管理ガイド

AWS AppFabric

AWS AppFabric: 管理ガイド

Table of Contents

とは AWS AppFabric 1
製品 1
利点 1
ユースケース 2
AppFabric の仕組み 2
料金 3
可用性 3
セキュリティ AWS AppFabric とは何ですか？ 3
利点 1
ユースケース 2
セキュリティ AppFabric のためのアクセス 4
関連サービス 5
OCSF スキーマ 6
前提条件と推奨事項 7
開始 13
サポートされているアプリケーション 23
互換性のあるセキュリティツール 121
リソースの削除 136
for AWS AppFabric productivity とは 138
利点 1
ユースケース 2
for productivity AppFabric へのアクセス 4
使用を開始する: アプリケーションデベロッパー向け 141
使用を開始する: エンドユーザー向け 169
AppFabric productivity APIs 186
データ処理 209
用語と概念 211
セキュリティ 215
データ保護 216
保管中の暗号化 217
転送中の暗号化 217
キー管理 217
キーポリシー 218
で 許可 AppFabric を使用する方法 AWS KMS 219

の暗号化キーのモニタリング AppFabric 221
ID およびアクセス管理 223
対象者 223
アイデンティティを使用した認証 224
ポリシーを使用したアクセスの管理 227
と の AWS AppFabric 連携方法 IAM 230
アイデンティティベースポリシーの例 237
サービスリンクロールの使用 247
AWS マネージドポリシー 250
トラブルシューティング 255
コンプライアンス検証 257
セキュリティに関するベストプラクティス 259
管理者アクセスなしでアプリケーションを監視する 259
AppFabric イベントのモニタリング 259
耐障害性 259
インフラストラクチャセキュリティ 260
設定と脆弱性の分析 260
モニタリング 261
によるモニタリング CloudWatch 261
CloudTrail ログ 262
AppFabric の情報 CloudTrail 263
AppFabric ログファイルエントリについて 264
クォータ 266
ドキュメント履歴 268
..... cclxxii

とは AWS AppFabric

AWS AppFabric は、Software as a Service (SaaS) アプリケーションを組織全体にすばやく接続するため、IT チームとセキュリティチームは標準スキーマを使用してアプリケーションを簡単に管理および保護でき、従業員は生成 AI を使用して日常的なタスクをより迅速に完了できます。

トピック

- 製品
- 利点
- ユースケース
- AppFabric の仕組み
- 料金
- 可用性
- セキュリティ AWS AppFabric とは何ですか？
- for AWS AppFabric productivity とは

製品

の 2 つの側面について説明します AWS AppFabric。セキュリティ AppFabric のため、管理とセキュリティの合理化のために設計され、生成 AI 機能で強化された生産性 (プレビュー) AppFabric のために設計されています。詳細については、次のトピックを参照してください。

- セキュリティ AWS AppFabric とは何ですか？
- for AWS AppFabric productivity とは

利点

を使用して AppFabric 、次の操作を実行できます。

- アプリケーションを数分以内に接続し、運用コストを削減します。
- SaaS アプリケーションデータ全体の可視性を高め、セキュリティ体制を強化します。
- 生成 AI を使用してアプリケーション全体のタスクを自動的に実行できます。

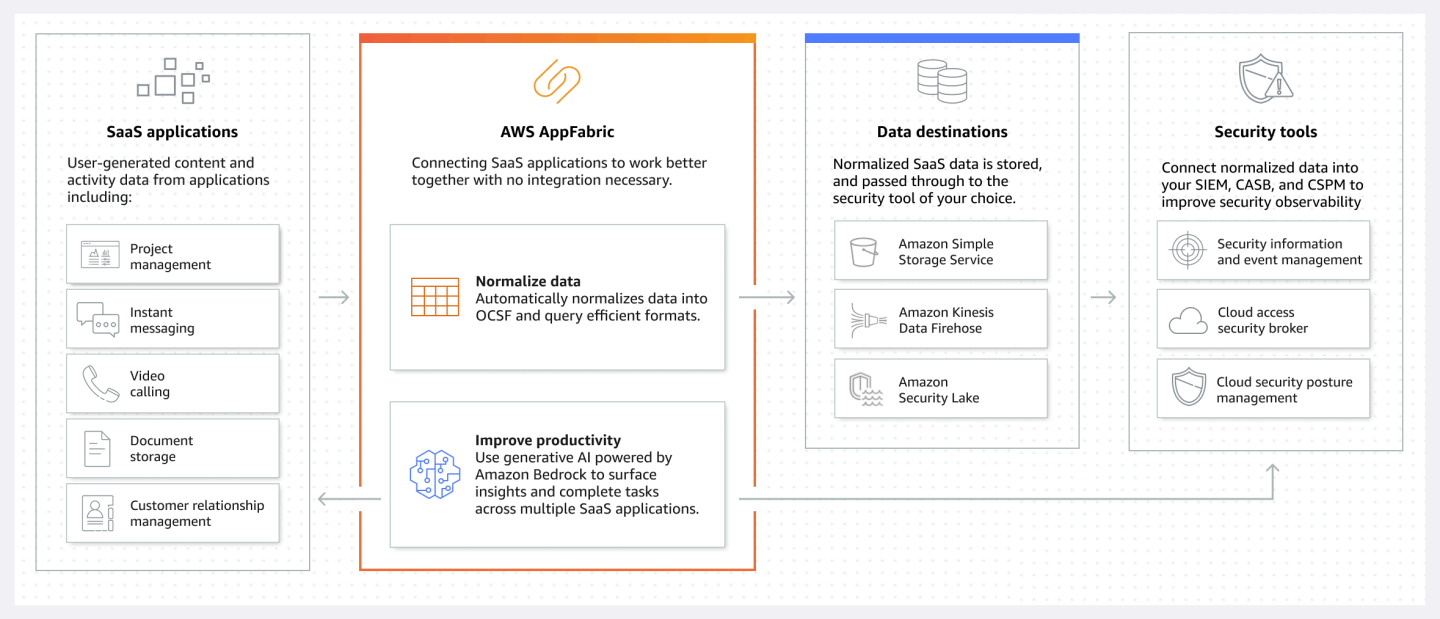
ユースケース

AppFabric を使用して次のことができます。

- SaaS アプリケーションを迅速に接続する
  - AppFabric for security は、最高の SaaS 生産性向上アプリケーションとセキュリティアプリケーションを相互にネイティブに接続し、フルマネージド型の SaaS 相互運用性ソリューションを提供します。
- セキュリティ体制を強化する
  - アプリケーションデータは自動的に正規化されるため、管理者は共通のポリシーを設定し、セキュリティアラートを標準化し、複数のアプリケーションにわたるユーザーアクセスを簡単に管理できます。
- 生産性を再構築する
  - 一般的な生成 AI アシスタントを使用すると、生産性 AppFabric 向上のために、従業員は迅速に回答を得て、タスク管理を自動化し、SaaS 生産性向上アプリケーション全体でインサイトを生成できます。

