andere Parameter wie, oder andere ändern müssen AppName starterUserEmails, müssen Sie diese löschen AppClient und einen neuen erstellen. Weitere Informationen finden Sie unter UpdateAppClient.

Um einen zu aktualisieren AppClient, müssen Sie mindestens über die `"appfabric:UpdateAppClient"` IAM-Richtlinienberechtigungen verfügen. Weitere Informationen finden Sie unter Erlauben Sie den Zugriff auf das Update AppClients.

Felder anfordern

- `appClientId`(erforderlich) — Die AppClient ID, mit der Sie die Redirect-URLs aktualisieren.

- `redirectUrls`(erforderlich) — Die aktualisierte Liste der RedirectURLs. Sie können bis zu 5 RedirectURLs hinzufügen.

Antwortfelder

- `appName`- Der Name der Anwendung, die den Benutzern auf der Zustimmungsseite des AppFabric Benutzerportals angezeigt wird.
- `customerManagedKeyIdentifier`(optional) — Der ARN des vom Kunden verwalteten Schlüssels (generiert von KMS), der zur Verschlüsselung der Daten verwendet werden soll. Wenn nicht angegeben, wird der AWS AppFabric verwaltete Schlüssel verwendet.
- `description`- Eine Beschreibung der Anwendung.
- `redirectUrls`— Der URI, zu dem Endbenutzer nach der Autorisierung weitergeleitet werden sollen. z. B. `https://localhost:8080`.
- `starterUserEmails`- Eine Benutzer-E-Mail-Adresse, der Zugriff gewährt wird, um die Erkenntnisse zu erhalten, bis die Anwendung verifiziert ist. Es ist nur eine E-Mail-Adresse zulässig. z. B. `anyuser@example.com`.
- `verificationStatus`- Der AppClient Bestätigungsstatus.
  - `pending_verification`- Die Überprüfung von AppClient ist noch im Gange AppFabric. Bis zur AppClient Überprüfung von kann nur ein Benutzer (angegeben unter`starterUserEmails`) den verwenden AppClient.
  - `verified`- Der Überprüfungsprozess wurde erfolgreich abgeschlossen AppFabric und AppClient ist nun vollständig verifiziert.
  - `rejected`- Der Überprüfungsprozess für AppClient wurde von abgelehnt AppFabric. Der AppClient kann erst dann von weiteren Benutzern verwendet werden, wenn der Überprüfungsprozess erneut initiiert und erfolgreich abgeschlossen wurde.

```
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"]
```

```
}'
```

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

```
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"
        }
    }
}
```

Löschen Sie ein AppClient

Verwenden Sie den AppFabric `DeleteAppClient` API-Vorgang, um alle zu löschen, die AppClients Sie nicht mehr benötigen. Weitere Informationen finden Sie unter DeleteAppClient.

Um eine zu löschen AppClient, müssen Sie mindestens über die `"appfabric:DeleteAppClient"` IAM-Richtlinienberechtigungen verfügen. Weitere Informationen finden Sie unter Erlauben Sie den Zugriff zum Löschen AppClients.

Felder anfordern

- `appClientId`- Die AppClient ID.

Antwortfelder

- Es gibt keine Antwortfelder.

```
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
```

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP-204-Antwort mit leerem HTTP-Textinhalt zurück.

Tokens für Endbenutzer aktualisieren

Die Token, die AppClient Sie für Endbenutzer erwerben, können nach Ablauf aktualisiert werden. Dies kann mithilfe der Token API mit dem `refresh_token` Grant_Type erfolgen. Der `refresh_token` zu verwendende Wert wird als Teil der Token-API-Antwort zurückgegeben, wenn der Grant_Type `authorization_code` Die Standardablaufzeiten sind 12 Stunden.
Um die Aktualisierungs-API aufzurufen, benötigen Sie die `"appfabric:Token"` IAM-Richtlinienberechtigung. Weitere Informationen finden Sie unter Token und Erlauben Sie den Zugriff auf das Update AppClients.

Felder anfordern

- `refresh_token`(erforderlich) — Das Aktualisierungstoken, das bei der ersten `/token` Anfrage empfangen wurde.
- `app_client_id`(erforderlich) — Die ID der AppClient Ressource, die für die erstellt wurde AWS-Konto.
- `grant_type`(erforderlich) — Das muss sein`refresh_token`.

Antwortfelder

- `expires_in`- Wie lange dauert es, bis das Token abläuft. Die Standardablaufzeit beträgt 12 Stunden.
- `refresh_token`— Das Aktualisierungstoken, das von der ersten /token-Anforderung empfangen wurde.
- `token`— Das Token, das von der ersten /token-Anforderung empfangen wurde.
- `token_type`- Der Wert wird sein. `Bearer`

- `appfabric_user_id`- Die AppFabric Benutzer-ID. Dies wird nur für Anfragen zurückgegeben, die den `authorization_code` Grant-Typ verwenden.

```
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\"
}"
```

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

```
200 OK

{
    "expires_in": 43200,
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "${UserID}"
}
```

Fehlerbehebung

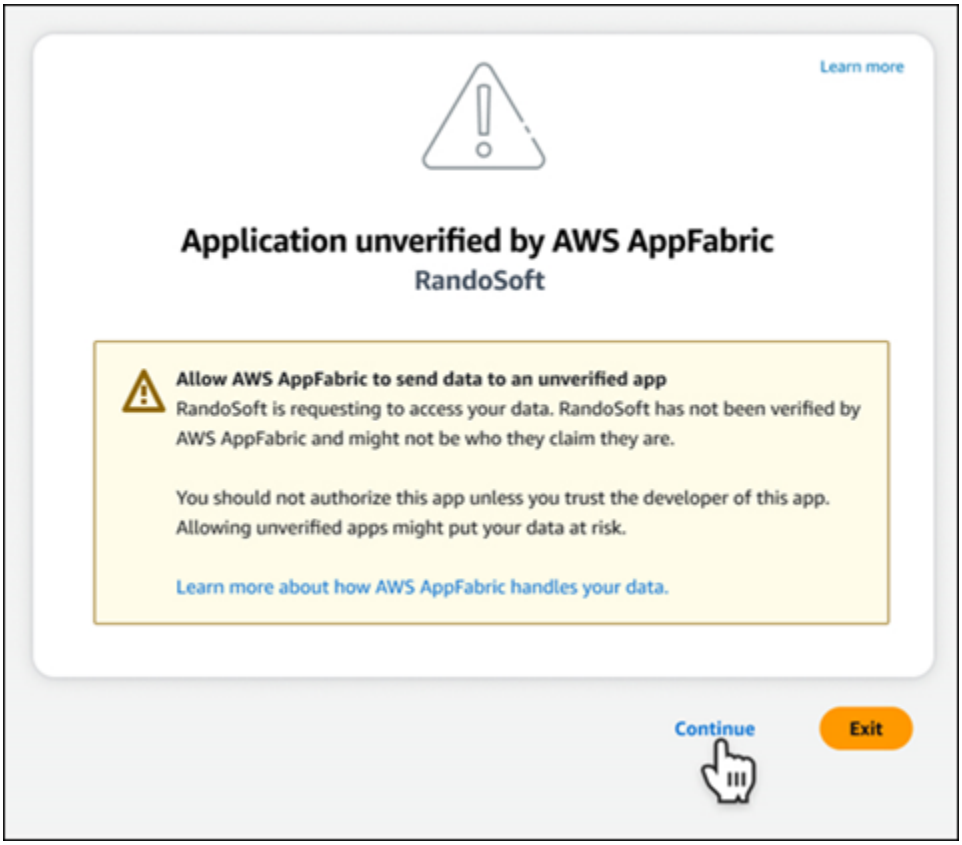
Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

In diesem Abschnitt werden häufig auftretende Fehler und Problembehebungen aus AppFabric Produktivitätsgründen beschrieben.

Unbestätigter Antrag

App-Entwickler, die aus AppFabric Produktivitätsgründen ihr App-Erlebnis bereichern, werden vor der Einführung ihrer Funktionen für Endbenutzer einen Verifizierungsprozess durchlaufen.

Alle Anwendungen beginnen als nicht verifiziert und werden erst dann zu verifiziert, wenn der Überprüfungsprozess abgeschlossen ist. Dies bedeutet, dass das, was `starterUserEmails` Sie beim Erstellen eines verwendet haben, diese Meldung sehen AppClient wird.



`CreateAppClient`-Fehler

ServiceQuotaExceededException

Wenn Sie beim Erstellen einer die folgende Ausnahme erhalten AppClient, haben Sie die Anzahl der Dateien überschritten AppClients , die pro erstellt werden können AWS-Konto. Das Limit ist 1. HTTPStatuscode: 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-Fehler

ResourceNotFoundException

Wenn Sie beim Abrufen von Informationen zu einem die folgende Ausnahme erhalten AppClient, stellen Sie sicher, dass Sie die richtige AppClient Kennung eingegeben haben. Dieser Fehler bedeutet, dass die angegebene Datei nicht gefunden AppClient wurde.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you’ve entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

DeleteAppClient-Fehler

ConflictException

Wenn Sie beim Löschen eines die folgende Ausnahme erhalten AppClient, wird gerade eine weitere Löschanforderung ausgeführt. Warten Sie, bis der Vorgang abgeschlossen ist, und versuchen Sie es dann erneut. HTTPStatuscode: 409

```
ConflictException
Another delete request is in progress. Wait until it completes then try again.
HTTP Status Code: 409
```

ResourceNotFoundException

Wenn Sie beim Löschen eines die folgende Ausnahme erhalten AppClient, stellen Sie sicher, dass Sie den richtigen AppClient Bezeichner eingegeben haben. Dieser Fehler bedeutet, dass die angegebene Datei nicht gefunden AppClient wurde.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you’ve entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

`UpdateAppClient`-Fehler

ResourceNotFoundException

Wenn Sie beim Aktualisieren von die folgende Ausnahme erhalten AppClient, stellen Sie sicher, dass Sie den richtigen AppClient Bezeichner eingegeben haben. Dieser Fehler bedeutet, dass die angegebene Datei nicht gefunden AppClient wurde.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

`Authorize`-Fehler

ValidationException

Möglicherweise wird die folgende Ausnahme angezeigt, wenn einer der API Parameter die in den API Spezifikationen definierten Einschränkungen nicht erfüllt.

```
ValidationException
HTTP Status Code: 400
```

Grund 1: Wenn die AppClient ID nicht angegeben ist

Das `app_client_id` fehlt in den Anforderungsparametern. Erstellen Sie das AppClient, falls es noch nicht erstellt wurde, oder verwenden Sie Ihr vorhandenes `app_client_id` und versuchen Sie es erneut. Verwenden Sie die ListAppClientAPIOperation, um die AppClient ID zu finden.

Grund 2: Wann AppFabric hat er keinen Zugriff auf den vom Kunden verwalteten Schlüssel

```
Message: AppFabric couldn't access the customer managed key configured for AppClient.
```

AppFabric kann derzeit nicht auf die vom Kunden verwalteten Schlüssel zugreifen, was wahrscheinlich auf kürzliche Änderungen seiner Berechtigungen zurückzuführen ist. Stellen Sie sicher, dass der angegebene Schlüssel vorhanden AppFabric ist, und stellen Sie sicher, dass ihm die entsprechenden Zugriffsberechtigungen erteilt wurden.

Grund 3: Die URL angegebene Weiterleitung ist nicht gültig

```
Message: Redirect url invalid
```

Stellen Sie sicher, dass die Weiterleitung URL in Ihrer Anfrage korrekt ist. Sie muss mit einer der Weiterleitungen übereinstimmen, die Sie bei der Erstellung oder Aktualisierung der URLs angegeben haben AppClient. Verwenden Sie den GetAppClientAPIVorgangURLs, um die Liste der zulässigen Weiterleitungen anzuzeigen.

Token-Fehler

TokenException

Möglicherweise wird Ihnen aus verschiedenen Gründen die folgende Ausnahme angezeigt.

```
TokenException
HTTP Status Code: 400
```

Grund 1: Wenn eine ungültige E-Mail-Adresse angegeben wird

```
Message: Invalid Email used
```

Stellen Sie sicher, dass die E-Mail-Adresse, die Sie verwenden, mit der übereinstimmt, die für das `starterUserEmails` Attribut aufgeführt wurde, als Sie das erstellt haben AppClient. Wenn die E-Mails nicht übereinstimmen, wechseln Sie zur entsprechenden E-Mail-Adresse und versuchen Sie es erneut. Verwenden Sie den GetAppClientAPIVorgang, um die verwendete E-Mail anzuzeigen.

Grund 2: Für grant_type als refresh_token, wenn das Token nicht angegeben ist.

```
Message: refresh_token must be non-null for Refresh Token Grant-type
```

Das in der Anfrage angegebene Aktualisierungstoken ist Null oder leer. Geben Sie in der APIToken-Anrufantwort ein aktives `refresh_token` Objekt an.

ThrottlingException

Möglicherweise erhalten Sie die folgende Ausnahme, wenn die API Geschwindigkeit, mit der das zulässige Kontingent überschritten wird, aufgerufen wird.

```
ThrottlingException
HTTP Status Code: 429
```

`ListActionableInsights` `ListMeetingInsights`, und **`PutFeedback`** Fehler

ValidationException

Möglicherweise wird die folgende Ausnahme angezeigt, wenn einer der API Parameter die in den API Spezifikationen definierte Einschränkung nicht erfüllt.

```
ValidationException
HTTP Status Code: 400
```

ThrottlingException

Möglicherweise wird die folgende Ausnahme angezeigt, wenn der mit einer Geschwindigkeit aufgerufen API wird, die über dem zulässigen Kontingent liegt.

```
ThrottlingException
HTTP Status Code: 429
```

Erste Schritte mit AppFabric Produktivitätssteigerung (Vorschau) für Endbenutzer

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Dieser Abschnitt richtet sich an Endbenutzer von SaaS-Anwendungen, die die Produktivitätssteigerung (Vorschau) aktivieren AWS AppFabric möchten, um ihr Aufgabenmanagement und ihre Workflow-Effizienz zu verbessern. Gehen Sie wie folgt vor, um Ihre Anwendungen zu verbinden und AppFabric um Zugriff auf anwendungsübergreifende Einblicke zu erhalten und Ihnen zu helfen, Aktionen (z. B. eine E-Mail zu senden oder ein Meeting zu vereinbaren) von Ihren bevorzugten Anwendungen aus durchzuführen. Sie können Anwendungen wieAsana,,Atlassian Jira Suite,Google Workspace, Microsoft 365 Miro SlackSmartsheet, und mehr verbinden. Nachdem Sie AppFabric den Zugriff auf Ihre Inhalte autorisiert haben, AppFabric bietet es anwendungsübergreifende Einblicke und Aktionen direkt in Ihren bevorzugten Apps. So können Sie effizienter arbeiten und Ihre aktuellen Workflows einhalten.

AppFabric for productivity verwendet generative KI, die von Amazon Bedrock unterstützt wird. AppFabric generiert Erkenntnisse und Maßnahmen erst, wenn Sie Ihre ausdrückliche Genehmigung erhalten haben. Sie autorisieren jede einzelne Anwendung, die volle Kontrolle darüber zu behalten,

welche Inhalte verwendet werden. AppFabric wird Ihre Daten nicht verwenden, um die zugrunde liegenden großen Sprachmodelle zu trainieren oder zu verbessern, die zur Gewinnung von Erkenntnissen verwendet werden. Weitere Informationen finden Sie auf Amazon Bedrock FAQs.

Themen

Voraussetzungen

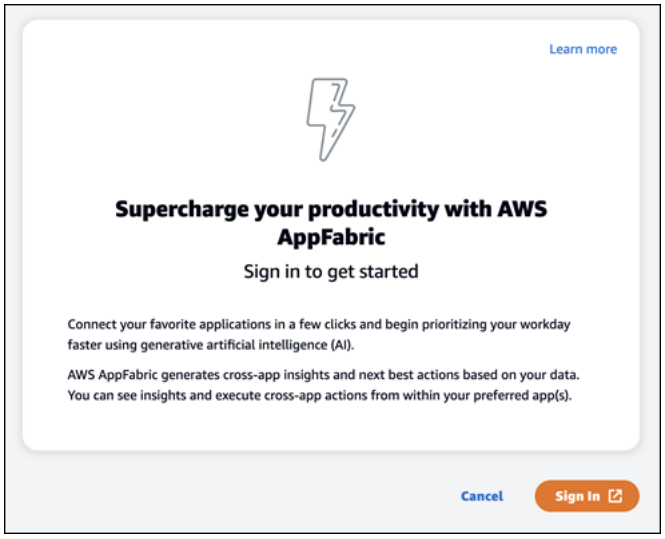
Bevor Sie beginnen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Anmeldeinformationen AppFabric für die Anmeldung AppFabric: Um mit der Nutzung aus Produktivitätsgründen beginnen zu können, benötigen Sie Verbundanmeldedaten (Benutzername und Passwort) für einen der folgenden Anbieter:Asana, Google WorkspaceMicrosoft 365, oder. Slack Wenn Sie sich anmelden, AppFabric können wir Sie als Benutzer für jede Anwendung identifizieren, die Sie aus AppFabric Produktivitätsgründen aktivieren. Nachdem Sie sich angemeldet haben, können Sie Ihre Anwendungen verbinden, um Erkenntnisse zu generieren.
- Anmeldeinformationen für die Verbindung Ihrer Anwendungen: App-übergreifende Einblicke und Aktionen werden nur auf der Grundlage von Anwendungen generiert, die Sie autorisieren. Sie benötigen Anmeldedaten (Benutzername und Passwort) für jede der Anwendungen, die Sie autorisieren möchten. Zu den unterstützten Anwendungen gehören AsanaAtlassian Jira Suite,Google Workspace,Microsoft 365, MiroSlack, und. Smartsheet

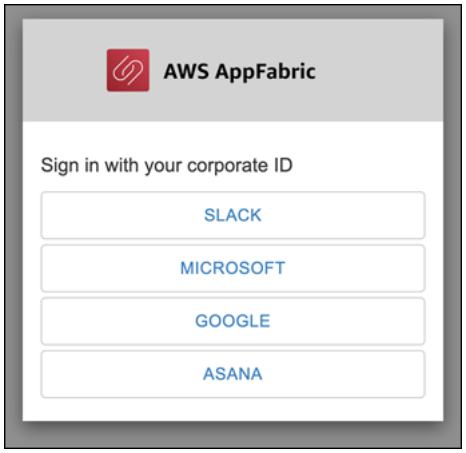
Schritt 1. Melden Sie sich an bei AppFabric

Verbinden Sie Anwendungen mit AppFabric , um Ihre Inhalte und Erkenntnisse direkt in Ihre bevorzugten Anwendungen zu integrieren.

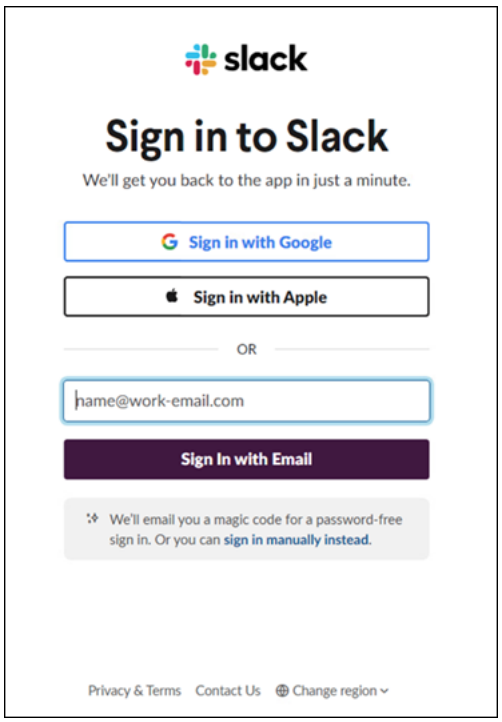
1. Jede Anwendung wird auf unterschiedliche Weise AppFabric zur Steigerung der Produktivität genutzt, um Ihnen ein umfassenderes App-Erlebnis zu bieten. Aus diesem Grund hat jede Anwendung einen anderen Einstiegspunkt, über den Sie auf die unten stehende Startseite AppFabric für Produktivitätsaspekte gelangen. Die Startseite legt den Kontext für den zu aktivierenden Prozess fest AppFabric und fordert Sie zunächst auf, sich anzumelden. Jede Anwendung, die Sie aktivieren möchten, wird AppFabric auf diesem Bildschirm angezeigt.

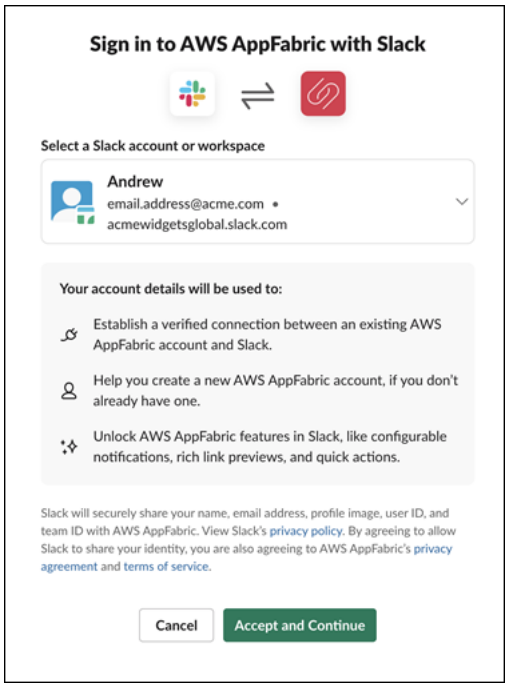


2. Melden Sie sich mit Ihren Anmeldeinformationen von einem der folgenden Anbieter an: AsanaGoogle Workspace,Microsoft 365, oderSlack. Für eine optimale Benutzererfahrung empfehlen wir, sich für jede Anwendung, die Sie aktivieren, mit demselben Anbieter AppFabric anzumelden. Wenn du zum Beispiel Google Workspace-Anmeldedaten in App1 auswählst, empfehlen wir, dich Google Workspace in App2 zu entscheiden, ebenso wie jedes Mal, wenn du dich erneut anmelden musst. Wenn du dich mit einem anderen Anbieter anmeldest, musst du den Verbindungsprozess der Anwendungen neu starten.



3. Wenn Sie dazu aufgefordert werden, geben Sie Ihre Anmeldeinformationen ein und akzeptieren Sie die Anmeldung AppFabric bei diesem Anbieter.

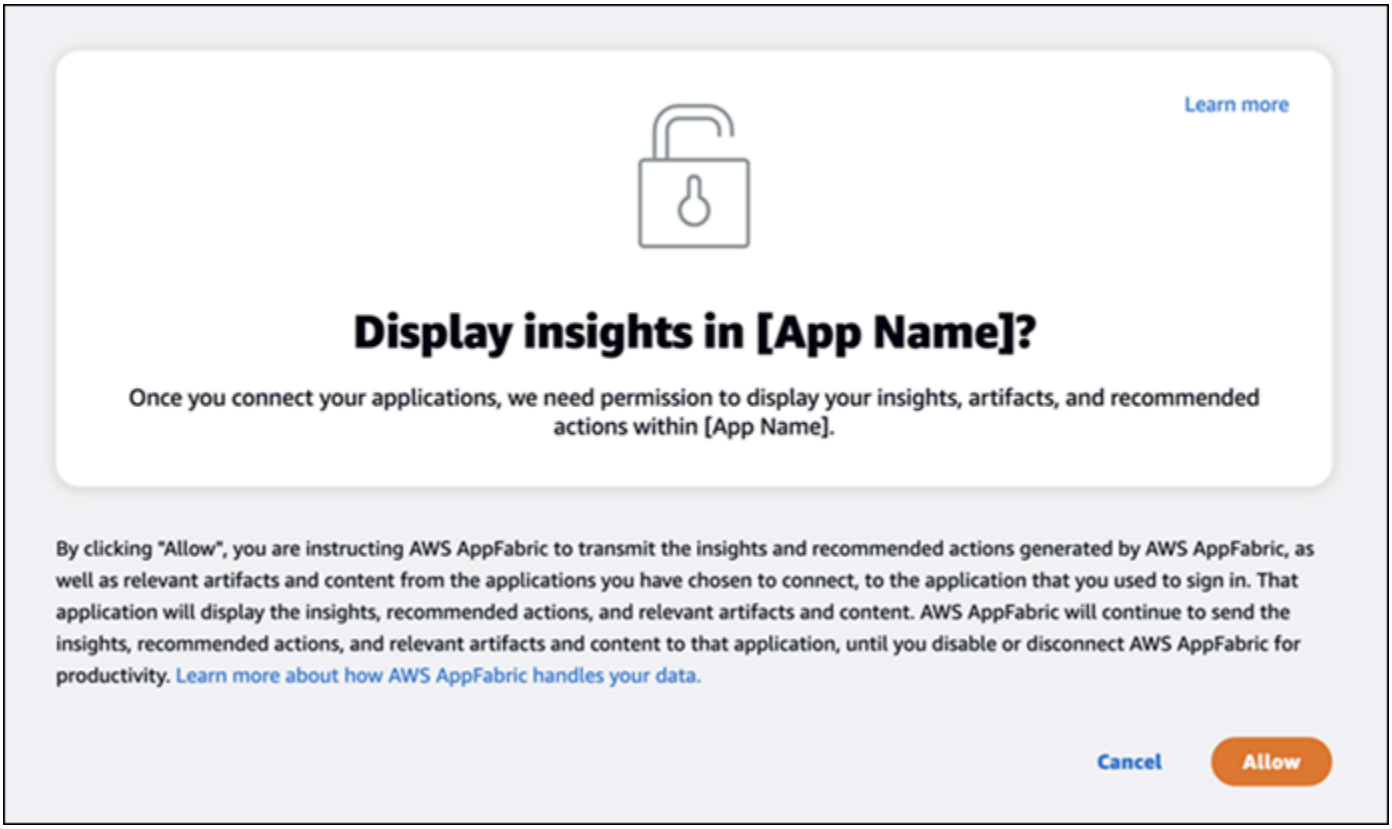




Schritt 2. Erteilen Sie Ihre Zustimmung zur Anzeige von Erkenntnissen durch die App

Nach der Anmeldung AppFabric wird eine Zustimmungsseite angezeigt, auf der Sie gefragt werden, ob Sie AppFabric die Anzeige von anwendungsübergreifenden Erkenntnissen und Aktionen in der Anwendung zulassen, in der Sie die Produktivität erhöhen möchten. AppFabric Erlauben Sie

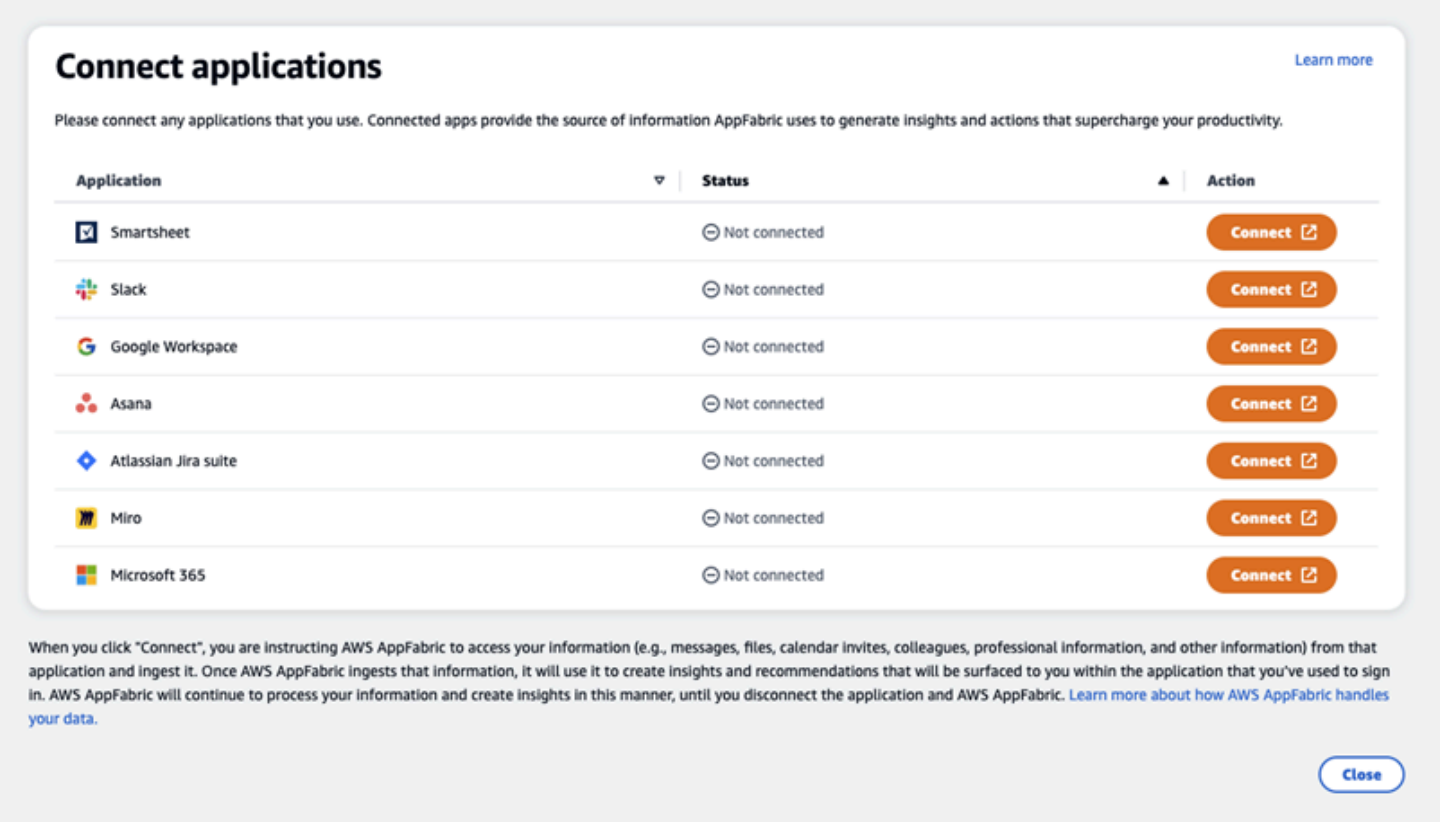
beispielsweise, AppFabric dass Ihre Google Workspace E-Mails und Kalendereereignisse dort angezeigt werden. Asana Sie müssen diesen Zustimmungsschritt pro Anwendung, AppFabric in der Sie ihn aktivieren, nur einmal abschließen.



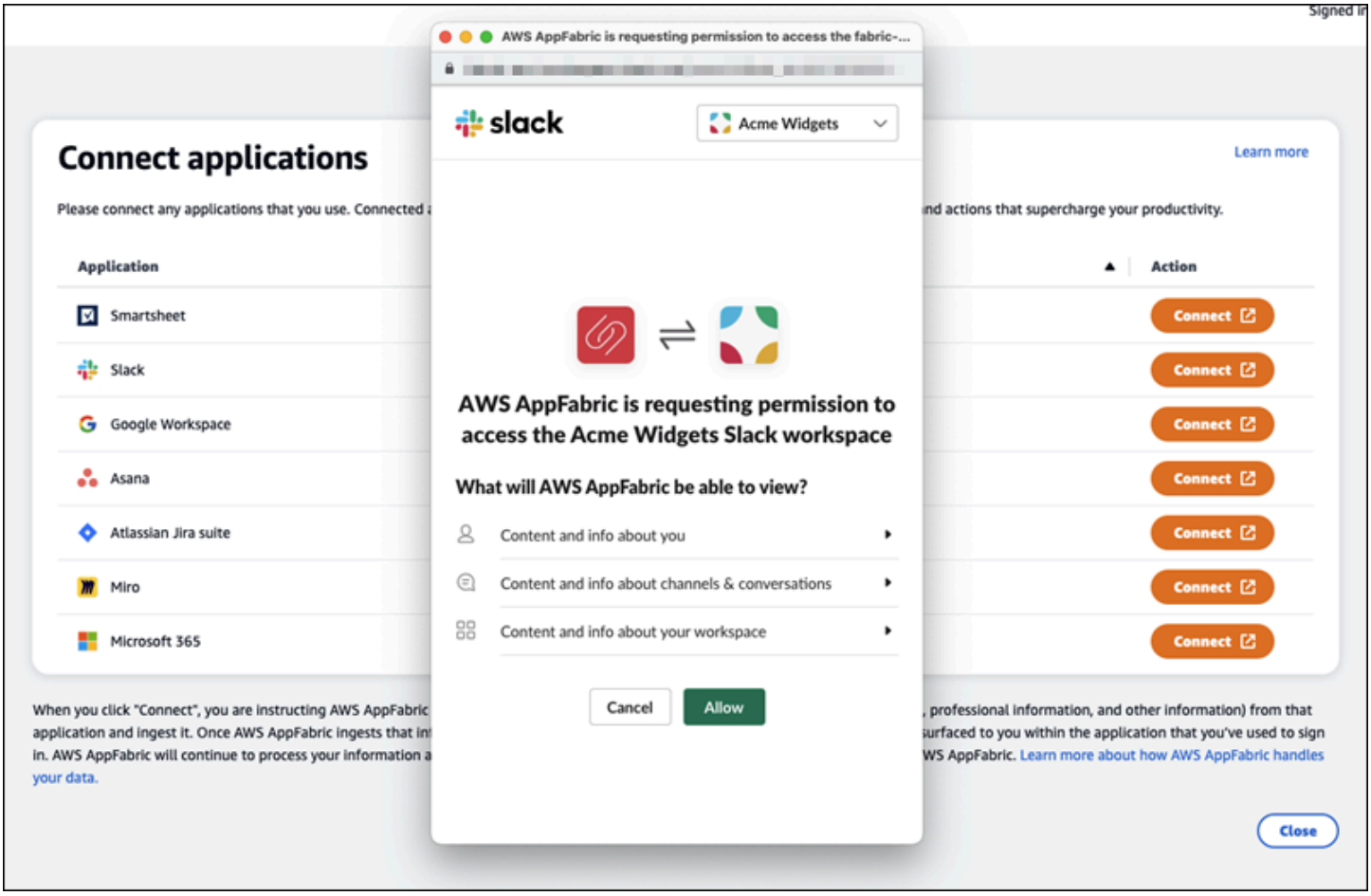
Schritt 3. Connect Sie Ihre Anwendungen, um Erkenntnisse und Maßnahmen zu generieren

Nachdem Sie die Zustimmungsseite ausgefüllt haben, werden Sie zur Seite Connect-Anwendungen weitergeleitet, auf der Sie einzelne Anwendungen verbinden, trennen oder erneut verbinden können, die letztendlich dazu verwendet werden, Ihre anwendungsübergreifenden Erkenntnisse und Aktionen zu generieren. In den meisten Fällen werden Sie diese Seite weiterhin verwenden, um Ihre verbundenen Anwendungen zu verwalten, nachdem Sie sich angemeldet und Ihre Zustimmung erteilt haben.

Um eine Anwendung zu Connect, klicken Sie neben einer beliebigen Anwendung, die Sie verwenden, auf die Schaltfläche Verbinden.



Sie müssen Ihre Anmeldedaten für die Anwendung angeben und den Zugriff auf Ihre Daten AppFabric erlauben, um Erkenntnisse zu gewinnen und Aktionen abzuschließen.



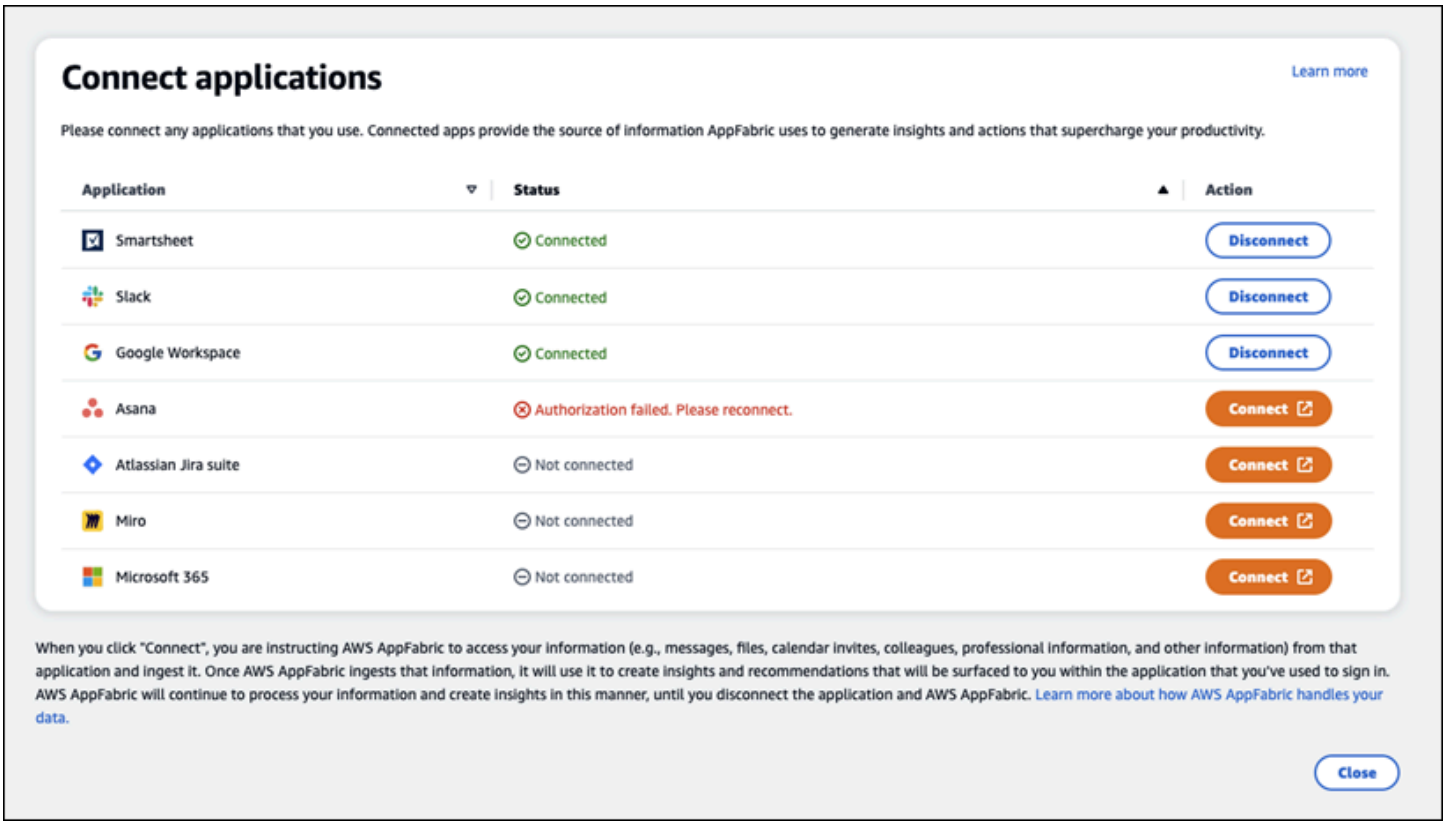
Nachdem Sie eine Anwendung erfolgreich verbunden haben, ändert sich der Status dieser Anwendung von „Nicht verbunden“ zu „Verbunden“. Zur Erinnerung: Sie müssen diesen Autorisierungsschritt für jede Anwendung abschließen, die Sie für die Generierung von Erkenntnissen und Aktionen verwenden möchten.