AppFabric の仕組み

AppFabric は、生産性とセキュリティを向上させるためにコーディングを必要とせずに、複数の SaaS アプリケーションをすばやく接続します。次の図は、 の利点を示しています AppFabric。



> **Note**
>
> AppFabric for productivity は現在プレビュー版としてリリースされており、米国東部 (バージニア北部) で利用可能です。 AWS リージョンの詳細については AWS リージョン、「」のAWS AppFabric 「 エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

料金

AppFabric 料金の詳細と例については、「 のAWS AppFabric 料金」を参照してください。

可用性

で現在サポートされている AWS リージョンとエンドポイントを確認するには AppFabric、「 AWS 全般のリファレンス」のAWS AppFabric 「 エンドポイントとクォータ」を参照してください。

セキュリティ AWS AppFabric とは何ですか？

AWS AppFabric for security は、Software as a Service (SaaS) アプリケーションを組織全体にすばやく接続するため、IT チームとセキュリティチームは標準スキーマを使用してアプリケーションを簡単に管理および保護できます。

トピック

- 利点
- ユースケース
- セキュリティ AppFabric のためのアクセス
- 関連サービス
- オープンサイバーセキュリティスキーマフレームワーク
- 前提条件と推奨事項
- セキュリティ AWS AppFabric のための の開始方法
- サポートされているアプリケーション
- 互換性のあるセキュリティツールとサービス

- セキュリティリソース AWS AppFabric の削除

利点

AppFabric のセキュリティのために を使用して、以下を実行できます。

- アプリケーションを数分以内に接続し、運用コストを削減します。
- SaaS アプリケーションデータ全体の可視性を高め、セキュリティ体制を強化します。

ユースケース

セキュリティ AppFabric のために を使用すると、次のことができます。

- SaaS アプリケーションを迅速に接続する
  - AppFabric for security は、最高の SaaS 生産性向上アプリケーションとセキュリティアプリケーションを相互にネイティブに接続し、フルマネージド型の SaaS 相互運用性ソリューションを提供します。
- セキュリティ体制を強化する
  - アプリケーションデータは自動的に正規化されるため、管理者は共通のポリシーを設定し、セキュリティアラートを標準化し、複数のアプリケーションにわたるユーザーアクセスを簡単に管理できます。

セキュリティ AppFabric のためのアクセス

AppFabric セキュリティ は、米国東部 (バージニア北部) 、欧州 (アイルランド) 、アジアパシフィック (東京) で利用できます AWS リージョン。の詳細については AWS リージョン、「」のAWS AppFabric 「 エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

各リージョンで、次のいずれかの方法で にアクセスしてセキュリティ AppFabric を確保できます。

AWS Management Console

AWS Management Console は、 リソースの作成と管理 AWS に使用できるブラウザベースのインターフェイスです。 AppFabric コンソールでは、 AppFabric リソースにアクセスできます。コンソール AppFabricを使用して、すべての AppFabric リソースを作成および管理できます。

AppFabric API

AppFabric プログラムで にアクセスするには、 AppFabric API を使用し、HTTPS リクエストを サービスに直接発行します。詳細については、AWS AppFabric 「 API リファレンス」を参照してください。

AWS Command Line Interface (AWS CLI)

を使用すると AWS CLI、システムのコマンドラインでコマンドを発行して、 やその他の と AppFabricやり取りできます AWS サービス。コマンドラインツールは、タスクを実行するスクリプトを作成する場合にも便利です。のインストールと使用の詳細については AWS CLI、「 AWS Command Line Interface バージョン 2 のユーザーガイド」を参照してください。の AWS CLI コマンドの詳細については AppFabric、「 AppFabric リファレンス」の AWS CLI 「」セクションを参照してください。

関連サービス

セキュリティ AppFabric のため、 AWS サービス で以下を使用できます。

Amazon Data Firehose

Amazon Data Firehose は、データレイク、データストア、分析サービスにストリーミングデータを確実にキャプチャ、変換、配信する抽出、変換、ロード (ETL) サービスです。を使用する場合 AppFabric、Open Cybersecurity Schema Framework (OCSF) の正規化された監査ログまたは raw 監査ログを JSON 形式で Firehose ストリームに送信先として出力することを選択できます。詳細については、「Firehose で出力場所を作成する」を参照してください。

Amazon Security Lake

Amazon Security Lake は、 AWS 環境、SaaS プロバイダー、オンプレミス、クラウドソースのセキュリティデータを、アカウントに保存されている専用のデータレイクに自動的に一元化します。AppFabric 監査ログデータを Security Lake と統合するには、Amazon Data Firehose を送信先として選択し、Security Lake で正しい形式とパスでデータを配信するように Firehose を設定します。詳細については、「Amazon Security Lake ユーザーガイド 」の「カスタムソースからのデータ収集」を参照してください。

Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) は、業界をリードするスケーラビリティ、データ可用性、セキュリティ、およびパフォーマンスを提供するオブジェクトストレージサービスです。を使用する場合 AppFabric、OCSF 正規化 (JSON または Apache Parquet) または raw (JSON) 監査ログを

送信先として新規または既存の Amazon S3 バケットに出力することを選択できます。詳細については、「Amazon S3 の出力場所の作成」を参照してください。

Amazon QuickSight

Amazon は、統合ビジネスインテリジェンス (BI) をハイパースケールで活用して、データ主導型の組織 QuickSight を強化します。を使用すると QuickSight、最新のインタラクティブダッシュボード、ページ分割レポート、埋め込み分析、自然言語クエリを通じて、すべてのユーザーが同じ信頼できるソースからさまざまな分析ニーズを満たすことができます。ログがソースとして保存されている Amazon S3 バケットを選択することで QuickSight、 で AppFabric 監査 AppFabric ログデータを分析できます。詳細については、Amazon S3 ファイルを使用したデータセットの作成 QuickSight 」を参照してください。Amazon S3 の AppFabric データを Amazon Athena にインポートし、Amazon Athena を のデータソースとして選択することもできます QuickSight。詳細については、Amazon Athena データを使用したデータセットの作成」を参照してください。 QuickSight

AWS Key Management Service

AWS Key Management Service （ AWS KMS) を使用すると、アプリケーションと 全体で暗号化キーを作成、管理、制御できます AWS サービス。でアプリケーションバンドルを作成するときは AppFabric、承認されたアプリケーションデータを安全に保護するための暗号化キーを設定します。このキーは、 AppFabric サービス内のデータを暗号化します。 AppFabric は AppFabric 、ユーザーに代わって によって AWS 所有のキー 作成および管理される 、または で作成および管理されるカスタマーマネージドキーを使用できます AWS KMS。詳細については、「キーの作成 AWS KMS」を参照してください。

オープンサイバーセキュリティスキーマフレームワーク

Open Cybersecurity Schema Framework (OCSF) は、サイバーセキュリティ業界における AWS および主要なパートナーによる、共同のオープンソースの取り組みです。OCSF は、一般的なセキュリティイベントの標準スキーマを提供し、スキーマの進化を容易にするバージョン管理基準を定義し、セキュリティログの作成者と利用者を対象とした自己管理プロセスを組み込んでいます。OCSF のパブリックソースコードは でホストされますGitHub。

の OCSF ベースのスキーマ AppFabric

AWS AppFabric for security OCSF 1.0.0-rc.3 ベースのスキーマは、正規化、 一貫性、 Software as a Service (SaaS) ポートフォリオのローエフォートオブザーバビリティ AppFabric。 OCSF オープンソースコミュニティと協力して、 は新しい OCSF イベントカテゴリを導入しました。 イベントクラス、 アクティビティ、 および オブジェクトは、OCSF が SaaS アプリケーションイベント

に適用できるように、 は SaaS アプリケーションから受信した監査イベント AppFabric を自動的に正規化し、このデータを の Amazon Simple Storage Service (Amazon S3) または Amazon Data Firehose サービスに配信します AWS アカウント。Amazon S3 の送信先では、2 つの正規化オプション (OCSF または Raw) と 2 つのデータ形式オプション (JSON またはParquet) を選択できます。Firehose に配信する場合、2 つの正規化オプション (OCSF または Raw) から選択することもできますが、データ形式は JSON に制限されます。

OCSF のイベントカテゴリとクラス

AppFabric は、次の 2 つの OCSF イベントカテゴリを使用します。

- Identity and Access Management – セキュリティ AppFabric では、このカテゴリ内で次のイベントクラスを使用します。
  - アカウント変更
  - 認証
  - ユーザー アクセス管理
  - グループ管理
- アプリケーションアクティビティ — セキュリティ AppFabric では、このカテゴリ内で次のイベントクラスを使用します。
  - Web リソースアクティビティ
  - Web リソースアクセスアクティビティ

前提条件と推奨事項

初めて AWS のお客様は、セキュリティ AWS AppFabric のために の使用を開始する前に、このページに記載されているセットアップの前提条件を完了してください。セットアップ手順には、 AWS Identity and Access Management (IAM) サービスを使用します。IAM の詳細については、「IAM ユーザーガイド」を参照してください。

トピック

- にサインアップする AWS アカウント
- 管理アクセスを持つユーザーを作成する
- (必須) アプリケーションの前提条件を完了させてください
- (オプション) 出力場所を作成します
- (オプション) AWS KMS キーを作成する

にサインアップする AWS アカウント

がない場合は AWS アカウント、次のステップを実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS サービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の アカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」の AWS アカウント 「ルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。

2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 ユーザーガイド」の「デフォルト でユーザーアクセスを設定する IAM アイデンティティセンターディレクトリAWS IAM Identity Center 」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、「 AWS サインインユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの参加」を参照してください。

(必須) アプリケーションの前提条件を完了させてください

セキュリティ AppFabric のために を使用してアプリケーションからユーザー情報と監査ログを受信するには、多くのアプリケーションに特定のロールと計画タイプが必要です。 AppFabric セキュリティのために で承認する各アプリケーションの前提条件を確認し、適切な計画とロールがあること

を確認します。アプリケーション別の前提条件の詳細については、「サポートされているアプリケーション」を参照するか、以下のアプリケーション別のトピックのいずれかを選択してください。

- 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
- Microsoft 365
- Miro
- Okta
- OneLogin by One Identity
- PagerDuty
- Ping Identity
- Salesforce
- ServiceNow
- Singularity Cloud
- Slack
- Smartsheet
- Terraform Cloud

- Webex by Cisco
- Zendesk
- Zoom

(オプション) 出力場所を作成します

AppFabric for security は、監査ログの取り込み先として Amazon Simple Storage Service (Amazon S3) と Amazon Data Firehose をサポートしています。

Amazon S3

取り込み先を作成するときに、 AppFabric コンソールを使用して新しい Amazon S3 バケットを作成できます。また、Amazon S3 サービスを使用してバケットを作成することもできます。Amazon S3 サービスを使用してバケットを作成する場合は、 AppFabric 取り込み先を作成する前にバケットを作成し、取り込み先を作成するときにバケットを選択する必要があります。既存のバケットの次の要件を満たしている限り AWS アカウント、 で既存の Amazon S3 バケットを使用することを選択できます。

- AppFabric セキュリティ上の理由から、Amazon S3 バケットは Amazon S3 リソースと同じ AWS リージョン にある必要があります。
- は、次のいずれかを使用してバケットを暗号化できます。
  - Amazon S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)
  - デフォルト AWS Key Management Service （ AWS KMS) を使用した () キー (SSE-KMS) によるサーバー側の暗号化 AWS マネージドキー `aws/s3`。

Amazon Data Firehose

セキュリティデータの の取り込み先として Amazon Data Firehose AppFabric を使用することを選択できます。Firehose を使用するには、取り込みを作成する AWS アカウント 前、または で取り込み先を作成するときに、 に Firehose 配信ストリームを作成できます AppFabric。Firehose 配信ストリームは、 AWS Management Console、 AWS CLI、または AWS APIs または SDKsを使用して作成できます。ストリーム設定の手順については、以下のトピックを参照してください。

- AWS Management Console 手順 — Amazon Data Firehose デベロッパーガイドの「Amazon Data Firehose 配信ストリームの作成」
- AWS CLI instructions – AWS CLI コマンドリファレンスcreate-delivery-streamの
- AWS APIsと SDKsCreateDeliveryStream「」