Nachdem Sie eine Anwendung verbunden haben, ist sie nicht für immer verbunden. Sie müssen die Anwendungen regelmäßig erneut verbinden. Wir tun dies, um sicherzustellen, dass wir weiterhin Ihre Erlaubnis haben, Erkenntnisse zu generieren.

Die möglichen Bewerbungsstatus sind:

- Verbunden — AppFabric ist autorisiert und generiert mithilfe Ihrer Daten aus dieser Anwendung Erkenntnisse.
- Nicht verbunden — generiert AppFabric keine Erkenntnisse mithilfe von Daten aus dieser Anwendung. Sie können eine Verbindung herstellen, um mit der Generierung von Erkenntnissen zu beginnen.

- Die Autorisierung ist fehlgeschlagen. Bitte stellen Sie die Verbindung erneut her. - Bei einer bestimmten Anwendung ist möglicherweise ein Autorisierungsfehler aufgetreten. Wenn Sie diesen Fehler sehen, versuchen Sie, Ihre Anwendung über die Schaltfläche Connect erneut zu verbinden.



Die Einrichtung ist abgeschlossen und Sie können zu Ihrer Anwendung zurückkehren. Es kann mindestens ein paar Stunden dauern, bis Sie Einblicke in Ihre Anwendungen erhalten.

Bei Bedarf können Sie zu dieser Seite zurückkehren, um Ihre verbundenen Anwendungen zu verwalten. Wenn Sie die Verbindung zu einer Anwendung trennen, verwendet AppFabric diese Anwendung keine Daten mehr und sammelt keine neuen Daten mehr, um neue Erkenntnisse zu gewinnen. Daten aus getrennten Anwendungen werden innerhalb von 7 Tagen automatisch gelöscht, wenn Sie sich dafür entscheiden, die Verbindung zur Anwendung innerhalb dieser Zeit nicht erneut herzustellen.

Schritt 4. Verschaffen Sie sich Einblicke und führen Sie anwendungsübergreifende Aktionen in Ihrer Anwendung aus

Nachdem Sie Ihre Anwendungen mit verbunden haben AppFabric, haben Sie Zugriff auf wertvolle Erkenntnisse und können anwendungsübergreifende Aktionen direkt von Ihrer bevorzugten

Anwendung aus ausführen. Hinweis: Diese Funktionalität ist nicht in jeder App garantiert und hängt ausschließlich davon ab, welche AppFabric Produktivitätsfunktionen der Anwendungsentwickler aktiviert hat.

Anwendungsübergreifende Einblicke

AppFabric for Productivity bietet zwei Arten von Erkenntnissen:

- Umsetzbare Erkenntnisse: AppFabric Analysiert Informationen aus Ihren E-Mails, Kalenderereignissen, Aufgaben und Nachrichten in Ihren verbundenen Apps und generiert wichtige Erkenntnisse, deren Priorisierung für Sie wichtig sein kann. Darüber hinaus AppFabric können empfohlene Aktionen generiert werden (z. B. E-Mail senden, Besprechung planen und Aufgabe erstellen), die Sie bearbeiten und ausführen können, während Sie in Ihrer bevorzugten Anwendung bleiben. Möglicherweise erhalten Sie beispielsweise Informationen darüber, dass eine Kundeneskalation zu bewältigen ist, und einen Vorschlag für die nächste Aktion, um ein Treffen mit Ihrem Kunden zu vereinbaren.
- Einblicke in die Vorbereitung von Besprechungen: Mit dieser Funktion können Sie sich optimal auf bevorstehende Besprechungen vorbereiten. AppFabric analysiert Ihre bevorstehenden Besprechungen und erstellt eine kurze Zusammenfassung des Besprechungszwecks. Darüber hinaus werden relevante Artefakte (wie E-Mails, Nachrichten und Aufgaben) aus Ihren verbundenen Anwendungen angezeigt, sodass Sie sich effizient auf das Meeting vorbereiten können, ohne zwischen Apps wechseln zu müssen, um nach Inhalten zu suchen.

App-übergreifende Aktionen

Für bestimmte Erkenntnisse AppFabric können auch Handlungsempfehlungen generiert werden, z. B. das Senden einer E-Mail, das Planen eines Meetings oder das Erstellen einer Aufgabe. Bei der Generierung von Aktionen AppFabric kann es sein, dass bestimmte Felder je nach Inhalt und Kontext Ihrer verbundenen Anwendungen vorab ausgefüllt werden. AppFabric Kann beispielsweise basierend auf den Erkenntnissen eine vorgeschlagene E-Mail-Antwort oder einen Aufgabennamen generieren. Wenn Sie auf eine vorgeschlagene Aktion klicken, werden Sie zu einer AppFabric eigenen Benutzeroberfläche weitergeleitet, auf der Sie den bereits ausgefüllten Inhalt bearbeiten können, bevor Sie die Aktion ausführen. AppFabric führt keine Aktionen ohne vorherige Überprüfung und Eingabe durch den Benutzer aus, da generative KI und die zugrunde liegenden großen Sprachmodelle (LLM) von Zeit zu Zeit halluzinieren können.

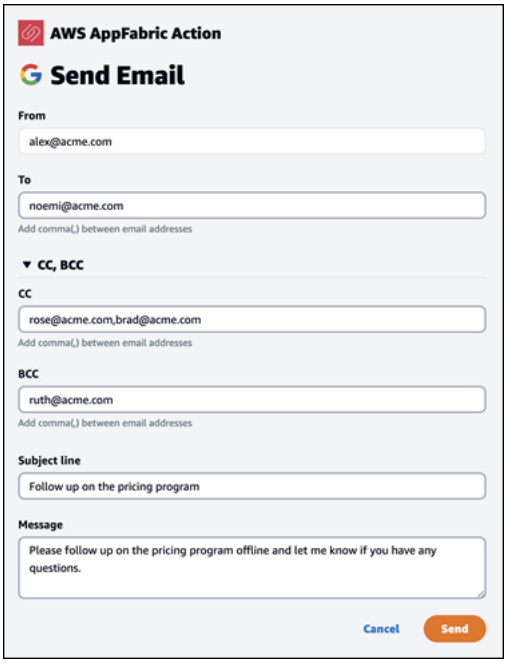
> **Note**
>
> Sie sind dafür verantwortlich, die Ergebnisse zu validieren und zu bestätigen. AppFabric LLM AppFabric garantiert nicht die Richtigkeit oder Qualität seiner LLM Ergebnisse. Weitere Informationen finden Sie unter Richtlinie AWS für verantwortungsvolle KI.

E-Mails erstellen (Google Workspace,Microsoft 365)

AppFabric ermöglicht es Ihnen, eine E-Mail von Ihrer bevorzugten Anwendung aus zu bearbeiten und zu versenden. Wir unterstützen grundlegende E-Mail-Felder wie „Von“, „An“, „Cc/Bcc“, „E-Mail-Betreffzeile“ und „E-Mail-Hauptnachricht“. AppFabric kann Inhalte in diesen Feldern generieren, um Ihnen zu helfen, die Zeit bis zur Erledigung der Aufgabe zu verkürzen. Wenn Sie mit der Bearbeitung der E-Mail fertig sind, wählen Sie Senden, um die E-Mail zu senden.

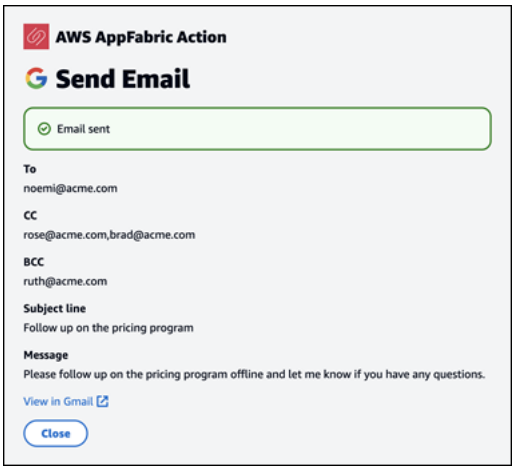
Die folgenden Felder sind erforderlich, um eine E-Mail zu senden:

- Mindestens eine der Empfänger-E-Mails (An, CC undBCC) ist erforderlich und es muss sich um gültige E-Mail-Adressen handeln.
- Felder für Betreffzeile und Nachricht.



Nachdem die E-Mail gesendet wurde, wird eine Bestätigung angezeigt, dass die E-Mail gesendet wurde. Darüber hinaus wird in der entsprechenden Anwendung ein Link zum Anzeigen der E-Mail

angezeigt. Sie können diesen Link verwenden, um schnell zur Anwendung zu navigieren und zu überprüfen, ob die E-Mail gesendet wurde.

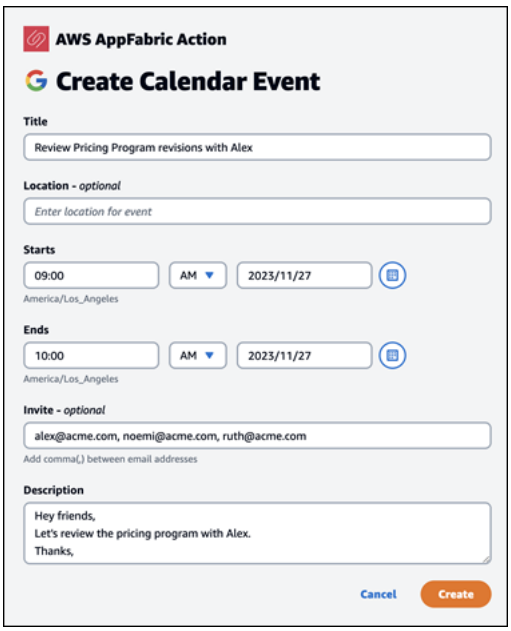


Kalenderereignisse erstellen (Google Workspace,Microsoft 365)

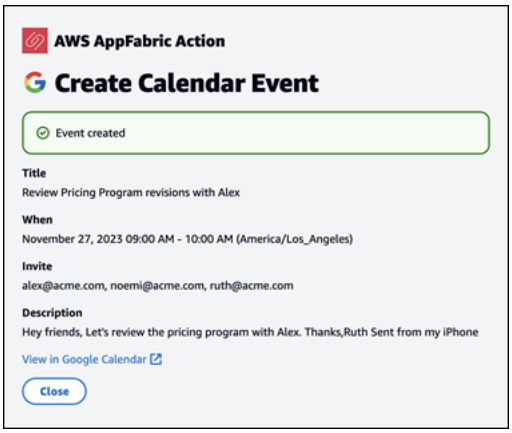
AppFabric ermöglicht es Ihnen, ein Kalenderereignis in Ihrer bevorzugten Anwendung zu bearbeiten und zu erstellen. Wir unterstützen grundlegende Kalenderereignisfelder wie den Titel der Veranstaltung, den Ort, die Start-/Endzeit und das Datum, die Liste der eingeladenen Personen und die Veranstaltungsdetails. AppFabric kann Inhalte in diesen Feldern generieren, um Ihnen zu helfen, die Zeit bis zur Erledigung der Aufgabe zu verkürzen. Wenn Sie mit der Bearbeitung des Kalenderereignisses fertig sind, wählen Sie Erstellen aus, um das Ereignis zu erstellen.

Die folgenden Felder sind erforderlich, um ein Kalenderereignis zu erstellen:

- Felder für Titel, Beginn, Ende und Beschreibung.
- Startzeit und -datum dürfen nicht vor Uhrzeit und Datum des Endes liegen.
- Das Einladungsfeld ist optional, erfordert jedoch gültige E-Mail-Adressen, sofern angegeben.



Nach dem Senden des Kalenderereignisses erhalten Sie eine Bestätigung, dass das Ereignis erstellt wurde. Darüber hinaus sehen Sie in der dafür vorgesehenen Anwendung einen Link, über den Sie sich das Ereignis ansehen können. Sie können diesen Link verwenden, um schnell zur Anwendung zu navigieren und zu überprüfen, ob das Ereignis erstellt wurde.

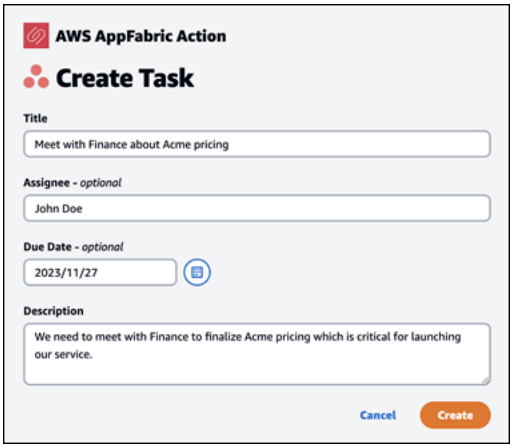


Aufgaben erstellen (Asana)

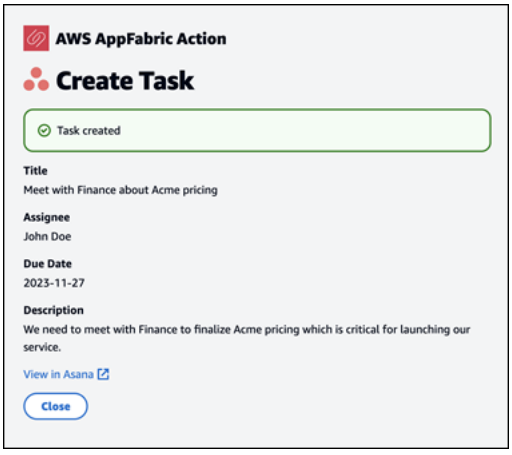
AppFabric ermöglicht es Ihnen, eine Aufgabe in Ihrer bevorzugten Anwendung Asana zu bearbeiten und zu erstellen. Wir unterstützen grundlegende Aufgabenfelder wie Aufgabenname, Aufgabenbesitzer, Fälligkeitsdatum und Aufgabenbeschreibung. AppFabric kann Inhalte in diesen Feldern generieren, um Ihnen zu helfen, die Zeit für die Erstellung der Aufgabe zu verkürzen. Wenn Sie mit der Bearbeitung der Aufgabe fertig sind, wählen Sie Erstellen aus, um die Aufgabe zu erstellen. Aufgaben werden im entsprechenden Asana Arbeitsbereich, Projekt oder Aufgabe erstellt, wie von der vorgeschlagenLLM.

Die folgenden Felder sind erforderlich, um eine Asana Aufgabe zu erstellen:

- Felder für Titel und Beschreibung.
- Der Bevollmächtigte muss eine gültige E-Mail-Adresse haben, falls sie geändert wurde.



Nachdem die Aufgabe erstellt wurde, wird eine Bestätigung angezeigt, dass die Aufgabe in erstellt wurde. Asana Darüber hinaus sehen Sie einen Link, über den Sie sich die Aufgabe ansehen könnenAsana. Mithilfe dieses Links können Sie schnell zur Anwendung navigieren, um zu überprüfen, ob die Aufgabe erstellt wurde, oder sie in den entsprechenden Asana Arbeitsbereich, das Projekt oder die Aufgabe verschieben.



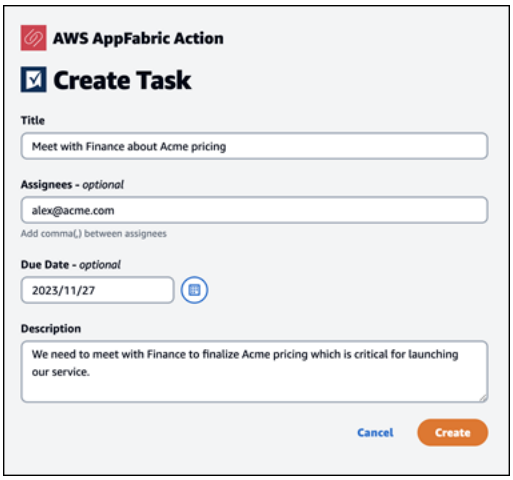
Aufgaben erstellen (Smartsheet)

AppFabric ermöglicht es Ihnen, eine Aufgabe in Ihrer bevorzugten Anwendung Smartsheet zu bearbeiten und zu erstellen. Wir unterstützen grundlegende Aufgabenfelder wie Aufgabenname, Aufgabenbesitzer, Fälligkeitsdatum und Aufgabenbeschreibung. AppFabric kann Inhalte in diesen Feldern generieren, um Ihnen zu helfen, die Zeit für die Erstellung der Aufgabe zu verkürzen. Wenn

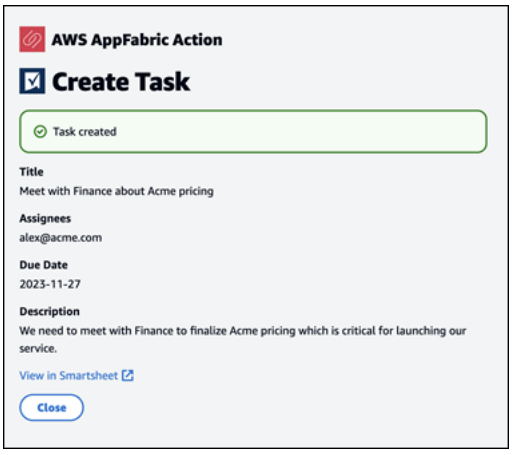
Sie mit der Bearbeitung der Aufgabe fertig sind, wählen Sie Erstellen aus, um die Aufgabe zu erstellen. Erstellt für Smartsheet Aufgaben ein neues privates Smartsheet Blatt und füllt alle erstellten Aufgaben aus. AppFabric Dies dient dazu, AppFabric generierte Aktionen strukturiert an einem einzigen Ort zu zentralisieren.