セキュリティ出力の送信 AppFabric 先として Amazon Data Firehose を使用する場合の要件は次のとおりです。

- セキュリティリソース AppFabric の AWS リージョン と同じ にストリームを作成する必要があります。
- ソースとして [ダイレクト PUT] を選択する必要があります。
- AmazonKinesisFirehoseFullAccess AWS 管理ポリシーをユーザーにアタッチするか、次のアクセス許可をユーザーにアタッチします。

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

Firehose は、 Splunkや などのさまざまなサードパーティーのセキュリティツールとの統合をサポートしていますLogz.io。これらのツールにデータを出力するように Amazon Kinesis を適切に設定する方法については、「Amazon Data Firehose デベロッパーガイド」の「送信先設定」を参照してください。

(オプション) AWS KMS キーを作成する

セキュリティアプリケーションバンドル AppFabric 用の を作成するプロセスでは、暗号化キーを選択または設定して、承認されたすべてのアプリケーションからデータを安全に保護します。このキーは、 AppFabric サービス内のデータを暗号化するために使用されます。

AppFabric for security は、デフォルトでデータを暗号化します。 AppFabric for security は、 AWS 所有のキー AppFabric ユーザーに代わって によって作成および管理される 、または AWS Key Management Service () で作成および管理されるカスタマーマネージドキーを使用できますAWS KMS。 AWS 所有のキー は、 が AWS サービス 所有および管理する AWS KMS キーのコレクションであり、複数の で使用できます AWS アカウント。カスタマーマネージドキーは、ユーザーが作成、所有、管理する の AWS KMS キー AWS アカウント です。 AWS 所有のキー およびカスタマーマネージドキーの詳細については、「 AWS Key Management Service デベロッパーガイド」の「カスタマーキーと AWS キー」を参照してください。

カスタマーマネージドキーを使用して、セキュリティ AppFabric のために 内の認証トークンなどのデータを暗号化する場合は、 で作成できますAWS KMS。でカスタマーマネージドキーへのアクセスを許可するアクセス許可ポリシーの詳細については AWS KMS、このガイドの「キーポリシー」セクションを参照してください。

セキュリティ AWS AppFabric のための の開始方法

セキュリティ AWS AppFabric のために の使用を開始するには、まずアプリケーションバンドルを作成し、次にアプリケーションを認可してアプリケーションバンドルに接続する必要があります。アプリケーション認証がアプリケーションに接続されたら、監査ログの取り込みやユーザーアクセスなどのセキュリティ機能 AppFabric に を使用できます。

このセクションでは、 AppFabric で の使用を開始する方法について説明します AWS Management Console。

トピック

- 前提条件
- ステップ 1: アプリケーションバンドルを作成する
- ステップ 2: アプリケーションを認証する
- ステップ 3: 監査ログの取り込みの設定
- ステップ 4: ユーザーアクセスツールを使用する
- ステップ 5: セキュリティツールやその他の送信先のセキュリティデータ AppFabric に接続する

前提条件

開始する前に、まず AWS アカウント と管理ユーザーを作成する必要があります。詳細については、「にサインアップする AWS アカウント」および「管理アクセスを持つユーザーを作成する」を参照してください。

ステップ 1: アプリケーションバンドルを作成する

アプリケーションバンドルは、セキュリティアプリケーションの認証と取り込み AppFabric のためにすべての を保存します。アプリバンドルを作成するには、認証されたアプリケーションデータを安全に保護するための暗号化キーを設定します。

1. https://console.aws.amazon.com/appfabric/ で AppFabric コンソールを開きます。

2. ページの右上隅にあるリージョンの選択セレクターで、米国東部 (バージニア北部) 、欧州 (アイルランド) 、アジアパシフィック (東京) リージョンでのみ利用可能な AWS リージョン AppFabric を選択します。
3. [開始方法] を選択します。
4. 「開始方法」ページのステップ 1 を行います。「アプリバンドルの作成」で [アプリバンドルの作成] を選択します。
5. 「暗号化」セクションで、認証されたすべてのアプリケーションからのデータを安全に保護するための暗号化キーを設定します。このキーは、セキュリティサービスのために 内の AppFabric データを暗号化するために使用されます。

   AppFabric for security は、デフォルトでデータを暗号化します。 AppFabric は AppFabric 、ユーザーに代わって によって AWS 所有のキー 作成および管理される 、または () で AWS Key Management Service 作成および管理されるカスタマーマネージドキーを使用できますAWS KMS。
6. 「AWS KMS キー」には、「使用 AWS 所有のキー」または「カスタマーマネージドキー」を選択します。

   カスタマーマネージドキーを選んで使用する場合は、Amazon リソースネーム (ARN) または使用したい既存のキーのキー ID のいずれかを入力するか、あるいは [AWS KMS キーの作成] を選択します。

   AWS 所有のキー またはカスタマーマネージドキーを選択するときは、次の点を考慮してください。

   - AWS 所有のキー は、 が複数の で使用するために AWS サービス 所有および管理する AWS Key Management Service （ AWS KMS) キーのコレクションです AWS アカウント。 AWS 所有のキー は にはありませんが AWS アカウント、 AWS サービス は AWS 所有のキー を使用してアカウントのリソースを保護できます。 AWS 所有のキー アカウントのクォータには AWS KMS カウントされません。キーまたはそのキーポリシーを作成または管理する必要はありません。のローテーションはサービス AWS 所有のキー によって異なります。 AWS 所有のキー の のローテーションの詳細については AppFabric、「保管時の暗号化」を参照してください。
   - カスタマーマネージドキーは、ユーザーが作成、所有、管理する の KMS キー AWS アカウント です。これらの AWS KMS キーは完全に制御できます。キーポリシー、 AWS Identity and Access Management (IAM) ポリシー、グラントを確立し維持することができます。これらを有効または無効にしたり、暗号化マテリアルをローテーションしたり、タグを追加したり、AWS KMS キーを参照するエイリアスを作成したり、 AWS KMS キーの削除をスケジュー

ルしたりできます。カスタマーマネージドキーは、 AWS Management Console の のカスタマーマネージドキーページに表示されます AWS KMS。

カスタマーマネージドキーを明確に識別するには、`DescribeKey` オペレーションを使用します。カスタマーマネージドキーでは、`DescribeKey` レスポンスの `KeyManager` フィールドの値は `CUSTOMER` です。暗号化オペレーションではカスタマーマネージドキーを使用し、AWS CloudTrail ログでは使用状況を監査できます。と統合 AWS サービス されている多くのでは AWS KMS、カスタマーマネージドキーを指定して、保存および管理されるデータを保護できます。カスタマーマネージドキーには、 AWS 無料利用枠を超える月額料金と使用料が発生します。カスタマーマネージドキーは、アカウントの AWS KMS クォータに対してカウントされます。

AWS 所有のキー およびカスタマーマネージドキーの詳細については、「 AWS Key Management Service デベロッパーガイド」の「カスタマーキーと AWS キー」を参照してください。

> **Note**
>
> アプリケーションバンドルが作成されると、セキュリティ AppFabric 上の理由から、 のサービスにリンクされたロール (SLR) AWS アカウント と呼ばれる特別な IAM ロールも に作成されます AppFabric。これにより、サービスは Amazon にメトリクスを送信できます CloudWatch。監査ログの送信先を追加すると、SLR は AWS リソース (Amazon S3 バケット、Amazon Data Firehose 配信ストリーム) へのセキュリティサービスアクセス AppFabric を に許可します。詳細については、「 AppFabric のサービスにリンクされたロールの使用」を参照してください。

7. (オプション) [タグ] で、アプリバンドルにタグを追加することができます。タグは、作成したリソースにメタデータを割り当てるキーと値のペアです。詳細については、「タグエディタユーザーガイド」の AWS「リソースのタグ付け」を参照してください。 AWS
8. アプリバンドルを作成するには、「アプリバンドルの作成」を選択します。

ステップ 2: アプリケーションを認証する

アプリケーションバンドルが正常に作成されたら、セキュリティ AppFabric が各アプリケーションに接続して操作することを承認できるようになりました。認証されたアプリケーションは暗号化され、アプリバンドルに保存されます。アプリバンドルごとに複数のアプリ認証を設定するには、アプリケーションごとに必要に応じてアプリ認証手順を繰り返します。

アプリケーションを認証する手順を開始する前に、サポートされているアプリケーションで各アプリケーションの前提条件（必要なプランタイプなど）をよく確認してください。

1. 「開始方法」ページのステップ 2 を行います。アプリケーションの認証で、[アプリ認証の作成] を選択します。
2. アプリケーション認証セクションで、アプリケーションドロップダウンから、セキュリティ AppFabric が に接続するためのアクセス許可を付与するアプリケーションを選択します。表示されるアプリケーションは、セキュリティ AppFabric のために で現在サポートされているアプリケーションです。
3. アプリケーションを選択すると、必須の情報フィールドが表示されます。これらのフィールドには、テナント ID とテナント名のほか、クライアント ID、クライアントシークレット、または個人アクセストークンが含まれる場合があります。これらのフィールドの入力値はアプリケーションによって異なります。これらの値の検索方法に関するアプリケーション別の詳細な手順については、「サポートされているアプリケーション」を参照してください。
4. (オプション) [タグ] で、アプリ認証にタグを追加することができます。タグは、作成したリソースにメタデータを割り当てるキーと値のペアです。詳細については、「タグエディタユーザーガイド」の AWS「リソースのタグ付け」を参照してください。 AWS
5. [アプリ認証の作成] を選択します。
6. ポップアップウィンドウが表示された場合 (接続されているアプリケーションに応じて）、「セキュリティがアプリケーションに接続することを許可する AppFabric 」を選択します。

   アプリ認証が成功すると、「開始方法」ページに「アプリ認証が接続されました」という成功メッセージが表示されます。
7. アプリ認証のステータスは、ナビゲーションペインに表示される「アプリ認証」ページの [各アプリケーションのステータス] でいつでも確認できます。接続ステータスは、アプリケーションに接続するためのセキュリティ AppFabric のためにアプリケーション認証が付与され、完了していることを意味します。
8. 関連するエラーを修正するために実行できるトラブルシューティング手順を含め、考えられるアプリ認証ステータスを以下の表に示します。

ステータス名	ステータス情報	トラブルシューティングのステップ
[保留中]	ステータスが Pending の場合、アプリケーションのアプリケーション認証が作成	このステータスが表示されたら、「アプリ認証」ページの [アクション] ドロップダウン

ステータス名	ステータス情報	トラブルシューティングのステップ
	されますが、セキュリティ AppFabric 上の はまだアプリケーションに接続されていません。	で [接続] を選択して接続を開始します。このエラーが解決されない場合は、ブラウザのポップアップブロッカーが無効になっていないか確認してください。ポップアップウィンドウに「400 不良なリクエスト」などのエラーメッセージが表示される場合は、テナント ID、クライアント ID、クライアントシークレットなどのすべての情報が正しく入力されていることを確認してください。また、アプリケーションのアプリ認証が正しく作成されていない可能性もあります。詳細については、「サポートされるアプリケーション」を参照してください。
接続が検証できませんでした	接続検証に失敗したステータスは、セキュリティ AppFabric 上の がアプリケーションとのアプリケーション認証の接続を検証できないことを意味します。	テナント ID、クライアント ID、クライアントシークレットなどのすべての情報がアプリ認証用に正しく入力されていることを確認してください。
トークンの自動ローテーションに失敗しました	「トークンの自動ローテーションに失敗しました」のステータスは、アプリ認証が正常に接続された後に OAuth 更新トークンが失敗したことを意味します。	このエラーが解決されない場合は、アプリケーションの認証アプリを確認してください。詳細については、「サポートされるアプリケーション」を参照してください。

9. 他のアプリケーションを認証するには、必要に応じてステップ 1 ~ 8 を繰り返します。

ステップ 3: 監査ログの取り込みの設定

アプリバンドルで少なくとも 1 つのアプリ認証を作成したら、監査ログの取り込みを設定できるようになります。監査ログの取り込みにより、認証アプリからの監査ログが消費され、オープンサイバーセキュリティスキーマフレームワーク (OCSF) に標準化されます。次に、それらは AWS内の1つまたは複数の転送先に配信されます。Raw JSON ファイルを転送先に配信することもできます。

1. 「開始方法」ページのステップ 3 を行います。「監査ログ取り込みの設定」セクションで、[取り込みの Quick Setup] を選択します。

> **Note**
>
> セットアップを迅速に行うには、「開始方法」ページからのみアクセスできる 「取り込みの Quick Setup」ページを使用して、同じ転送先に対する複数のアプリ認証の取り込みを一度に作成します。例えば、同じ Amazon S3 バケットまたは Amazon Data Firehose データストリームなどです。
> ナビゲーションペインからアクセスできる「取り込み」ページから取り込みを作成することもできます。「取り込み」ページでは、異なる転送先への取り込みを一度に 1 つずつ設定できます。「取り込み」ページでは、取り込みのタグを作成することもできます。以下の説明は、「取り込み Quick Setup」ページ用です。