Die folgenden Felder sind erforderlich, um eine Smartsheet Aufgabe zu erstellen:

- Felder für Titel und Beschreibung.
- Der Bevollmächtigte muss eine gültige E-Mail-Adresse haben, falls angegeben.



Nachdem die Aufgabe erstellt wurde, wird eine Bestätigung angezeigt, dass die Aufgabe in erstellt wurde. Smartsheet Darüber hinaus sehen Sie einen Link, über den Sie sich die Aufgabe ansehen könnenSmartsheet. Sie können diesen Link verwenden, um schnell zu der Anwendung zu navigieren und die Aufgabe im erstellten Smartsheet Blatt anzuzeigen. Alle future Smartsheet Aufgaben werden in dieses Blatt eingetragen. Wenn das Blatt gelöscht wird, AppFabric wird ein neues erstellt.



Achtung IT- und Sicherheitsadministratoren: Verwaltung des Zugriffs auf Funktionen AppFabric zur Produktivitätssteigerung (Vorschauversion)

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Das Benutzerportal AppFabric für Produktivität ist für alle Benutzer von SaaS-Anwendungen, die Funktionen AppFabric für Produktivität (Vorschauversion) integriert haben, öffentlich zugänglich. Wenn Sie ein IT-Administrator sind, der den Zugriff auf diese generativen KI-Funktionen in Ihrem Unternehmen verwalten möchte, sollten Sie die folgenden Optionen in Betracht ziehen:

- Einschränken der Anmeldung durch den Identitätsanbieter (IdP): Sie können den Anmeldezugriff über Ihren Identity Provider blockieren, um den Benutzerzugriff auf generative KI-Funktionen zu kontrollieren.
- OAuth für bestimmte Anwendungen deaktivieren: Implementieren Sie nachgelagerte Einschränkungen, indem Sie OAuth deaktivieren. Diese Aktion verhindert, dass Benutzer Anwendungen, für die eine OAuth-Authentifizierung erforderlich ist, mit dem Workspace des Unternehmens verbinden.

Fehlerbehebung

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

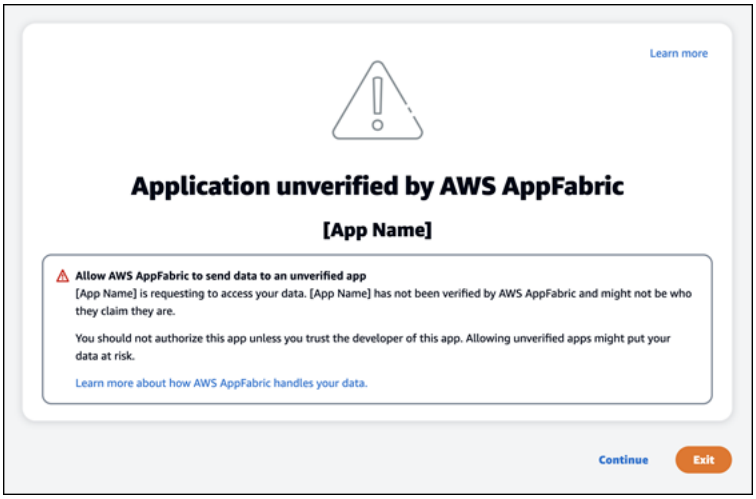
In diesem Abschnitt werden häufig auftretende Fehler und Problembehebungen aus AppFabric Produktivitätsgründen beschrieben.

Unbestätigter Antrag

Anwendungen, die aus AppFabric Produktivitätsgründen ihr App-Erlebnis verbessern, werden vor der Einführung ihrer Funktionen für Endbenutzer einem Verifizierungsprozess unterzogen. Wenn Sie bei dem Versuch, sich anzumelden, auf ein Banner mit der Aufschrift „Nicht verifiziert“ stoßen AppFabric, bedeutet dies, dass die Anwendung noch keinen Verifizierungsprozess durchlaufen AppFabric hat, der die Identität des App-Entwicklers und die Richtigkeit der Registrierungsinformationen

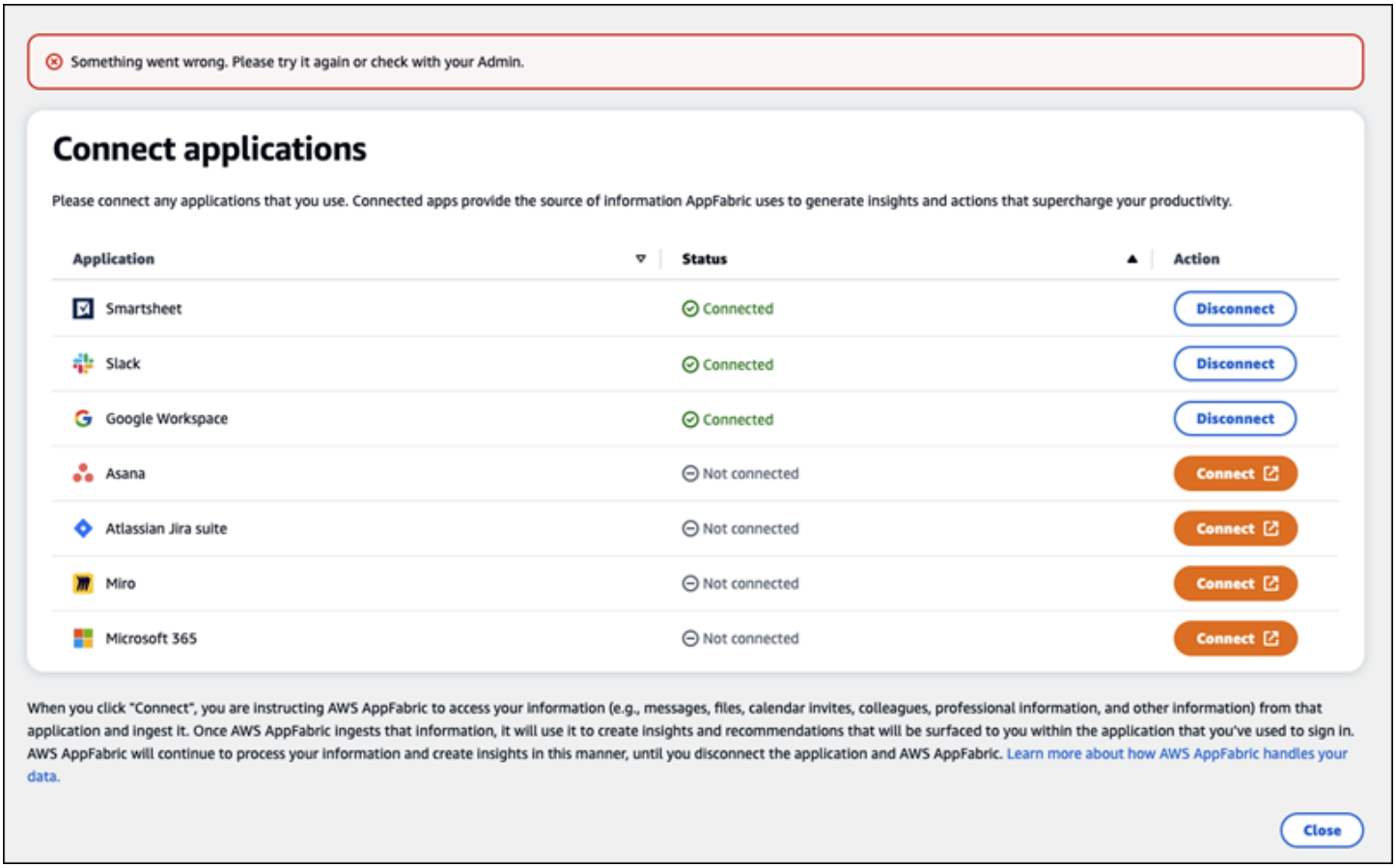
der Anwendung bestätigt. Alle Anwendungen beginnen als nicht verifiziert und werden erst dann bestätigt, wenn der Überprüfungsprozess abgeschlossen ist.

Seien Sie vorsichtig, wenn Sie eine nicht verifizierte Anwendung verwenden. Wenn Sie sich bezüglich der App-Entwickler nicht sicher sind, können Sie warten, bis die Anwendung den Status „Verifiziert“ erreicht hat, bevor Sie fortfahren.



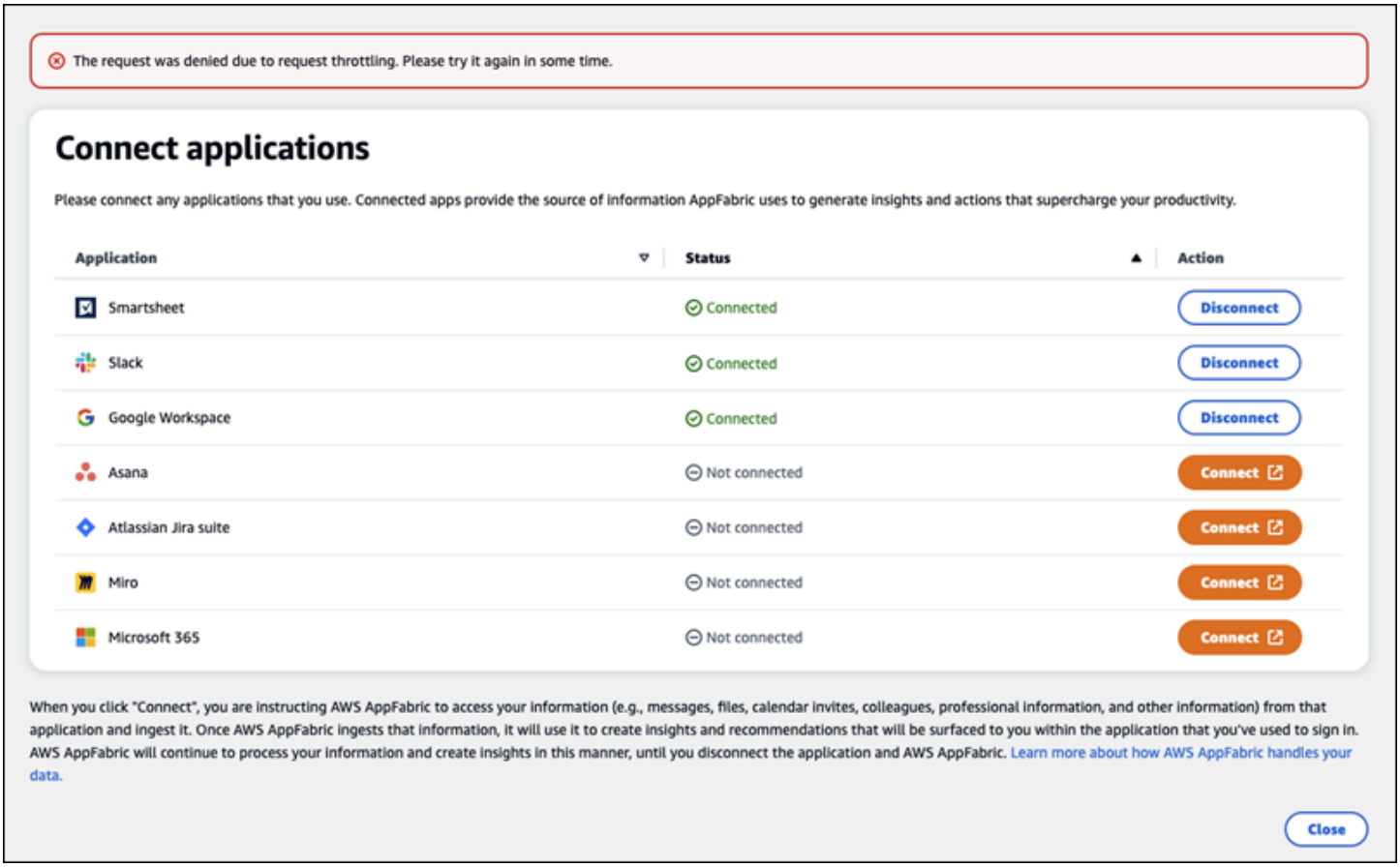
Etwas ist schief gelaufen. Bitte versuchen Sie es erneut oder erkundigen Sie sich bei Ihrem Admin (**`InternalServerException`**)

Möglicherweise erhalten Sie diese Meldung, wenn das AppFabric Benutzerportal die Anwendungen nicht auflistet oder eine Anwendung aufgrund eines unbekannten Fehlers, einer Ausnahme oder eines Fehlers abbricht. Bitte versuchen Sie es später erneut.



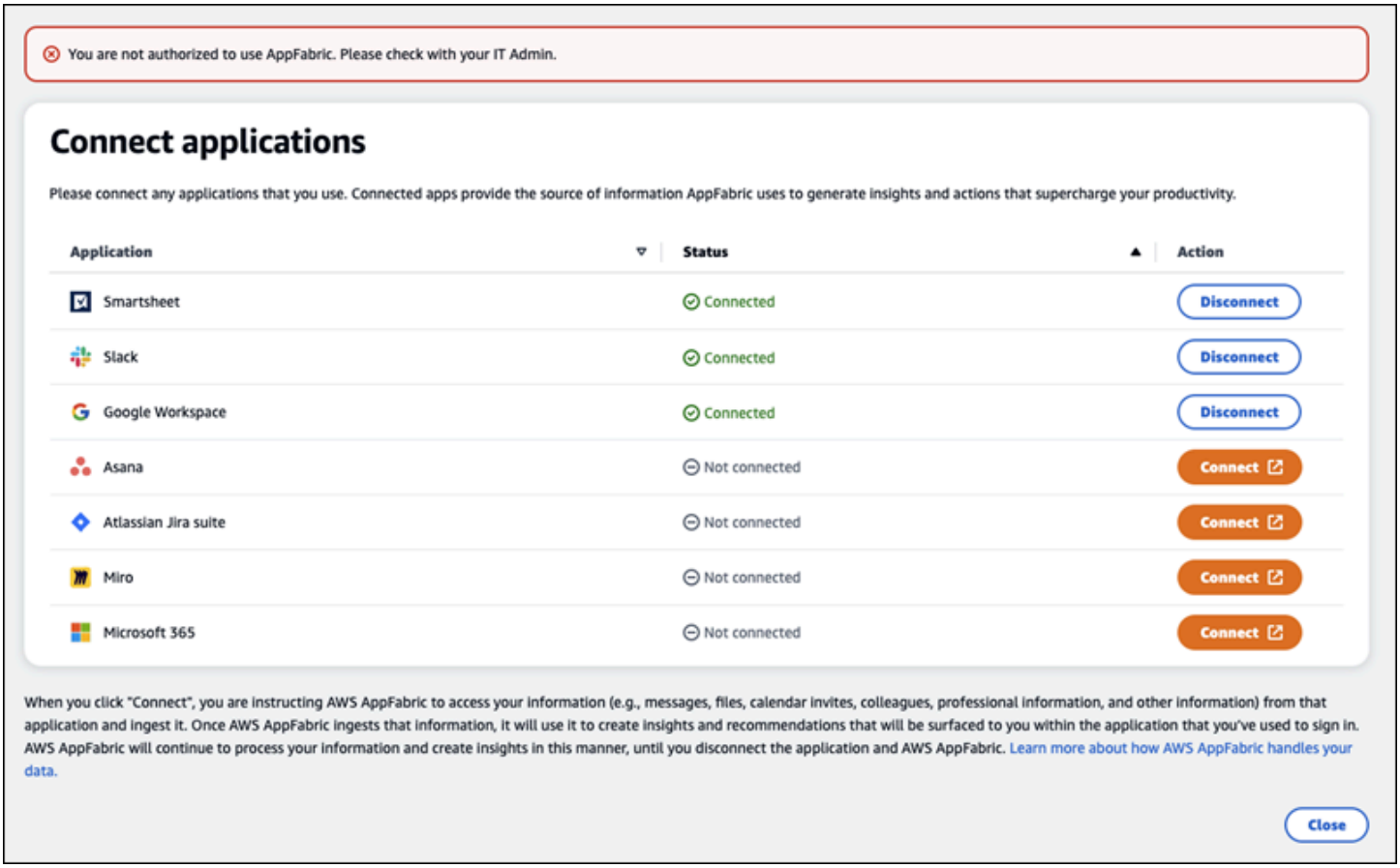
Die Anforderung wurde aufgrund der Drosselung von Anforderungen abgelehnt. Bitte versuchen Sie es in einiger Zeit erneut () **`ThrottlingException`**

Möglicherweise erhalten Sie diese Meldung, wenn das AppFabric Benutzerportal die Anwendungen nicht auflistet oder wenn eine Anwendung aufgrund eines Drosselungsproblems getrennt wird. Bitte versuchen Sie es später erneut.



Sie sind nicht zur Nutzung berechtigt. AppFabric Bitte melden Sie sich AppFabric erneut an (**`AccessDeniedException`**)

Möglicherweise erhalten Sie diese Meldung, wenn das AppFabric Benutzerportal die Anwendungen nicht auflistet oder eine Anwendung aufgrund einer Ausnahme vom Typ „Zugriff verweigert“ abbricht. Melden Sie sich AppFabric erneut an.



AppFabric Produktivitäts-APIs

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

In diesem Abschnitt werden die API-Operationen, Datentypen und häufig auftretende Fehler für die AWS AppFabric Produktivitätsfunktionen beschrieben.

> **Note**
>
> Alle anderen AppFabric APIs finden Sie in der AWS AppFabric API-Referenz.

Themen

- Aktionen
- Datentypen

- Häufige Fehler

Aktionen

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Die folgenden Aktionen werden für die AppFabric Produktivitätsfunktionen unterstützt.

Alle anderen AppFabric API-Aktionen finden Sie unter AWS AppFabric API-Aktionen.

Themen

- Autorisieren
- CreateAppClient
- DeleteAppClient
- GetAppClient
- ListActionableInsights
- ListAppClients
- ListMeetingInsights
- PutFeedback
- Token
- UpdateAppClient

Autorisieren

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Autorisiert eine AppClient.

Themen

- Anforderungstext

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Parameter	Beschreibung
app_client_id	Die ID des zu autorisierenden. AppClient
redirect_uri	Der URI, zu dem Endbenutzer nach der Autorisierung weitergel eitet werden sollen.
state	Ein eindeutiger Wert, um den Status zwischen der Anfrage und dem Rückruf beizubehalten.

CreateAppClient

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Erzeugt eine AppClient.

Themen

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Parameter	Beschreibung
Anwendungsname	Gibt den Namen der App an. Typ: Zeichenfolge Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 255 Zeichen.