2. 「アプリ認証の選択」で、監査ログの取り込みを作成したいアプリ認証を選択します。アプリ認証ドロップダウンに表示されるテナント名は、セキュリティ AppFabric のために でアプリ認証を以前に作成したアプリケーションのテナント名です。
3. 「転送先の追加」では、選択したアプリケーションの監査ログの取り込み先を選択します。送信先オプションには、Amazon S3 - 既存のバケット、Amazon S3 - 新しいバケット、または Amazon Data Firehose が含まれます。複数のテナント名を選択した場合、選択した転送先がアプリケーション認証の取り込みのたびに適用されます。
4. 転送先を選択すると、追加の必須フィールドが表示されます。
   a. [Amazon S3 — 新規バケット] を転送先として選択した場合は、作成したい S3 バケットの名前を入力する必要があります。Amazon S3 バケットの作成に関する詳しい手順については、「出力先の作成」を参照してください。
   b. [Amazon S3 — 既存のバケット] を送信先として選択した場合は、使用したい Amazon S3 バケットの名前を選択します。

c. 送信先として Amazon Data Firehose を選択した場合は、Firehose 配信ストリーム名のドロップダウンリストから配信ストリームの名前を選択します。Amazon Data Firehose 配信ストリームを作成する方法の詳細については、「出力先 を作成する」および「セキュリティのために に必要なアクセス許可ポリシー AppFabric 」を参照してください。

5. Schema & Format では、監査ログを Raw - JSON 、OCSF - JSON 、OCSF - Amazon S3 バケットParquetの場合は 、Raw - JSON または Firehose の場合は OCSF-JSON に保存することを選択できます。

   Raw データ形式では、監査ログデータがデータ文字列から JSON に変換されます。OCSF データ形式は、セキュリティオープンサイバーセキュリティスキーマフレームワーク (OCSF) スキーマ AppFabric の監査ログデータを に正規化します。が OCSF AppFabric を使用する方法の詳細については、「」を参照してくださいオープンサイバーセキュリティスキーマフレームワーク。一度に取り込むことができるスキーマと形式のデータタイプは 1 つだけです。スキーマと形式のデータタイプを追加する場合は、取り込み作成プロセスを繰り返すことで追加の取り込み先を設定できます。

6. (オプション) 取り込みにタグを追加する場合は、ナビゲーションペインの「取り込み」 ページに移動します。「取り込みの詳細」ページに移動するには、テナント名を選択します。[タグ] で、取り込みにタグを追加することができます。タグは、作成したリソースにメタデータを割り当てるキーと値のペアです。詳細については、「タグエディタユーザーガイド」の AWS「リソースのタグ付け」を参照してください。 AWS

7. [取り込みの設定] を選択します。

   取り込みの設定が正常に完了すると、「開始方法」ページに「取り込みが作成されました」という成功メッセージが表示されます。

8. また、ナビゲーションペインの「取り込み」ページで、取り込みの状態と取り込み先のステータスをいつでも確認できます。このページでは、アプリ認証の作成時に作成されたテナント名、転送先、および取り込みの状態を確認することができます。取り込みの状態が [有効] の場合は、取り込みが有効になっていることを意味します。このページでアプリ認証のテナント名を選択すると、転送先の詳細やステータスなど、そのアプリ認証の詳細ページが表示されます。取り込み先のステータスが [有効] の場合は、その取り込み先が適切に設定され、有効になっていることを意味します。アプリ認証のステータスが [接続済み] で、取り込み先のステータスが [有効] の場合は、監査ログは処理および配信されているはずです。アプリ認証ステータスまたは取り込み先ステータスがいずれかの「失敗」状態である場合、取り込みステータスが有効になっていても監査ログは処理も配信もされません。アプリ認証の失敗を修正するには、ステップ 2 を参照してください。アプリケーションを認証する。

9. エラーステータスを修正するために実行できるトラブルシューティング手順を含め、考えられる取り込み先と取り込み先ステータスを以下の表に示します。

状態またはステータス名	説明	トラブルシューティングのステップ
[Disabled] (無効)	取り込みが [無効] の状態になっている場合、取り込みは無効になっています。	取り込みを有効にするには、「取り込み」ページの [アクション] ドロップダウンから [有効にする] を選択します。
[失敗]	取り込み先が [失敗] の状態になっている場合、取り込み先が監査ログを受け付けていないことを意味します。たとえば、保存場所がいっぱいのためにこの状態になることがあります。	これらの問題を解決するには、Amazon S3 または Firehose コンソールに移動します。

ステップ 4: ユーザーアクセスツールを使用する

セキュリティユーザーアクセスツール AppFabric の を使用すると、セキュリティチームと IT 管理者チームは、従業員の会社の E メールアドレスを使用して簡単な検索を実行することで、特定のアプリケーションにアクセスできるユーザーをすばやく確認できます。このアプローチは、ユーザーのプロビジョニング解除など、SaaS アプリケーション全体にわたるユーザーアクセスを手動で確認または監査する必要があるタスクに費やす時間を削減するのに役立ちます。ユーザーが見つかった場合、セキュリティ AppFabric 上、アプリケーション内のユーザー名と、アプリケーションから提供された場合はアプリケーション内のユーザーステータス (アクティブなど) を指定します。セキュリティ AppFabric 上、 はアプリケーションバンドル内のすべての承認されたアプリケーションを検索して、ユーザーがアクセスできるアプリケーションのリストを返します。

1. 「開始方法」ページのステップ 4 を行います。ユーザーアクセスツールを使用して、[ユーザーの検索] を選択します。
2. [メールアドレス] フィールドに、ユーザーのメールアドレスを入力し、[検索] を選択します。

3. 「検索結果」セクションには、ユーザーがアクセスできるすべての認証済みアプリケーションのリストが表示されます。アプリケーション内のユーザー名とステータス (可能な場合) を表示するには、検索結果を選択します。
4. 検索結果列に「ユーザーが見つかりました」というメッセージが表示されている場合は、そのユーザーはリストに表示されているアプリにアクセスできることを意味します。考えられる検索結果、エラー、およびエラーに対処するために実行できるアクションを以下の表で示します。