Parameter	Beschreibung
	Erforderlich: Ja
clientToken	Gibt einen eindeutigen Bezeichner an, bei dem die Groß- und Kleinschreibung berücksichtigt wird, den Sie angeben, um die Idempotenz der Anfrage sicherzustellen. Auf diese Weise können Sie die Anfrage sicher wiederholen, ohne versehentlich denselben Vorgang ein zweites Mal auszuführen. Wenn Sie denselben Wert an einen späteren Aufruf einer Operation übergeben, müssen Sie denselben Wert auch für alle anderen Parameter übergeben. Es wird empfohlen, einen Wert vom Typ UUID zu verwenden. Wenn Sie diesen Wert nicht angeben, wird ein zufälliger Wert für Sie AWS generiert. Wenn Sie den Vorgang mit denselben `ClientToken` , aber mit anderen Parametern wiederholen, schlägt der Vorgang mit einem `IdempotentParameterMismatch` Fehler fehl. Typ: Zeichenfolge Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Erforderlich: Nein

Parameter	Beschreibung
customerManagedKey Bezeichner	Der ARN des Kundenverwalteter Schlüssel generierten von AWS Key Management Service. Der Schlüssel wird verwendet, um die Daten zu verschlüsseln. Wenn kein Schlüssel angegeben ist, Von AWS verwalteter Schlüssel wird ein verwendet. Eine Zuordnung der Schlüssel -Wert-Paare des Tags oder der Tags, die der Ressource zugewiesen werden sollen. Weitere Informationen zu AWS-eigene Schlüssel und vom Kunden verwalteten Schlüsseln finden Sie unter Kundensch lüssel und AWS Schlüssel im AWS Key Management Service Entwicklerhandbuch. Typ: Zeichenfolge Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Die maximale Länge beträgt 1011. Pattern: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Erforderlich: Nein
description	Eine Beschreibung für die App. Typ: Zeichenfolge Erforderlich: Ja
URL des Symbols	Die URL zum Symbol oder Logo für. AppClient Typ: Zeichenfolge Erforderlich: Nein

Parameter	Beschreibung
URLs umleiten	Der URI, zu dem Endbenutzer nach der Autorisierung weitergel eitet werden sollen. Sie können bis zu 5 Weiterleitungs-URLs hinzufügen. z. B. `https://localhost:8080` . Typ: Zeichenfolgen-Array Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente. Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 2048 Zeichen. Pattern: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` Erforderlich: Ja
starterUserEmails	Einstiegs-E-Mail-Adressen für Benutzer, denen Zugriff gewährt wird, um Einblicke zu erhalten, bis diese verifiziert sind. AppClient Typ: Zeichenfolgen-Array Array-Mitglieder: Feste Anzahl von 1 Element. Längenbeschränkungen: Minimale Länge von 0. Maximale Länge von 320. Pattern: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Erforderlich: Ja

Parameter	Beschreibung
Tags	Eine Zuordnung der Schlüssel-Wert-Paare des Tags oder der Tags, die der Ressource zugewiesen werden sollen. Typ: Array von Tag-Objekten Array-Mitglieder: Die Mindestanzahl beträgt 0 Elemente. Die maximale Anzahl beträgt 50 Elemente. Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP-201-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Parameter	Beschreibung
appClientSummary	Enthält eine Zusammenfassung der AppClient. Typ: AppClientSummary Objekt

DeleteAppClient

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Löscht einen Anwendungsclient.

Themen

- Anforderungstext
- Antwortelemente

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Parameter	Beschreibung
appClientIdentifier	Der Amazon-Ressourcenname (ARN) oder der Universal Unique Identifier (UUID) der Person, die für die AppClient Anfrage verwendet werden soll. Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Die maximale Länge beträgt 1011. Pattern: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Erforderlich: Ja

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP-204-Antwort mit leerem HTTP-Textinhalt zurück.

GetAppClient

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Gibt Informationen über eine zurück AppClient.

Themen

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Parameter	Beschreibung
appClientIdentifier	Der Amazon-Ressourcenname (ARN) oder der Universal Unique Identifier (UUID) der Person, die für die AppClient Anfrage verwendet werden soll. Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Die maximale Länge beträgt 1011. Pattern: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Erforderlich: Ja

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Parameter	Beschreibung
App-Client	Enthält Informationen über einen AppClient. Typ: AppClient Objekt

ListActionableInsights

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Listet die wichtigsten umsetzbaren E-Mail-Nachrichten, Aufgaben und andere Updates auf.

Themen

- Anforderungstext
- Antwortelemente

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Parameter	Beschreibung
nextToken	Wenn zurückgegeben `nextToken` wird, sind mehr Ergebnisse verfügbar. Der Wert von `nextToken` ist ein eindeutiges Paginierungstoken für jede Seite. Rufen Sie erneut mit dem zurückgegebenen Token auf, um die nächste Seite abzurufen. Behalten Sie alle anderen Argumente unverändert bei. Jedes Paginierungstoken läuft nach 24 Stunden ab. Die Verwendung eines abgelaufenen Paginierungstokens führt zu einem HTTP InvalidToken 400-Fehler.

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP-201-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Parameter	Beschreibung
ActionableInsightsList	Führt die umsetzbaren Erkenntnisse auf, einschließlich eines Titels, einer Beschreibung, der Aktionen und des erstellten Zeitstempels. Weitere Informationen finden Sie unter ActionableInsights.
nextToken	Wenn zurückgegeben `nextToken` wird, sind mehr Ergebnisse verfügbar. Der Wert von `nextToken` ist ein eindeutiges Paginierungstoken für jede Seite. Rufen Sie erneut mit dem zurückgegebenen Token auf, um die nächste Seite abzurufen. Behalten Sie alle anderen Argumente unverändert bei. Jedes Paginierungstoken läuft nach 24 Stunden ab. Die Verwendung eines abgelaufenen Paginierungstokens führt zu einem HTTP InvalidToken 400-Fehler. Typ: Zeichenfolge

ListAppClients

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Gibt eine Liste aller zurück AppClients.

Themen

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Parameter	Beschreibung
maxResults	Die maximale Anzahl von Ergebnissen, die pro Anruf zurückgegeben werden. Sie können `nextToken` sie verwenden, um weitere Ergebnisseiten zu erhalten. Dies ist nur eine Obergrenze. Die tatsächliche Anzahl der pro Anruf zurückgegebenen Ergebnisse liegt möglicherweise unter dem angegebenen Höchstwert. Gültiger Bereich: Mindestwert 1. Maximalwert 100.
nextToken	Wenn zurückgegeben `nextToken` wird, sind mehr Ergebnisse verfügbar. Der Wert von `nextToken` ist ein eindeutiges Paginierungstoken für jede Seite. Rufen Sie erneut mit dem zurückgegebenen Token auf, um die nächste Seite abzurufen. Behalten Sie alle anderen Argumente unverändert bei. Jedes Paginierungstoken läuft nach 24 Stunden ab. Die Verwendung eines abgelaufenen Paginierungstokens führt zu einem HTTP InvalidToken 400-Fehler.

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Parameter	Beschreibung
appClientList	Enthält eine Liste von AppClient Ergebnissen. Typ: Array von AppClientSummary-Objekten
nextToken	Wenn zurückgegeben `nextToken` wird, sind mehr Ergebnisse verfügbar. Der Wert von `nextToken` ist ein eindeutiges Paginierungstoken für jede Seite. Rufen Sie erneut mit dem zurückgegebenen Token auf, um die nächste Seite abzurufen. Behalten Sie alle anderen Argumente unverändert bei. Jedes Paginierungstoken läuft nach 24 Stunden ab. Die Verwendung eines abgelaufenen Paginierungstokens führt zu einem HTTP InvalidToken 400-Fehler. Typ: Zeichenfolge

ListMeetingInsights

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Listet die wichtigsten umsetzbaren Kalenderereignisse auf.

Themen

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Parameter	Beschreibung
nextToken	Wenn zurückgegeben `nextToken` wird, sind mehr Ergebnisse verfügbar. Der Wert von `nextToken` ist ein eindeutiges Paginierungstoken für jede Seite. Rufen Sie erneut mit dem zurückgegebenen Token auf, um die nächste Seite abzurufen. Behalten Sie alle anderen Argumente unverändert bei. Jedes Paginierungstoken läuft nach 24 Stunden ab. Die Verwendung eines abgelaufenen Paginierungstokens führt zu einem HTTP InvalidToken 400-Fehler.

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP-201-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Parameter	Beschreibung
MeetingInsightList	Listet die umsetzbaren Erkenntnisse aus dem Meeting auf. Weitere Informationen finden Sie unter MeetingInsights.
nextToken	Wenn zurückgegeben `nextToken` wird, sind mehr Ergebnisse verfügbar. Der Wert von `nextToken` ist ein eindeutiges Paginierungstoken für jede Seite. Rufen Sie erneut mit dem zurückgegebenen Token auf, um die nächste Seite abzurufen. Behalten Sie alle anderen Argumente unverändert bei. Jedes Paginierungstoken läuft nach 24 Stunden ab. Die Verwendung eines abgelaufenen Paginierungstokens führt zu einem HTTP InvalidToken 400-Fehler. Typ: Zeichenfolge

PutFeedback

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Ermöglicht Benutzern, Feedback zu einem bestimmten Einblick oder einer bestimmten Aktion einzureichen.

Themen

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Parameter	Beschreibung
id	Die ID des Objekts, für das Feedback eingereicht wird. Dies kann entweder der InsightId oder der sein ActionId.
Feedback für	Der Insight-Typ, für den das Feedback eingereicht wird. Mögliche Werte: `ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION`
FeedbackBewertung	Feedback Bewertung von bis1. 5 Je höher die Bewertung, desto besser.

Antwortelemente

Wenn die Aktion erfolgreich ist, gibt der Dienst eine HTTP-201-Antwort mit leerem HTTP-Textinhalt zurück.

Token

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Enthält Informationen, die AppClients den Austausch eines Autorisierungscodes gegen ein Zugriffstoken ermöglichen.

Themen

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Parameter	Beschreibung
Code	Der vom Autorisierungsendpunkt empfangene Autorisierungscode. Typ: Zeichenfolge Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 2048 Zeichen. Erforderlich: Nein
grant_type	Der Grant-Typ für das Token. Es muss entweder `authorization_code` oder `refresh_token` sein. Typ: Zeichenfolge Erforderlich: Ja
app_client_id	Die ID der AppClient. Typ: Zeichenfolge

Parameter	Beschreibung
	Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Erforderlich: Ja
redirect_uri	Die Umleitungs-URI, die an den Autorisierungsendpunkt übergeben wurde. Typ: Zeichenfolge Erforderlich: Nein
refresh_token	Das Aktualisierungstoken, das von der ersten Token-Anfrage empfangen wurde. Typ: Zeichenfolge Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 4096 Zeichen. Erforderlich: Nein

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Parameter	Beschreibung
appfabric_user_id	Die ID des Benutzers für das Token. Dies wird nur für Anfragen zurückgegeben, die den `authorization_code` Grant-Typ verwenden. Typ: Zeichenfolge
expires_in	Die Anzahl der Sekunden, bis das Token abläuft.

Parameter	Beschreibung
	Type: Long
refresh_token	Das Aktualisierungstoken, das für eine nachfolgende Anfrage verwendet werden soll. Typ: Zeichenfolge Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 2048 Zeichen.
Token	Das Zugriffstoken. Typ: Zeichenfolge Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 2048 Zeichen.
token_type	Der Token-Typ. Typ: Zeichenfolge

UpdateAppClient

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Aktualisiert und AppClient.

Themen

- Anforderungstext
- Antwortelemente

Anforderungstext

Die Anforderung akzeptiert die folgenden Daten im JSON-Format.

Parameter	Beschreibung
appClientIdentifier	Der Amazon-Ressourcenname (ARN) oder der Universal Unique Identifier (UUID) der Person, die für die AppClient Anfrage verwendet werden soll. Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Die maximale Länge beträgt 1011. Pattern: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Erforderlich: Ja
URLs umleiten	Der URI, zu dem Endbenutzer nach der Autorisierung weitergeleitet werden sollen. Sie können bis zu 5 Weiterleitungs-URLs hinzufügen. z. B. `https://localhost:8080` . Typ: Zeichenfolgen-Array Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente. Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 2048 Zeichen. Pattern: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

Antwortelemente

Wenn die Aktion erfolgreich ist, sendet der Service eine HTTP 200-Antwort zurück.

Die folgenden Daten werden vom Service im JSON-Format zurückgegeben.

Parameter	Beschreibung
AppClient	Enthält Informationen über einen AppClient.

Parameter	Beschreibung
	Typ: AppClient Objekt

Datentypen

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Die AppFabric API enthält mehrere Datentypen, die von verschiedenen Aktionen verwendet werden. In diesem Abschnitt werden die Datentypen für die AppFabric Produktivitätsfunktionen ausführlich beschrieben.

Alle anderen AppFabric API-Datentypen finden Sie unter AWS AppFabric API-Datentypen.

> **Important**
>
> Die Reihenfolge der einzelnen Elemente in einer Datentypstruktur ist nicht garantiert. Anwendungen sollten keine bestimmte Reihenfolge annehmen.

Themen

- ActionableInsights
- AppClient
- AppClientSummary
- MeetingInsights
- VerificationDetails

ActionableInsights

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Enthält eine Zusammenfassung wichtiger und geeigneter Aktionen für einen Benutzer auf der Grundlage von E-Mails, Kalendereinladungen, Nachrichten und Aufgaben aus seinem App-Portfolio. Benutzer können proaktive Erkenntnisse aus allen ihren Anwendungen abrufen, die ihnen helfen, ihren Tag optimal zu gestalten. Diese Erkenntnisse liefern eine Begründung dafür, warum sich ein Benutzer für die Zusammenfassung der Erkenntnisse interessieren sollte, zusammen mit Verweisen, wie z. B. eingebetteten Links, auf einzelne Apps und Artefakte, die die Erkenntnisse generiert haben.

Parameter	Beschreibung
Insight-ID	Die eindeutige ID für den generierten Einblick.
Insight-Inhalt	Dadurch werden eine Zusammenfassung der Erkenntnisse und eingebettete Links zu Artefakten zurückgegeben, die zur Generierung der Erkenntnisse verwendet wurden. Dies wäre ein HTML-Inhalt, der eingebettete Links (<a>Tags) enthält.
Insight-Titel	Der Titel des generierten Einblicks.
createdAt	Wann der Einblick generiert wurde.
Aktionen	Eine Liste von Aktionen, die für den generierten Einblick empfohlen werden. Das Aktionsobjekt enthält die folgenden Parameter: • `actionId`— Die eindeutige ID für die generierte Aktion. • `actionIconUrl` — Die Icon-URL für die App, in der die Aktion ausgeführt werden soll. • `actionTitle` — Der Titel der generierten Aktion. • `actionUrl` — Die eindeutige URL, über die der Endbenutzer die Aktion im AppFabric Benutzerportal anzeigen und ausführen kann. Für die Ausführung von Aktionen leiten ISV-Apps Benutzer mithilfe dieser URL zum AppFabric Benutzerportal (Popup-Bildschirm) weiter.

Parameter	Beschreibung
	• `actionExecutionStatus` — Eine Aufzählung, die den Status der Aktion angibt. Die möglichen Werte sind: `EXECUTED | NOT_EXECUTED`

AppClient

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Enthält Informationen zu einem AppClient.

Parameter	Beschreibung
Anwendungsname	Der Name der Anwendung. Typ: Zeichenfolge Erforderlich: Ja
arn	Der Amazon-Ressourcenname (ARN) der AppClient. Typ: Zeichenfolge Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Die maximale Länge beträgt 1011. Pattern: `arn:.+` Erforderlich: Ja
description	Eine Beschreibung der Anwendung. Typ: Zeichenfolge Erforderlich: Ja

Parameter	Beschreibung
Icon-URL	Die URL zum Symbol oder Logo für. AppClient Typ: Zeichenfolge Erforderlich: Nein
URLs umleiten	Die zulässigen Umleitungs-URLs für die. AppClient Typ: Zeichenfolgen-Array Array-Mitglieder: Die Mindestanzahl beträgt 1 Element. Die maximale Anzahl beträgt 5 Elemente. Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Maximale Länge beträgt 2048 Zeichen. Pattern: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` Erforderlich: Ja
starterUserEmails	Starter-E-Mail-Adressen für Benutzer, denen Zugriff gewährt wird, um Einblicke zu erhalten, bis AppClient dies bestätigt ist. Typ: Zeichenfolgen-Array Array-Mitglieder: Feste Anzahl von 1 Element. Längenbeschränkungen: Minimale Länge von 0. Maximale Länge von 320. Pattern: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Erforderlich: Ja

Parameter	Beschreibung
Einzelheiten zur Überprüfung	Enthält den Status und den Grund für die AppClient Überprüfung. Typ: VerificationDetails Objekt Erforderlich: Ja
customerManagedKeyArn	Der Amazon-Ressourcenname (ARN) des Kundenverwalteter Schlüssel generierten AWS Key Management Service für AppClient. Typ: Zeichenfolge Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Die maximale Länge beträgt 1011. Pattern: `arn:.+` Erforderlich: Nein
appClientId	Die ID der AppClient. Soll in O-Auth-Flows für den App-Client verwendet werden. Typ: Zeichenfolge Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Erforderlich: Nein

AppClientSummary

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Enthält Informationen zu einem AppClient.

Parameter	Beschreibung
Arn	Der Amazon-Ressourcenname (ARN) der AppClient. Typ: Zeichenfolge Längenbeschränkungen: Minimale Länge beträgt 1 Zeichen. Die maximale Länge beträgt 1011. Pattern: `arn:.+` Erforderlich: Ja
Status der Überprüfung	Der Status der AppClient Überprüfung. Typ: Zeichenfolge Zulässige Werte: `pending_verification | verified | rejected` Erforderlich: Ja
appClientId	Die ID der AppClient. Zur Verwendung in O-Auth-Flows für den App-Client vorgesehen. Typ: Zeichenfolge Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Erforderlich: Nein

MeetingInsights

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Enthält eine Zusammenfassung der drei wichtigsten Besprechungen sowie den Zweck der Besprechung, zugehörige anwendungsübergreifende Artefakte und Aktivitäten aus Aufgaben, E-Mails, Nachrichten und Kalenderereignissen.

Parameter	Beschreibung
Insight-ID	Die eindeutige ID für den generierten Einblick.
Insight-Inhalt	Die Beschreibung des Insights, in der die Details in einem Zeichenkettenformat hervorgehoben werden. Zum Beispiel, warum diese Erkenntnis wichtig ist.
Titel der Einsicht	Der Titel des generierten Einblicks.
createdAt	Wann der Einblick generiert wurde.
Kalender/Ereignis	Das wichtige Kalenderereignis oder die wichtige Besprechung, auf die sich der Benutzer konzentrieren sollte. Objekt „Kalenderereignis“: • `startTime` — Die Startzeit des Ereignisses. • `endTime`— Die Endzeit der Veranstaltung. • `eventUrl`— Die URL für das Kalenderereignis in der ISV-App.
Ressourcen	Die Liste mit den anderen Ressourcen, die sich auf die Generate The Insight beziehen. Ressourcenobjekt: • `appName`— Der Name der App, zu der die Ressource gehört. • `resourceTitle` — Der Titel der Ressource. • `resourceType` — Der Typ der Ressource. Die möglichen Werte sind: `EMAIL | EVENT | MESSAGE | TASK` • `resourceUrl` — Die Ressourcen-URL in der App.

Parameter	Beschreibung
	• `appIconUrl` — Die Bild-URL der App, zu der die Ressource gehört.
nextToken	Das Paginierungstoken zum Abrufen der nächsten Reihe von Erkenntnissen. Es ist ein optionales Feld, das, wenn es Null zurückgegeben wird, bedeutet, dass keine weiteren Erkenntnisse geladen werden müssen.

VerificationDetails

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Enthält den Status und den Grund für die AppClient Überprüfung.

Parameter	Beschreibung
Status der Überprüfung	Der Status der AppClient Überprüfung. Typ: Zeichenfolge Zulässige Werte: `pending_verification | verified | rejected` Erforderlich: Ja
Grund für den Status	Der Grund AppClient für den Bestätigungsstatus. Typ: Zeichenfolge Längenbeschränkungen: Minimale Länge von 1. Maximale Länge beträgt 1024 Zeichen. Erforderlich: Nein

Häufige Fehler

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

In diesem Abschnitt sind die Fehler aufgeführt, die bei den API-Aktionen für die AWS AppFabric Produktivitätsfunktionen häufig auftreten.

Alle anderen AppFabric häufigen API-Fehler finden Sie Fehlerbehebung in der AWS AppFabric API-Referenz unter Häufig auftretende AWS AppFabric API-Fehler.

Name der Ausnahme	Beschreibung
TokenException	Die Token-Anfrage ist nicht gültig. HTTP Status Code: 400

Datenverarbeitung

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

AppFabric unternimmt Schritte, um Benutzerinhalte einzeln, in einem Amazon S3 S3-Bucket, der von und getrennt verwaltet wird AppFabric, zu speichern. Dadurch wird sichergestellt, dass wir benutzerspezifische Erkenntnisse generieren. Wir treffen angemessene Sicherheitsvorkehrungen, um Ihre Inhalte zu schützen. Dazu kann auch die Verschlüsselung im Speicher und bei der Übertragung gehören. Wir haben unsere Systeme so konfiguriert, dass Kundeninhalte innerhalb von 30 Tagen nach der Aufnahme automatisch gelöscht werden. AppFabric generiert keine Erkenntnisse mithilfe von Datenartefakten, auf die ein Benutzer keinen Zugriff mehr hat. Zum Beispiel, wenn ein Benutzer die Verbindung zu einer Datenquelle (einer App) trennt, die Erfassung von Daten aus dieser App AppFabric beendet und keine verbleibenden Artefakte aus den getrennten Apps verwendet, um Erkenntnisse zu generieren. AppFabricDie Systeme sind so konfiguriert, dass sie solche Daten innerhalb von 30 Tagen löschen.

AppFabric verwendet keine Benutzerinhalte, um die zugrunde liegenden großen Sprachmodelle zu trainieren oder zu verbessern, die zur Gewinnung von Erkenntnissen verwendet werden. Weitere Informationen AppFabric zur generativen KI-Funktion finden Sie in den häufig gestellten Fragen zu Amazon Bedrock.

Verschlüsselung im Ruhezustand

AWS AppFabric unterstützt Verschlüsselung im Ruhezustand, eine serverseitige Verschlüsselungsfunktion, mit der alle Benutzerdaten AppFabric transparent verschlüsselt werden, wenn sie dauerhaft auf der Festplatte gespeichert werden, und sie beim Zugriff auf die Daten entschlüsselt werden.

Verschlüsselung während der Übertragung

AppFabric sichert alle Inhalte während der Übertragung mit TLS 1.2 und signiert API-Anfragen für AWS Dienste mit AWS Signature Version 4.

Terminologie und Konzepte

In diesem Thema werden die wichtigsten Begriffe und Konzepte beschrieben AWS AppFabric , um Ihnen den Einstieg zu erleichtern.

App-Paket

In einem AppFabric App-Bundle werden alle Ihre AppFabric App-Autorisierungen und -Eingaben gespeichert (siehe die folgende Definition von Datenerfassungen). Sie können pro Person ein App-Bundle erstellen. AWS-Konto AWS-Region

AppClient (auch App-Client und Anwendungsclient)

Eine OAuth AppClient für die Datenempfänger-App. Jede Datenempfänger-App muss sich registrieren und auf AppClient Daten zugreifen AppFabric . Ein Entwickler-Benutzer benötigt ein AWS Konto, um sich zu registrieren AppClient. Jedes AWS Konto kann nur eines registrieren AppClient. AppFabric verkauft Zugriffstoken auf der Grundlage von. AppClient AppClient enthält Informationen rund um die Datenempfänger-App, die über diese AppClient App auf AppFabric Daten zugreift.

Autorisierung der App

Eine App-Autorisierung gewährt die AppFabric Erlaubnis, eine Verbindung zu Ihren Anwendungen herzustellen und mit ihnen zu interagieren. Sie ermöglicht die Erfassung von Audit-Logs aus Ihren Anwendungen mithilfe von OAuth (Open Authorization — ein offener Standard für die Delegierung von Zugriffen, um Anwendungen Zugriff zu gewähren) oder PAT (Personal Access Token). Sie können mehrere App-Autorisierungen (bis zu 50) pro App-Bundle einrichten. Auf diese Weise können AppFabric Auditprotokolle von mehreren Mandanten von Anwendungen aufgenommen werden, indem der Schritt zur Erstellung der App-Autorisierung nach Bedarf für jeden Mandanten der Anwendung wiederholt wird. Die gemeinsam genutzten Anmeldeinformationen werden mit einem AWS-eigener Schlüssel oder einem vom Kunden verwalteten Schlüssel aus AWS Key Management Service (AWS KMS) verschlüsselt und in AppFabric gespeichert.

Verschlucken

Bei einer AppFabric Aufnahme wird eine App-Autorisierung verwendet, um Audit-Logs aus einer Anwendung über die öffentlichen APIs der Anwendung abzurufen. Anschließend werden die Auditprotokolle an ein oder mehrere (bis zu fünf) Ziele gesendet.

Client-ID

Wenn Sie eine App-Autorisierung für die Verbindung mit einer Anwendung erstellen, die den OAuth-Flow verwendet, werden Sie AppFabric möglicherweise nach der Client-ID und dem geheimen Client-Schlüssel gefragt. Die Client-ID und das Client-Geheimnis finden Sie in der Authentifizierungs-App Ihrer Anwendung. Anweisungen, wo Sie die Client-ID in einer bestimmten Authentifizierungs-App finden, finden Sie unter Unterstützte Anwendungen. Die Client-ID und der geheime Client-Schlüssel, die gemeinsam genutzt werden, werden mit einem AWS-eigener Schlüssel oder einem vom Kunden verwalteten AWS KMS Schlüssel verschlüsselt und in gespeichert AppFabric.

Clientschlüssel

Wenn Sie eine App-Autorisierung für die Verbindung mit einer Anwendung erstellen, die den OAuth-Flow verwendet, werden Sie AppFabric möglicherweise nach der Client-ID und dem geheimen Client-Schlüssel gefragt. Die Client-ID und das Client-Geheimnis finden Sie in der Authentifizierungs-App Ihrer Anwendung. Anweisungen dazu, wo Sie den geheimen Client-Schlüssel in einer bestimmten Authentifizierungs-App finden, finden Sie unter Unterstützte Anwendungen. Die Client-ID und der geheime Client-Schlüssel, die gemeinsam genutzt werden, werden mit einem AWS-eigener Schlüssel oder einem vom Kunden verwalteten AWS KMS Schlüssel verschlüsselt und in gespeichert AppFabric.

Ziel der Aufnahme

Ein Aufnahmeziel definiert, wo die Audit-Logs, die aus einer Aufnahme abgerufen wurden, gespeichert werden sollen. Bei jeder Aufnahme können Auditprotokolle an ein oder mehrere Ziele (bis zu fünf) gesendet werden, bei denen es sich um einen Amazon Simple Storage Service (Amazon S3) -Bucket oder eine Amazon Data Firehose in Ihrem handelt. AWS-Konto Für jedes Ziel können Sie definieren, ob die Protokolle in Rohform oder in einem Open Cybersecurity Schema Framework (OCSF) -Schema (OCSF) normalisiert werden sollen. Wenn Sie das OCSF-Schema auswählen, können Sie das Format der Protokolle (JSON oder) definieren. Apache Parquet Das Apache Parquet Format kann nur verwendet werden, wenn Amazon S3 als Ziel ausgewählt ist.

Apps für Datenempfänger

Apps, die anrufen AppFabric , um generierte Erkenntnisse zu erhalten AppFabric.

OAuth

OAuth ist ein offenes Protokoll, das eine sichere Autorisierung mit einer einfachen Standardmethode über Web-, Mobil- und Desktop-Anwendungen ermöglicht. AppFabric verwendet OAuth, um einige App-Autorisierungen zu erstellen.

Öffnen Sie das Cybersecurity Schema Framework (OCSF)

Das Open Cybersecurity Schema Framework (OCSF) ist ein Open-Source-Projekt, das ein erweiterbares Framework für die Entwicklung von Schemas sowie ein herstellerunabhängiges Kernsicherheitsschema bereitstellt. Anbieter und andere Datenproduzenten können das Schema für ihre spezifischen Domänen übernehmen und erweitern. Ziel ist es, einen offenen Standard bereitzustellen, der in jeder Umgebung, Anwendung oder Lösung eingesetzt werden kann und gleichzeitig bestehende Sicherheitsstandards und -prozesse ergänzt. AppFabric hat dieses Schema erweitert, um eine auf Software as a Service (SaaS) ausgerichtete Ereignisstruktur zu erstellen, auf die alle von SaaS-Anwendungen unterstützten Audit-Logs normalisiert AppFabric werden. Weitere Informationen finden Sie unter Öffnen Sie das Cybersecurity Schema Framework.

Persönliches Zugriffstoken (PAT)

Ein Personal Access Token (PAT) ist eine Zeichenfolge, die anstelle des üblichen Passworts für den Zugriff auf ein Computersystem verwendet werden kann. Wenn Sie eine App-Autorisierung für die Verbindung mit einer Anwendung erstellen, die den PAT-Flow verwendet, werden Sie AppFabric möglicherweise nach einem PAT gefragt. Die PAT finden Sie in der Authentifizierungs-App Ihrer Anwendung. Anweisungen dazu, wo Sie die PAT in einer bestimmten Authentifizierungs-App finden, finden Sie unter Unterstützte Anwendungen. Die gemeinsam genutzten Dienstkonto-Token werden mit einem AWS-eigener Schlüssel oder einem vom Kunden verwalteten AWS KMS Schlüsselschlüssel verschlüsselt und in gespeichert AppFabric.

Dienstkonto-Token

Wenn Sie eine AppFabric App-Autorisierung für die Verbindung mit einer Anwendung erstellen, muss für einige Anwendungen ein Dienstkonto für die Anwendungsauthentifizierung erstellt werden. AppFabric fragt möglicherweise im Rahmen des App-Autorisierungsprozesses nach dem Dienstkonto-Token. Anweisungen dazu, wo Sie das Dienstkonto-Token in einer bestimmten Authentifizierungs-App finden, finden Sie unter Unterstützte Anwendungen. Die gemeinsam genutzten Dienstkonto-Token werden mit einem AWS-eigener Schlüssel oder einem vom Kunden verwalteten AWS KMS Schlüsselschlüssel verschlüsselt und in gespeichert AppFabric.

Tenant-ID

Wenn Sie eine App-Autorisierung erstellen, werden Sie AppFabric möglicherweise nach der Mandanten-ID und dem Mandantennamen Ihrer App gefragt. Die Mandanten-ID ist eine eindeutige Kennung für Ihren Anwendungsmandanten. Jede Anwendung kann unterschiedliche Begriffe für einen Mandanten haben, z. B. Workspace-ID für Slack oder Domain-ID fürAsana. Anweisungen

dazu, wo Sie die Mandanten-ID in einer bestimmten Anwendung finden, finden Sie unter Unterstützte Anwendungen.

Name des Mandanten

Wenn Sie eine App-Autorisierung erstellen, werden Sie AppFabric möglicherweise nach der Mandanten-ID und dem Mandantennamen Ihrer App gefragt. Der Mandantenname ist ein eindeutiger Name, den Sie der Mandanten-ID geben und der innerhalb eines App-Bundles verwendet werden soll. Dieser Wert wird verwendet, um die App-Autorisierung und alle damit verbundenen Datenerfassungen zu kennzeichnen.

Sicherheit in AWS AppFabric

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS -Services in der läuft AWS Cloud. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für gelten AWS AppFabric, finden Sie unter AWS Services im Umfang nach Compliance-Programmen AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS -Service , was Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung anwenden können AppFabric. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AppFabric , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere verwenden können AWS -Services , die Ihnen bei der Überwachung und Sicherung Ihrer AppFabric Ressourcen helfen.

Themen

Datenschutz in AWS AppFabric

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS AppFabric. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS -Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie im Abschnitt Datenschutz FAQ. Informationen zum Datenschutz in Europa finden Sie im AWS Shared Responsibility Model und im GDPR Blogbeitrag auf dem AWS Security Blog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden SieSSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS -Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie FIPS 140-3 validierte kryptografische Module für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine benötigenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter Federal Information Processing Standard () 140-3. FIPS

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole arbeiten AppFabric oder sie anderweitig AWS -Services verwenden,API, AWS CLI oder. AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen in den angebenURL, um Ihre Anfrage an diesen Server zu überprüfen.

> **Note**
>
> Weitere Informationen zum Datenschutz in Bezug auf die Sicherheit AppFabric finden Sie unterDatenverarbeitung.

Verschlüsselung im Ruhezustand

AWS AppFabric unterstützt Verschlüsselung im Ruhezustand, eine serverseitige Verschlüsselungsfunktion, mit der alle Daten, die sich auf Ihre App-Bundles beziehen, AppFabric transparent verschlüsselt werden, wenn sie dauerhaft auf der Festplatte gespeichert sind, und sie beim Zugriff auf die Daten entschlüsselt werden. AppFabric Verschlüsselt Ihre Daten standardmäßig mit einem from (). AWS-eigener Schlüssel AWS Key Management Service AWS KMS Sie können sich auch dafür entscheiden, Ihre Daten mit Ihrem eigenen, vom Kunden verwalteten Schlüssel von zu verschlüsseln. AWS KMS

Wenn Sie ein App-Bundle löschen, werden alle zugehörigen Metadaten dauerhaft gelöscht.

Verschlüsselung während der Übertragung

Wenn Sie ein App-Bundle konfigurieren, können Sie entweder einen AWS-eigener Schlüssel oder einen vom Kunden verwalteten Schlüssel wählen. Beim Sammeln und Normalisieren der Daten für eine Audit-Log-Ingestion werden die Daten vorübergehend in einem Zwischenspeicher von Amazon Simple Storage Service (Amazon S3) AppFabric gespeichert und mit diesem Schlüssel verschlüsselt. Dieser Zwischen-Bucket wird nach 30 Tagen mithilfe einer Bucket-Lifecycle-Richtlinie gelöscht.

AppFabric sichert alle Daten während der Übertragung mithilfe von TLS 1.2 und signiert API Anfragen für AWS -Services mit AWS Signature V4.

Schlüsselverwaltung

AppFabric unterstützt die Verschlüsselung von Daten mit einem AWS-eigener Schlüssel oder einem vom Kunden verwalteten Schlüssel. Wir empfehlen Ihnen, einen vom Kunden verwalteten Schlüssel zu verwenden, da Sie damit die volle Kontrolle über Ihre verschlüsselten Daten haben. Wenn Sie sich für einen vom Kunden verwalteten Schlüssel entscheiden, AppFabric fügt er dem vom Kunden verwalteten Schlüssel eine Ressourcenrichtlinie hinzu, die ihm Zugriff auf den vom Kunden verwalteten Schlüssel gewährt.

Kundenverwalteter Schlüssel

Um einen vom Kunden verwalteten Schlüssel zu erstellen, folgen Sie den Schritten zum Erstellen symmetrischer KMS Verschlüsselungsschlüssel im AWS KMS Entwicklerhandbuch.

Schlüsselrichtlinie

Wichtige Richtlinien regeln den Zugriff auf Ihre vom Kunden verwalteten Schlüssel. Jeder vom Kunden verwaltete Schlüssel muss über genau eine Schlüsselrichtlinie verfügen, die aussagt, wer den Schlüssel wie verwenden kann. Wenn Sie Ihren vom Kunden verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Informationen zum Erstellen einer Schlüsselrichtlinie finden Sie unter Erstellen einer Schlüsselrichtlinie im AWS KMS Entwicklerhandbuch.

Um einen vom Kunden verwalteten Schlüssel mit verwenden zu können AppFabric, muss der Benutzer oder die Rolle AWS Identity and Access Management (IAM), die Ihre AppFabric Ressourcen erstellt haben, über die Berechtigung verfügen, Ihren vom Kunden verwalteten Schlüssel zu verwenden. Wir empfehlen Ihnen, einen Schlüssel zu erstellen, den Sie nur mit diesem Schlüssel verwenden, AppFabric und Ihre AppFabric Benutzer als Benutzer des Schlüssels hinzuzufügen. Dieser Ansatz schränkt den Umfang des Zugriffs auf Ihre Daten ein. Die Berechtigungen, die Ihre Benutzer benötigen, lauten wie folgt:

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Decrypt`

Die AWS KMS Konsole führt Sie durch die Erstellung eines Schlüssels mit der entsprechenden Schlüsselrichtlinie. Weitere Informationen zu wichtigen Richtlinien finden Sie unter Wichtige Richtlinien AWS KMS im AWS KMS Entwicklerhandbuch.

Im Folgenden finden Sie ein Beispiel für eine wichtige Richtlinie, die Folgendes ermöglicht:

- Die Root-Benutzer des AWS-Kontos vollständige Kontrolle über den Schlüssel.
- Benutzer, mit denen Sie AppFabric Ihren vom Kunden verwalteten Schlüssel verwenden dürfen AppFabric.
- Eine wichtige Richtlinie für die Einrichtung eines App-Bundles in`us-east-1`.

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow access to principals authorized to use AWS AppFabric",
            "Effect": "Allow",
            "Principal": {"AWS": "IAM-role/user-creating-appfabric-resources"},
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "appfabric.us-east-1.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        }
    ]
```

```
}
```

Wie AppFabric verwendet Zuschüsse in AWS KMS

AppFabric erfordert einen Zuschuss, um Ihren vom Kunden verwalteten Schlüssel verwenden zu können. Weitere Informationen finden Sie unter Grants AWS KMS im AWS KMS Developer Guide.

Wenn Sie ein App-Bundle erstellen, AppFabric erstellt es in Ihrem Namen einen Zuschuss, indem Sie eine `CreateGrant` Anfrage an senden AWS KMS. Zuschüsse in AWS KMS werden verwendet, um AppFabric Zugriff auf einen AWS KMS Schlüssel in einem Kundenkonto zu gewähren. AppFabric setzt voraus, dass der Zuschuss Ihren vom Kunden verwalteten Schlüssel für die folgenden internen Operationen verwendet:

- Senden Sie `GenerateDataKey` Anfragen AWS KMS zur Generierung von Datenschlüsseln, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt sind.
- Senden Sie `Decrypt` Anfragen AWS KMS zur Entschlüsselung der verschlüsselten Datenschlüssel, sodass diese zur Verschlüsselung Ihrer Daten und zur Entschlüsselung von Anwendungszugriffstoken während der Übertragung verwendet werden können.
- Senden Sie `Encrypt` Anfragen an, AWS KMS um Zugriffstoken für Anwendungen während der Übertragung zu verschlüsseln.

Im Folgenden finden Sie ein Beispiel für einen Zuschuss.