検索結果	説明
ユーザーが見つかりません	使用されたメールアドレスを持つユーザーが見つかりません。
認証トークンが見つかりません。アプリケーションのアプリ認証に接続します。	テナント ID、クライアント ID、クライアントシークレットなどのすべての情報がアプリ認証用に正しく入力されていることを確認してください。
認証トークンは取り消されました。アプリケーションのアプリ認証に接続します。	テナント ID、クライアント ID、クライアントシークレットなどのすべての情報がアプリ認証用に正しく入力されていることを確認してください。
認証トークンをローテーションできませんでした。アプリケーションのアプリ認証に接続します。	アプリ認証が正常に接続された後、OAuth 更新トークンは失敗しました。このエラーが解決されない場合は、アプリケーションの認証アプリを確認してください。詳細については、「サポートされるアプリケーション」を参照してください。
必要な許可が見つかりません。アプリケーションのアプリ認証に接続します。	テナント ID、クライアント ID、クライアントシークレットなどのすべての情報がアプリ認証用に正しく入力されていることを確認してください。
アプリ認証が無効です。	テナント ID、クライアント ID、クライアントシークレットなどのすべての情報がアプリ

検索結果	説明
	認証用に正しく入力されていることを確認してください。
アクセス許可が不十分なため、アプリケーション API を呼び出すことができませんでした。	テナント ID、クライアント ID、クライアントシークレットなどのすべての情報がアプリ認証用に正しく入力されていることを確認してください。
アプリケーションリクエスト制限を超えました。	これはアプリケーションから受け取ったエラーメッセージです。後でもう一度メールアドレスを検索してください。
アプリケーションに内部サーバーエラーが発生しました	これはアプリケーションから受け取ったエラーメッセージです。後でもう一度メールアドレスを検索してください。
アプリケーションに不正なゲートウェイエラーが発生しました	これはアプリケーションから受け取ったエラーメッセージです。後でもう一度メールアドレスを検索してください。
アプリケーションはリクエストを処理する準備ができていません	これはアプリケーションから受け取ったエラーメッセージです。後でもう一度メールアドレスを検索してください。
アプリケーションに不正なリクエストエラーが発生しました。	これはアプリケーションから受け取ったエラーメッセージです。後でもう一度メールを検索してください。
アプリケーションでサービス使用不可エラーが発生しました。	これはアプリケーションから受け取ったエラーメッセージです。後でもう一度メールを検索してください。

ステップ 5: セキュリティツールやその他の送信先のセキュリティデータ AppFabric に接続する

からの正規化された (または raw) アプリケーションデータは AppFabric 、、、、、、Dynatrace、Barracuda XDR、 などのセキュリティツール Splunkや独自のセキュリティソリューションなど、Amazon S3 からのデータ取り込み Logz.ioNetskopeNetWitnessRapid7と Firehose との統合をサポートするすべてのツールと互換性があります。から正規化 (または raw) されたアプリケーションデータを取得するには AppFabric、前のステップ 1 ~ 3 に従います。特定のセキュリティツールやサービスの設定方法の詳細については、「互換性のあるセキュリティツールとサービス」を参照してください。

サポートされているアプリケーション

AWS AppFabric for security は、以下のアプリケーションとの統合をサポートしています。アプリケーションの名前を選択すると、セキュリティ AppFabric が接続するように を設定する方法の詳細が表示されます。

トピック

- 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
- Microsoft 365

- Miro
- Okta
- OneLogin by One Identity
- PagerDuty
- Ping Identity
- Salesforce
- ServiceNow
- Singularity Cloud
- Slack
- Smartsheet
- Terraform Cloud
- Webex by Cisco
- Zendesk
- Zoom

1Password

1Password は、すべてのオンラインアカウントで強力なパスワードを作成、保存、使用するのに役立つパスワードマネージャーです。また、暗号化によってデータを保護し、違反について警告し、パスワードを共有することもできます。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信し 1Password、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート 1Password
- 1Password アカウント AppFabric への接続

AppFabric のサポート 1Password

AppFabric は、 からのユーザー情報と監査ログの受信をサポートします1Password。

前提条件

AppFabric を使用して からサポートされている宛先1Passwordに監査ログを転送するには、次の要件を満たす必要があります。

- 有効な有料 1Password Business または Enterprise サブスクリプションプランが必要です。詳細については、 1Passwordウェブサイトの1Password「エンタープライズ」を参照してください。
- 1Password アカウントには管理者ロールまたはチーム所有者が必要です。詳細については、1Passwordサポートウェブサイトの「グループ」を参照してください。

レート制限に関する考慮事項

1Password AuditLog Events API は、リクエストを 1 分あたり 600 件、1 時間あたり最大 30,000 件に制限します。これらの制限を超えると、エラーが返されます。詳細については、「 Events 1Password API リファレンス」の「API レート制限」を参照してください。 1Password

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

1Password アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要があります1Password。1Password で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

個人用1Passwordアクセストークンを作成する

1Password は、パブリッククライアントの個人用アクセストークンをサポートします。個人用アクセストークンを生成するには、次のステップを実行します。

1. 1Password アカウントにサインインします。
2. ナビゲーションペインで統合を選択します。
3. 既存の統合が存在する場合は、ディレクトリ を選択します。それ以外の場合は、次の手順に進んでください。

4. 「イベントレポート統合」で「その他」を選択します。
5. 統合の追加ページで、セキュリティ情報とイベント管理 (SIEM) システム名 (Secure など) を入力します。 AppFabric
6. 統合の追加 を選択し、トークンの設定 ページで次のステップを実行します。
   a. AppFabric セキュア環境で使用するトークン名を指定します。
   b. 「有効期限後」ドロップダウンリストで「Never」を選択することをお勧めします。 他の値を選択した場合、 は有効期限が経過した後にトークンを1Password取り消します。
   c. レポートするイベント セクションで、サインイン試行 、アイテム使用状況イベント 、監査イベント を選択します。
7. トークンを発行を選択してトークンを作成します。
8. 保存 1Passwordを選択し、次のステップを完了します。
   a. タイトルは、システムとトークン名に基づいて自動的に入力されます。
   b. ボールトの選択でプライベート を選択します。
   c. [保存] を選択します。

詳細については、 1Passwordウェブサイトの1Password「イベントレポートの開始方法」を参照してください。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID は1Passwordサインインアドレス AppFabric になります。テナント ID を検索するには、次のステップを実行します。

1. 1Password アカウントにサインインします。
2. ナビゲーションペインで [設定] を選択します。
3. 1Password サインインがページに表示されます。例えば、example-account.1password.com などです。

テナント名

この一意の1Password組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

サービスアカウントトークン

アプリ認証に入力 AppFabric 1Passwordするには、 サービスアカウントの1Passwordサービスアカウントトークンが必要です。サービスアカウントトークンをお持ちでない場合は、次に説明する手順に従ってください。