```
{
  "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"
    }
  }
},
```

Wenn Sie ein App-Paket löschen, werden gewährte Zuschüsse für Ihren vom Kunden verwalteten Schlüssel AppFabric zurückgezogen.

Überwachen Sie Ihre Verschlüsselungsschlüssel für AppFabric

Wenn Sie vom AWS KMS Kunden verwaltete Schlüssel mit verwenden AppFabric, können Sie AWS CloudTrail Protokolle verwenden, um Anfragen nachzuverfolgen, die AppFabric an gesendet AWS KMS werden.

Im Folgenden finden Sie ein Beispiel `CreateGrant` für ein CloudTrail Ereignis, das protokolliert wird, wenn Ihr vom Kunden verwalteter Schlüssel AppFabric verwendet wird.

```
{
    "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"
    }
}
```

Identitäts- und Zugriffsmanagement für AWS AppFabric

AWS Identity and Access Management (IAM) hilft einem Administrator AWS -Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um AppFabric Ressourcen zu verwenden. IAMist eine AWS -Service , die Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie arbeiten AppFabric.

Dienstbenutzer — Wenn Sie den AppFabric Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AppFabric Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in nicht auf eine Funktion zugreifen können AppFabric, finden Sie weitere Informationen unterFehlerbehebung bei AWS AppFabric Identität und Zugriff.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für AppFabric Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf AppFabric. Es ist Ihre Aufgabe, zu bestimmen, auf welche AppFabric Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit verwenden kann AppFabric, finden Sie unterWie AWS AppFabric funktioniert mit IAM.

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff darauf zu verwalten AppFabric. Beispiele für AppFabric identitätsbasierte Richtlinien, die Sie in verwenden könnenIAM, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS AppFabric

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM Rolle übernehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAMIdentity Center-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit der Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAMBenutzerhandbuch unter AWS API Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-

Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS -Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS -Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS -Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach

Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe ist eine Identität, die eine Sammlung von IAM Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM Rollen im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in. IAM Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.

- Temporäre IAM Benutzerberechtigungen — Ein IAM Benutzer oder eine Rolle kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um jemandem (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS -Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM
- Serviceübergreifender Zugriff — Einige AWS -Services verwenden Funktionen in anderen. AWS -Services Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der an aufruft AWS -Service, kombiniert mit der Anforderung, Anfragen AWS -Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS -Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS -Service an eine.
  - Dienstbezogene Rolle — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS -Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance

ausgeführt werden und AWS API Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle (anstelle eines Benutzers) erstellt werden?. IAM

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

Administratoren können mithilfe von AWS JSON Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. AWS-Konto Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS -Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien nicht IAM in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Amazon S3 und AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bietenACLs. Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen AWS Organizations. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Geräte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt

wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAMBenutzerhandbuch unter Bewertungslogik für Richtlinien.

Wie AWS AppFabric funktioniert mit IAM

Informieren Sie sich vor der Verwendung IAM zur Verwaltung des Zugriffs auf AppFabric, welche IAM Funktionen zur Verwendung verfügbar sind AppFabric.

IAMFunktionen, die Sie zusammen verwenden können AWS AppFabric

IAMMerkmal	AppFabric Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Nein
ACLs	Nein
ABAC(Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Nein
Hauptberechtigungen	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie AppFabric und welche Funktionen mit den meisten IAM Funktionen AWS -Services funktionieren, finden Sie IAM im IAMBenutzerhandbuch unter AWS Dienste, die mit funktionieren.

Identitätsbasierte Richtlinien für AppFabric

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie im IAMBenutzerhandbuch unter Referenz zu IAM JSON Richtlinienelementen.

Beispiele für identitätsbasierte Richtlinien für AppFabric

Beispiele für AppFabric identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS AppFabric

Ressourcenbasierte Richtlinien finden Sie in AppFabric

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS -Services

Um den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource

unterscheiden AWS-Konten, muss ein IAM Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource gewähren. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie IAMim IAMBenutzerhandbuch unter Kontoübergreifender Ressourcenzugriff.

Politische Maßnahmen für AppFabric

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Action` Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der AppFabric Aktionen finden Sie unter Aktionen definiert von AWS AppFabric in der Serviceautorisierungsreferenz.

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AppFabric verwendet:

```
appfabric
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "appfabric:action1",
      "appfabric:action2"
         ]
```

Sie können mehrere Aktionen mithilfe von Platzhalterzeichen (*) angeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `List` beginnen, einschließlich der folgenden Aktion:

```
"Action": "appfabric:List*"
```

Beispiele für AppFabric identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS AppFabric

Politische Ressourcen für AppFabric

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der AppFabric Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Ressourcentypen definiert von AWS AppFabric in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie die ARN einzelnen Ressourcen spezifizieren können, finden Sie unter Aktionen definiert von AWS AppFabric.

Beispiele für AppFabric identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS AppFabric

Bedingungsschlüssel für Richtlinien für AppFabric

Unterstützt dienstspezifische Richtlinien-Bedingungsschlüssel: Nein

Administratoren können mithilfe von AWS JSON Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontext-Schlüssel für AWS globale Bedingungen im IAMBenutzerhandbuch.

Eine Liste der AppFabric Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS AppFabric in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Aktionen definiert von AWS AppFabric.

Beispiele für AppFabric identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS AppFabric

ACLsin AppFabric

UnterstütztACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

ABACmit AppFabric

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt vonABAC. Anschließend entwerfen Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu finden Sie ABAC unter Was ist? ABAC im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

Verwenden temporärer Anmeldeinformationen mit AppFabric

Unterstützt temporäre Anmeldeinformationen: Nein

Einige funktionieren AWS -Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen darüber, AWS -Services wie Sie mit temporären Anmeldeinformationen arbeiten können AWS -Services , finden Sie IAM im IAMBenutzerhandbuch unter Informationen zum Arbeiten mit.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Kennwort anmelden. Wenn

Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Rollenwechsel finden Sie unter Wechseln zu einer Rolle (Konsole) im IAMBenutzerhandbuch.

Mit dem AWS CLI oder können Sie manuell temporäre Anmeldeinformationen erstellen AWS API. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen unter IAM.

Serviceübergreifende Prinzipalberechtigungen für AppFabric

Unterstützt Forward-Access-Sitzungen (FAS): Ja

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS -Service, kombiniert mit der Anforderung, Anfragen AWS -Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS -Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AppFabric

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS -Service an eine.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann zu AppFabric Funktionseinschränkungen führen. Bearbeiten Sie Servicerollen nur, AppFabric wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für AppFabric

Unterstützt dienstbezogene Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS - Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von AppFabric dienstbezogenen Rollen finden Sie unter. Verwenden von serviceverknüpften Rollen für AppFabric

Beispiele für identitätsbasierte Richtlinien für AWS AppFabric

Standardmäßig sind Benutzer und Rollen nicht berechtigt, AppFabric Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen AWS API. Um Benutzern die Berechtigung zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter IAMRichtlinien erstellen im IAMBenutzerhandbuch.

Einzelheiten zu Aktionen und Ressourcentypen, die von definiert wurden AppFabric, einschließlich des Formats von ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS AppFabric in der Service Authorization Reference.

Inhalt

- Erlauben Sie vollen Zugriff auf Produktivitätsfunktionen
- Erlauben Sie den Zugriff zum Erstellen AppClients
- Erlauben Sie den Zugriff, um Details zu erhalten AppClients
- Erlauben Sie den Zugriff auf die Liste AppClients
- Erlauben Sie den Zugriff auf das Update AppClients
- Erlauben Sie den Zugriff zum Löschen AppClients
- Erlauben Sie den Zugriff, um Anwendungen zu autorisieren
- Andere IAM Richtlinienbeispiele
  - Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AppFabric Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie AWS im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen.
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen

verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS -Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.

- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.
- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Um festzulegen, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Verwenden der AppFabric Konsole

Hängen Sie die `AWSAppFabricReadOnlyAccess` AWS verwaltete Richtlinie an Ihre IAM Identitäten an, um ihnen nur Leseberechtigungen für den AppFabric Dienst zu gewähren, einschließlich der AppFabric Konsole in der. AWS Management Console Oder Sie können die `AWSAppFabricFullAccess` AWS verwaltete Richtlinie an Ihre IAM Identitäten anhängen, um ihnen vollständige Administratorrechte für den Dienst zu gewähren. AppFabric Weitere Informationen finden Sie unter AWS verwaltete Richtlinien für AWS AppFabric.

AppFabric für Beispiele für IAM Sicherheitsrichtlinien

Die folgenden Richtlinienbeispiele beziehen sich auf AppFabric die vier Sicherheitsfunktionen.

Erlauben Sie den Zugriff auf App-Bundles

Das folgende Richtlinienbeispiel gewährt Zugriff auf App-Bundles im AppFabric Dienst.

```
{
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Beschränken Sie den Zugriff auf App-Bundles

Das folgende Richtlinienbeispiel schränkt den Zugriff auf App-Bundles im Dienst ein. AppFabric

```
{
    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Schränkt das Löschen oder Stoppen von Datenerfassungen ein

Das folgende Richtlinienbeispiel schränkt das Löschen oder Stoppen von Datenerfassungen im Service ein. AppFabric

```
{
    "Statement": [
        {
```

```
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StopIngestion",
                "appfabric:DeleteIngestion",
                "appfabric:DeleteIngestionDestination"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

AppFabric für Beispiele für Produktivitätspolitik IAM

Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Die folgenden Richtlinienbeispiele gelten AppFabric für die Funktionen zur Steigerung der Produktivität.

Erlauben Sie den Lesezugriff auf Produktivitätsfunktionen

Das folgende Richtlinienbeispiel gewährt nur Lesezugriff auf die AppFabric Produktivitätsfunktionen.

> **Important**
>
> Beim Hinzufügen dieser Richtlinie im Richtlinien-Editor der Konsole wird möglicherweise der JSON Fehler „Ungültige Aktion“ angezeigt. IAM Das liegt daran, dass sich die Funktionen aus AppFabric Produktivitätsgründen derzeit in der Vorschauversion befinden. Sie sollten den Fehler ignorieren und mit der Erstellung der Richtlinie fortfahren.

```
{
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
                "appfabric:ListActionableInsights",
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights"
            ],
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

Erlauben Sie vollen Zugriff auf Produktivitätsfunktionen

Das folgende Richtlinienbeispiel gewährt vollen Zugriff auf AppFabric die Produktivitätsfunktionen.

> **Important**
>
> Beim Hinzufügen dieser Richtlinie im Richtlinien-Editor der IAM Konsole wird möglicherweise der JSON Fehler „Ungültige Aktion“ angezeigt. Das liegt daran, dass sich die Funktionen aus AppFabric Produktivitätsgründen derzeit in der Vorschauversion befinden. Sie sollten den Fehler ignorieren und mit der Erstellung der Richtlinie fortfahren.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient",
                "appfabric:DeleteAppClient",
                "appfabric:GetAppClient",
                "appfabric:ListActionableInsights",
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights",
                "appfabric:PutFeedback",
                "appfabric:Token"
                "appfabric:UpdateAppClient"
            ],
            "Resource": "*"
```

```
        }
    ],
    "Version": "2012-10-17"
}
```

Erlauben Sie den Zugriff zum Erstellen AppClients

Das folgende Richtlinienbeispiel gewährt Zugriff auf create AppClients. Weitere Informationen finden Sie unter Erstellen eines aus AppFabric Produktivitätsgründen AppClient.

> **Important**
>
> Beim Hinzufügen dieser Richtlinie im Richtlinien-Editor der IAM Konsole wird möglicherweise der JSON Fehler „Ungültige Aktion“ angezeigt. Das liegt daran, dass sich die Funktionen aus AppFabric Produktivitätsgründen derzeit in der Vorschauversion befinden. Sie sollten den Fehler ignorieren und mit der Erstellung der Richtlinie fortfahren.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Erlauben Sie den Zugriff, um Details zu erhalten AppClients

Das folgende Richtlinienbeispiel gewährt Zugriff auf das Abrufen von Details zu AppClients. Weitere Informationen finden Sie unter Details zu einem abrufen AppClient.

> **Important**
>
> Beim Hinzufügen dieser Richtlinie im JSON Richtlinieneditor der IAM Konsole wird möglicherweise der Fehler „Ungültige Aktion“ angezeigt. Das liegt daran, dass sich die

Funktionen aus AppFabric Produktivitätsgründen derzeit in der Vorschauversion befinden. Sie sollten den Fehler ignorieren und mit der Erstellung der Richtlinie fortfahren.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Erlauben Sie den Zugriff auf die Liste AppClients

Das folgende Richtlinienbeispiel gewährt Zugriff auf die Liste AppClients. Weitere Informationen finden Sie unter Details zu einem abrufen AppClient.

Important

Beim Hinzufügen dieser Richtlinie im JSON Richtlinieneditor der IAM Konsole wird möglicherweise der Fehler „Ungültige Aktion“ angezeigt. Das liegt daran, dass sich die Funktionen aus AppFabric Produktivitätsgründen derzeit in der Vorschauversion befinden. Sie sollten den Fehler ignorieren und mit der Erstellung der Richtlinie fortfahren.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:ListAppClients"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
```

```
    "Version": "2012-10-17"
}
```

Erlauben Sie den Zugriff auf das Update AppClients

Das folgende Richtlinienbeispiel gewährt Zugriff auf Updates AppClients. Weitere Informationen finden Sie unter Aktualisieren eines AppClient.

> **Important**
>
> Beim Hinzufügen dieser Richtlinie im Richtlinien-Editor der IAM Konsole wird möglicherweise der JSON Fehler „Ungültige Aktion“ angezeigt. Das liegt daran, dass sich die Funktionen aus AppFabric Produktivitätsgründen derzeit in der Vorschauversion befinden. Sie sollten den Fehler ignorieren und mit der Erstellung der Richtlinie fortfahren.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:UpdateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Erlauben Sie den Zugriff zum Löschen AppClients

Das folgende Richtlinienbeispiel gewährt Zugriff auf Löschen AppClients. Weitere Informationen finden Sie unter Aktualisieren eines AppClient.

> **Important**
>
> Beim Hinzufügen dieser Richtlinie im Richtlinien-Editor der IAM Konsole wird möglicherweise der JSON Fehler „Ungültige Aktion“ angezeigt. Das liegt daran, dass sich die Funktionen aus AppFabric Produktivitätsgründen derzeit in der Vorschauversion befinden. Sie sollten den Fehler ignorieren und mit der Erstellung der Richtlinie fortfahren.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:DeleteAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Erlauben Sie den Zugriff, um Anwendungen zu autorisieren

Das folgende Richtlinienbeispiel gewährt Zugriff, um Anwendungen mithilfe des Tokens zu autorisieren. API Weitere Informationen finden Sie unter Authentifizieren und Autorisieren Ihrer Anwendung.

> **Important**
>
> Beim Hinzufügen dieser Richtlinie im Richtlinien-Editor der Konsole wird möglicherweise der JSON Fehler „Ungültige Aktion“ angezeigt. IAM Das liegt daran, dass sich die Funktionen aus AppFabric Produktivitätsgründen derzeit in der Vorschauversion befinden. Sie sollten den Fehler ignorieren und mit der Erstellung der Richtlinie fortfahren.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:Token"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Andere IAM Richtlinienbeispiele

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die Inline- und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. AWS CLI AWS API

```
{
    "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": "*"
        }
    ]
}
```

Verwenden von serviceverknüpften Rollen für AppFabric

AWS AppFabric verwendet AWS Identity and Access Management (IAM) dienstbezogene Rollen. Eine dienstbezogene Rolle ist ein einzigartiger Rollentyp, mit dem direkt verknüpft ist. IAM AppFabric Mit Diensten verknüpfte Rollen sind vordefiniert AppFabric und enthalten alle Berechtigungen, die der Dienst benötigt, um in AWS -Services Ihrem Namen andere Personen anzurufen.

Eine dienstbezogene Rolle AppFabric erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AppFabric definiert die Berechtigungen ihrer dienstbezogenen Rollen und AppFabric kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Zu den definierten Berechtigungen gehören die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen IAM Entität zugeordnet werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre AppFabric Ressourcen geschützt, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Diensten, die dienstbezogene Rollen unterstützen, finden Sie unter AWS Dienste, die mit Diensten arbeiten, IAM und suchen Sie in der Spalte mit dienstbezogenen Rollen nach den Diensten, für die Ja angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für AppFabric

AppFabric verwendet die serviceverknüpfte Rolle mit dem Namen `AWSServiceRoleForAppFabric` — Ermöglicht AppFabric das Ablegen von Daten in eine Aufnahmezielressource, z. B. einen Amazon S3 S3-Bucket oder einen Amazon Data Firehose-Lieferstream. Es ermöglicht auch, CloudWatch metrische Daten AppFabric in den Namespace zu stellen. `AWS/AppFabric`

Die serviceverknüpfte Rolle `AWSServiceRoleForAppFabric` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `appfabric.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie `AWSAppFabricServiceRolePolicy` AppFabric ermöglicht es, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `cloudwatch:PutMetricData` im `AWS/AppFabric` Namespace. Diese Aktion erteilt die Erlaubnis AppFabric , Metrikdaten in den CloudWatch `AWS/AppFabric` Amazon-Namespace zu

stellen. Weitere Informationen zu den in verfügbaren AppFabric Metriken finden Sie CloudWatch unterÜberwachung AWS AppFabric mit Amazon CloudWatch.

- Aktion: `s3:PutObject` in einem Amazon S3 S3-Bucket. Diese Aktion erteilt die Erlaubnis AppFabric , aufgenommene Daten in einen von Ihnen angegebenen Amazon S3 S3-Bucket zu speichern.
- Aktion: `firehose:PutRecordBatch` in einem Amazon Data Firehose-Lieferstream. Diese Aktion erteilt die Erlaubnis AppFabric , aufgenommene Daten in einen von Ihnen angegebenen Amazon Data Firehose-Lieferstream einzufügen.

Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für. AppFabric

Sie müssen Berechtigungen konfigurieren, damit eine Benutzer, Gruppen oder Rollen eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Dienstbezogene Rollenberechtigungen.

Erstellen einer dienstbezogenen Rolle für AppFabric

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein AppFabric App-Bundle in der AWS Management Console, oder der erstellen AWS CLI AWS API, AppFabric erstellt die dienstverknüpfte Rolle für Sie.

Bearbeitung einer serviceverknüpften Rolle für AppFabric

AppFabric erlaubt es Ihnen nicht, die `AWSServiceRoleForAppFabric` dienstbezogene Rolle zu bearbeiten. Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten auf die Rolle verweisen könnten. Sie können die Beschreibung der Rolle jedoch mithilfe IAM von bearbeiten. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Bearbeiten einer dienstbezogenen Rolle.

Löschen einer serviceverknüpften Rolle für AppFabric

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch alle Ihre AppFabric App-Bundles löschen, bevor Sie die dienstverknüpfte Rolle löschen können.

Bereinigen einer serviceverknüpften Rolle

Bevor Sie eine dienstverknüpfte Rolle löschen könnenIAM, müssen Sie zunächst alle Ressourcen löschen, die von der Rolle verwendet werden. App-Bundles, in denen Sie erstellen, AppFabric werden von der Rolle verwendet. Weitere Informationen finden Sie unter Aus AWS AppFabric Sicherheitsgründen löschen.

> **Note**
>
> Wenn der AppFabric Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM Konsole, die oder AWS CLI, AWS API um die mit dem `AWSServiceRoleForAppFabric` Dienst verknüpfte Rolle zu löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Löschen einer dienstbezogenen Rolle.

Unterstützte Regionen für AppFabric dienstverknüpfte Rollen

AppFabric unterstützt die Verwendung von dienstbezogenen Rollen überall dort, AWS-Regionen wo der Dienst verfügbar ist. Weitere Informationen finden Sie unter AppFabric Endpunkte und Kontingente im. Allgemeine AWS-Referenz

AWS verwaltete Richtlinien für AWS AppFabric

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um vom IAMKunden verwaltete Richtlinien zu erstellen, die Ihrem Team nur die Berechtigungen gewähren, die es benötigt. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS -Services AWS verwaltete Richtlinien verwalten und aktualisieren. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche

die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die ReadOnlyAccess AWS verwaltete Richtlinie bietet beispielsweise nur Lesezugriff auf alle Ressourcen AWS -Services . Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und eine Beschreibung der Richtlinien für Jobfunktionen finden Sie im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien für Jobfunktionen.

AWS verwaltete Richtlinie: AWSAppFabricReadOnlyAccess

Sie können die `AWSAppFabricReadOnlyAccess` Richtlinie an Ihre IAM Identitäten anhängen. Diese Richtlinie gewährt dem Dienst nur Leseberechtigungen. AppFabric

> **Note**
>
> Die `AWSAppFabricReadOnlyAccess` Richtlinie gewährt keinen schreibgeschützten Zugriff auf die AppFabric Produktivitätsfunktionen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `appfabric`— Erteilt die Berechtigung zum Abrufen eines App-Bundles, zum Auflisten von App-Bundles, zum Abrufen einer App-Autorisierung, zum Auflisten von App-Autorisierungen, zum Abrufen einer Erfassung, zum Abrufen eines Aufnahmeziels, zum Auflisten von Aufnahmezielen und zum Auflisten von Ressourcen-Tags.

```
{
    "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 verwaltete Richtlinie: AWSAppFabricFullAccess

Sie können die `AWSAppFabricFullAccess` Richtlinie an Ihre IAM Identitäten anhängen. Diese Richtlinie gewährt Administratorberechtigungen für den AppFabric Dienst.

> **Important**
>
> Die `AWSAppFabricFullAccess` Richtlinie gewährt keinen Zugriff auf die AppFabric Produktivitätsfunktionen, da sie sich derzeit in der Vorschauversion befinden. Weitere Informationen zur Gewährung des Zugriffs auf die AppFabric Produktivitätsfunktionen finden Sie unterAppFabric für Beispiele für Produktivitätspolitik IAM.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `appfabric`— Erteilt volle Administratorrechte für AppFabric.
- `kms`— Erteilt die Erlaubnis, Aliase aufzulisten.
- `s3`— Erteilt die Erlaubnis, all Ihre Amazon S3 S3-Buckets aufzulisten und den Bucket-Standort abzurufen.
- `firehose`— Erteilt die Erlaubnis, Amazon Data Firehose-Lieferstreams aufzulisten und Lieferdatenströme zu beschreiben.
- `iam`— Erteilt die Berechtigung zum Erstellen der `AWSServiceRoleForAppFabric` serviceverknüpften Rolle für. AppFabric Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AppFabric.

```
{
    "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 verwaltete Richtlinie: AWSAppFabricServiceRolePolicy

Sie können die `AWSAppFabricServiceRolePolicy` Richtlinie nicht an Ihre IAM Entitäten anhängen. Diese Richtlinie ist mit einer dienstbezogenen Rolle verknüpft, die es AppFabric ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für AppFabric.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `cloudwatch`— Erteilt die Erlaubnis AppFabric , Metrikdaten in den CloudWatch `AWS/AppFabric` Amazon-Namespace zu stellen. Weitere Informationen zu den in verfügbaren AppFabric Metriken finden Sie CloudWatch unterÜberwachung AWS AppFabric mit Amazon CloudWatch.
- `s3`— Erteilt die Erlaubnis AppFabric , aufgenommene Daten in einen von Ihnen angegebenen Amazon S3 S3-Bucket zu speichern.
- `firehose`— Erteilt die Erlaubnis AppFabric , aufgenommene Daten in einen von Ihnen angegebenen Amazon Data Firehose-Lieferstream einzufügen.

```
{
    "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"}
            }
        }
    ]
}
```

AppFabric Aktualisierungen der verwalteten AWS Richtlinien

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AppFabric seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS Feed auf der Seite AppFabric Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AWSAppFabricReadOnlyAccess – Neue Richtlinie.	AppFabric hat eine neue Richtlinie hinzugefügt, um dem Dienst nur Leseberechtigungen zu gewähren. AppFabric	27. Juni 2023
AWSAppFabricFullAccess – Neue Richtlinie.	AppFabric hat eine neue Richtlinie hinzugefügt, um dem Dienst Administratorrechte zu gewähren. AppFabric	27. Juni 2023
AWSAppFabricServiceRolePolicy – Neue Richtlinie.	AppFabric hat eine neue Richtlinie für die `AWSServiceRoleForAppFabric` dienstbezogene Rolle hinzugefügt.	27. Juni 2023

Änderung	Beschreibung	Datum
AppFabric hat begonnen, Änderungen zu verfolgen	AppFabric hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	27. Juni 2023

Fehlerbehebung bei AWS AppFabric Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AppFabric und auftreten könnenIAM.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AppFabric
- Ich bin nicht zur Ausführung von iam:PassRole autorisiert.
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AppFabric Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AppFabric

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM Benutzer versucht, die Konsole zu verwenden, um Details zu einer fiktiven *`my-example-widget`* Ressource anzuzeigen, aber nicht über die fiktiven `appfabric:`*`GetWidget`* Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 appfabric:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `appfabric:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht zur Ausführung von iam:PassRole autorisiert.

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion auszuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an diese Person übergeben können AppFabric.

Einige AWS -Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AppFabric auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AppFabric Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AppFabric unterstützt werden, finden Sie unter. Wie AWS AppFabric funktioniert mit IAM
- Informationen darüber, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM Benutzerhandbuch unter Gewähren des Zugriffs auf einen anderen IAMBenutzer AWS-Konto , dessen Eigentümer Sie sind.

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

Überprüfung der Einhaltung von Vorschriften für AWS AppFabric

Informationen darüber, ob AWS -Service ein AWS -Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS -Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS -Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

> **Note**
>
> Nicht alle sind berechtigt AWS -Services . HIPAA Weitere Informationen finden Sie in der Referenz für HIPAA qualifizierte Dienste.

- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.

- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS -Services und die Leitlinien für Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zusammengefasst.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dies AWS -Service bietet einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS -Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- AWS Audit Manager— Auf diese AWS -Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Bewährte Sicherheitsmethoden für AWS AppFabric

AWS AppFabric bietet mehrere Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden stellen allgemeine Richtlinien und keine vollständige Sicherheitslösung dar. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Überwachen Sie nach Anwendungen ohne Administratorzugriff

Mit der Berechtigung read-only AWS Identity and Access Management (IAM) kann jeder Amazon QuickSight und andere Tools zur Verwaltung von Sicherheitsinformationen und Ereignissen (SIEM) integrieren AppFabric , wie z. Splunk Zur Überwachung der Anwendungssicherheit werden Daten

an einen Amazon Simple Storage Service (Amazon S3) -Bucket oder einen Amazon Data Firehose-Lieferstream übermittelt.

Überwachen Sie Ereignisse AppFabric

Sie können das AppFabric anhand von CloudWatch Amazon-Metriken überwachen. CloudWatch sammelt Daten aus AppFabric jeder Minute und verarbeitet sie zu Metriken. Sie können Alarme einrichten, die Benachrichtigungen auslösen, wenn die Messwerte bestimmten Schwellenwerten entsprechen. Weitere Informationen finden Sie unter Überwachung AWS AppFabric mit Amazon CloudWatch.

Resilienz in AWS AppFabric

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Sicherheit der Infrastruktur in AWS AppFabric

Als verwalteter Service AWS AppFabric ist er durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Sie verwenden AWS veröffentlichte API Aufrufe, um AppFabric über das Netzwerk darauf zuzugreifen. Clients müssen TLS 1.0 oder höher unterstützen. Wir empfehlen TLS 1.2 oder höher. Kunden müssen außerdem Cipher Suites mit Perfect Forward Secrecy (PFS) wie (Ephemeral Diffie-Hellman) oder (DHEElliptic Curve Ephemeral Diffie-Hellman) unterstützen. ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Oder um temporäre

Sicherheitsanmeldeinformationen zum Signieren von Anfragen zu generieren, können Sie die AWS Security Token Service(AWS STS) verwenden.

Konfiguration und Schwachstellenanalyse in AWS AppFabric

Konfiguration und IT-Kontrollen liegen in der gemeinsamen Verantwortung AWS von Ihnen, unserem Kunden. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Überwachung AWS AppFabric

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer AWS AppFabric anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, mit denen Sie beobachten AppFabric, melden können, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen ergreifen können:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer Amazon EC2 EC2-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von Amazon EC2 EC2-Instances und anderen Quellen überwachen AWS CloudTrail, speichern und darauf zugreifen. CloudWatch Logs können Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder in Ihrem Namen getätigt wurden, AWS-Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Überwachung AWS AppFabric mit Amazon CloudWatch

Sie können die AWS AppFabric Nutzung CloudWatch überwachen. Dabei werden Rohdaten gesammelt und zu lesbaren Metriken verarbeitet, die nahezu in Echtzeit verfügbar sind. Diese Statistiken werden 15 Monate gespeichert, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Der AppFabric Service meldet die folgenden Metriken im `AWS/AppFabric` Namespace.

Metrik	Beschreibung
AppFabric Status der App-Autorisierung	Der Status der App-Autorisierung (1für verbunden; `0` für alle anderen).
AppFabric Latenz bei der Datenbereitstellung	Die Zeit (in Sekunden), die benötigt wurde AppFabric , um Audit-Logs von der SaaS-Anwendung zu sammeln und sie an das konfigurierte Ziel (Amazon S3 oder Amazon Data Firehose) zu senden.
Status des Aufnahmeziels	Der Status des Aufnahmeziels (1für aktiv; `0` für jedes andere).
Allgemeine Datenverzögerung	Der Zeitunterschied (in Sekunden) zwischen dem Zeitpunkt, an dem die Ereignisse in der SaaS-Anwendung aufgetreten sind, und dem Zeitpunkt, zu dem die entsprechenden Audit-Logs an das konfigurierte Ziel (Amazon S3 oder Amazon Data Firehose) übermittelt wurden von AppFabric.
Volumen der aufgenommenen Daten	Die Größe der Daten, die an Amazon Simple Storage Service (Amazon S3) oder Amazon Data Firehose geliefert werden.

Die folgende Dimension wird für AppFabric Metriken unterstützt.

Dimension	Beschreibung
Ziel der Aufnahme: Arn	Der Amazon-Ressourcenname (ARN) des Aufnahmeziels.

Protokollieren von AWS AppFabric API-Aufrufen mit AWS CloudTrail

AWS AppFabric ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS -Service Mitglied ausgeführten Aktionen bereitstellt AppFabric. CloudTrail erfasst alle API-Aufrufe AppFabric als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AppFabric Konsole und Codeaufrufen für die AppFabric API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AppFabric. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurde AppFabric, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

AppFabric Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität in stattfindet AppFabric, wird diese Aktivität zusammen mit anderen AWS -Service Ereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können in Ihrem AWS-Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für AppFabric, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere konfigurieren, AWS -Services um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail -Benutzerhandbuch:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail

- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle AppFabric Aktionen werden von der AWS AppFabric API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe der `GetAppBundle` Aktionen `CreateAppBundleUpdateAppBundle`, und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS -Service gesendet wurde.

Weitere Informationen finden Sie unter CloudTrail userIdentityElement im AWS CloudTrail Benutzerhandbuch.

AppFabric Logdateieinträge verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateAppBundle` Aktion demonstriert.


```
{
    "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"
    }
}
```

Kontingente für AWS AppFabric

Ihr AWS-Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jedes Kontingent AWS -Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Um die Kontingente für anzuzeigen AppFabric, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS Dienste aus und wählen Sie AppFabric.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch. Wenn das Kontingent unter Service Quotas noch nicht in verfügbar ist, verwenden Sie das Formular zur Erhöhung des Service-Limits.

Die diesbezüglichen Kontingente AppFabric , die in Ihrem enthalten AWS-Konto sind, sind in der folgenden Tabelle aufgeführt.

Name	Standard	Anpas	Beschreibung
Anwendungspakete	Jede unterstützte Region: 1	Nein	Die maximale Anzahl von Anwendungspaketen, die Sie in einem Konto in der aktuellen AWS Region erstellen können.
Autorisierungen für Anwendungen	Jede unterstützte Region: 50	Nein	Die maximale Anzahl von Anwendungsautorisierungen, die Sie in einem Konto in der aktuellen AWS Region erstellen können.
Verschlucken	Jede unterstützte Region: 50	Nein	Die maximale Anzahl von Datenaufnahmen, die Sie in einem Konto in der aktuellen Region erstellen können. AWS

Name	Standard	Anpas	Beschreibung
Ziele für die Aufnahme	Jede unterstützte Region: 5	Nein	Die maximale Anzahl von Aufnahmezielen, die Sie pro Aufnahme in einem Konto in der aktuellen Region erstellen können. AWS
AppClient	Jede unterstützte Region: 1	Nein	Die maximale Anzahl davon AppClients , die Sie in einem Konto in der aktuellen Region erstellen können. AWS Die Funktion AWS AppFabric zur Steigerung der Produktivität befindet sich in der Vorschauversion und kann sich ändern.

Dokumentenverlauf für das AppFabric Administrationshandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für beschrieben AWS AppFabric.

Änderung	Beschreibung	Datum
Neue unterstützte Anwendung	JumpCloudAls unterstützte Anwendung hinzugefügt. Weitere Informationen finden Sie unter Unterstützte Anwendungen in AWS AppFabric.	5. Juni 2024
Neue unterstützte Anwendungen und Sicherheitstool	Hinzugefügt Azure Monitor und Google Analytics als unterstützte Anwendungen. Weitere Informationen finden Sie unter Unterstützte Anwendungen in AWS AppFabric. Singularity CloudAls unterstütztes Sicherheitstool hinzugefügt. Weitere Informationen finden Sie unter Kompatible Sicherheitstools.	30. April 2024
Neue unterstützte Anwendung	SentinelOneAls unterstützte Anwendung hinzugefügt. Weitere Informationen finden Sie unter Unterstützte Anwendungen in AWS AppFabric.	25. April 2024
Neue unterstützte Anwendung	1PasswordAls unterstützte Anwendung hinzugefü	23. April 2024

	gt. Weitere Informationen finden Sie unter Unterstützte Anwendungen in AWS AppFabric.	
Neues unterstütztes Sicherheitstool	DynatraceAls kompatibles Sicherheitstool hinzugefügt. Weitere Informationen finden Sie unter Kompatible Sicherheitstools.	26. März 2024
Neue Metrik	Die Metrik „ AppFabric App-Autorisierungsstatus“ wurde hinzugefügt. Weitere Informationen finden Sie unter Überwachung AWS AppFabric mit Amazon CloudWatch Logs.	8. März 2024
Neue unterstützte Anwendung	IBM Security® VerifyAls unterstützte Anwendung hinzugefügt. Weitere Informationen finden Sie unter Unterstützte Anwendungen in AWS AppFabric.	6. März 2024
Neue unterstützte Anwendung	BoxAls unterstützte Anwendung hinzugefügt. Weitere Informationen finden Sie unter Unterstützte Anwendungen in AWS AppFabric.	28. Februar 2024

Neue unterstützte Anwendungen und Metriken	Hinzugefügt Cisco DuoSalesforce, und Terraform Cloud als unterstützte Anwendungen. Weitere Informationen zu ihnen finden Sie unter Unterstützte Anwendungen in AWS AppFabric. Die Metriken „Latenz bei der AppFabric Datenübermittlung“ und „Datenverzögerung insgesamt “ wurden hinzugefügt. Weitere Informationen finden Sie unter Überwachung AWS AppFabric mit Amazon CloudWatch Logs.	1. Februar 2024
Atlassian Confluence,, Genesys CloudHubSpotOneLogin by One IdentityPagerDuty, und Ping Identity als unterstützte Anwendungen und Barracuda XDR als kompatibles Sicherheitstool hinzugefügt	Weitere Informationen zu den neuen unterstützten Anwendungen finden Sie unter Unterstützte Anwendungen in AWS AppFabric und Kompatible Sicherheitstools.	15. Dezember 2023
Atlassian Confluence,, Genesys CloudHubSpotOneLogin by One IdentityPagerDuty, und Ping Identity als unterstützte Anwendungen und Barracuda XDR als kompatibles Sicherheitstool hinzugefügt	Weitere Informationen zu den neuen unterstützten Anwendungen finden Sie unter Unterstützte Anwendungen in AWS AppFabric und Kompatible Sicherheitstools.	15. Dezember 2023

Die AWS AppFabric Vorschaudokumentation aus Produktivitätsgründen wurde hinzugefügt	Weitere Informationen AppFabric zur Steigerung der Produktivität finden Sie unter Was AWS AppFabric dient der Produktivität?	8. November 2023
Hinzugefügte GitHub und ServiceNow als unterstützte Anwendungen	Weitere Informationen zu den neuen unterstützten Anwendungen finden Sie unter Unterstützte Anwendungen.	31. Oktober 2023
Begonnen mit der Nachverfolgung AWS verwalteter Richtlinien für AWS AppFabric	Weitere Informationen zu den AWS verwalteten Richtlinien für AppFabric finden Sie unter AWS Verwaltete Richtlinien für AWS AppFabric.	27. Juni 2023
Erstversion	Erste Version des AWS AppFabric Administratorhandbuchs.	27. Juni 2023

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.