AppFabric はサービスアカウントトークンをリクエストします。のサービスアカウントトークン AppFabricは、作成した個人用アクセストークンです。1Password ポータルで次の手順を実行して、個人用アクセストークンを見つけます。

1. Dashboard を選択します。
2. People を選択します。
3. アカウント所有者名 を選択します。
4. [Private] (プライベート) を選択します。
5. ボールトの表示 を選択します。
6. トークン名 を選択します。

クライアント認証

テナント ID、テナント名、サービスアカウントトークン AppFabric を使用して、 でアプリケーション認証を作成します。次に、接続を選択して認証をアクティブ化します。

Asana

Asana は、日常業務から部門横断的な戦略的イニシアチブに至るまで、個人、チーム、組織が仕事を調整できるよう支援する業務管理プラットフォームです。誰もがコミュニケーション、コラボレーション、仕事の調整を行える、生き生きとしたわかりやすいシステムを提供します。Asana を使うと、チームは重要なビジネスツールを 1 か所に統合できるため、どこにいても仕事を進めることができます。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しAsana、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Asana
- Asana アカウント AppFabric への接続

AppFabric のサポート Asana

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますAsana。

前提条件

AppFabric を使用して からサポートされている宛先Asanaに監査ログを転送するには、次の要件を満たす必要があります。

- Asana の エンタープライズアカウントが必要です。Asana エンタープライズアカウントの作成またはアップグレードに関する詳細については、Asana ウェブサイトの「Asanaエンタープライズ」を参照してください。
- Asana アカウントにはスーパー管理者ロールを持つユーザーが必要です。ロールの詳細については、Asana ウェブサイトの「Asanaの管理者およびスーパー管理者」ロールを参照してください。

レート制限に関する考慮事項

Asana は、Asana API にレート制限を課します。AsanaAPI のレート制限の詳細については、「Asanaデベロッパーガイド」ウェブサイトの「レート制限」を参照してください。と既存の Asanaアプリケーションの組み合わせが制限を超える AppFabric と、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Asana アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますAsana。Asana で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric は、 のドメイン ID と呼ばれますAsana。ドメイン ID を見つけるには、Asana ホーム画面で以下の指示に従ってください。

1. アカウントのプロフィール画像を選択し、[管理コンソール] を選択します。
2. [設定] を選択します。
3. [ドメイン設定] までスクロールします。
4. このセクションのドメイン ID を AppFabric テナント ID 設定に入力します。

テナント名

この一意の Asana 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

サービスアカウントトークン

アプリ認証に入力 AppFabric Asanaするには、 サービスアカウントのAsanaサービスアカウントトークンが必要です。サービスアカウントトークンをお持ちでない場合は、次に説明する手順に従ってください。

1. サービスアカウントを作成するには、「Asanaガイド」ウェブサイトの「サービスアカウント」の指示に従います。
2. 「サービスアカウントの追加」ページが初めて表示されたときに、「サービスアカウントの追加」ページの下部にあるトークンをコピーして保存します。
3. トークンを保存する前に 「サービスアカウントの追加」ページを閉じた場合は、サービスアカウントを編集し、新しいトークンを生成して保存する必要があります。

Azure Monitor

Azure Monitor は、クラウドおよびオンプレミス環境からモニタリングデータを収集、分析、対応するための包括的なモニタリングソリューションです。を使用するとAzure Monitor、アプリケーションとサービスの可用性とパフォーマンスを最大化できます。これにより、アプリケーションのパフォーマンスを理解し、システムイベントに手動およびプログラムで対応できます。

Azure Monitor は、複数の Azure および Azure 以外のサブスクリプションとテナントにわたって、システムのすべてのレイヤーとコンポーネントからデータを収集および集約します。データに相関、分析、視覚化、および/または応答できる共通のツールセットが使用するために、共通のデータプラットフォームに保存します。他の Microsoft ツールと Microsoft 以外のツールを統合することもできます。Azure Monitor アクティビティログは、サブスクリプションレベルのイベントに関するインサイトを提供するプラットフォームログです。アクティビティログには、リソースが変更されたり、仮想マシンが開始されたりしたときなどの情報が含まれます。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しAzure Monitor、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Azure Monitor
- Azure Monitor アカウント AppFabric への接続

AppFabric のサポート Azure Monitor

AppFabric は、次のAzure Monitorサービスからユーザー情報と監査ログを受信できます。

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

前提条件

AppFabric を使用して からサポートされている宛先Azure Monitorに監査ログを転送するには、次の要件を満たす必要があります。

- 無料トライアルまたは pay-as-you-go サブスクリプションのいずれかのMicrosoft Azureアカウントが必要です。
- そのサブスクリプション内のイベントを取得するには、少なくとも 1 つのサブスクリプションが必要です。

レート制限に関する考慮事項

Azure Monitor は、リクエストを行うセキュリティプリンシパル (ユーザーまたはアプリケーション) とサブスクリプション ID またはテナント ID にレート制限を課します。Azure Monitor API レート制限の詳細については、「 Azure Monitorデベロッパーウェブサイト」の「 がリクエストをどのように Azure Resource Managerスロットリングするかを理解する」を参照してください。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Azure Monitor アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますAzure Monitor。Azure Monitor で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth2 Azure Monitorを使用して と統合します。で OAuth2 アプリケーションを作成するには、次のステップを実行しますAzure Monitor。

1. Microsoft Azure ポータルに移動してサインインします。
2. Microsoft Entra ID に移動します。
3. アプリ登録 を選択します。
4. 新規登録 を選択します。
5. OAuth Azure Monitor クライアントなどのクライアントの名前を入力します。これは登録されたアプリケーションの名前になります。
6. サポートされているアカウントタイプがシングルテナント に設定されていることを確認します。
7. リダイレクト URI には、プラットフォームとして Web を選択し、リダイレクト URI を追加します。リダイレクト URI には次の形式を使用します。

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

   そのアドレス AWS リージョン の `<region>`は、 AppFabric アプリバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://us-east-1.console.aws.amazon.com/appfabric/oauth2` です。

認証レスポンスは、ユーザーの認証に成功すると、指定された URI に送信されます。これを指定することはオプションであり、後で変更できますが、ほとんどの認証シナリオでは値が必要です。

8. [登録] を選択します。
9. 登録済みアプリで、証明書とシークレット を選択し、次に新しいクライアントシークレット を選択します。
10. シークレットの説明を追加します。
11. シークレットの有効期限を選択します。ドロップダウンから任意のプリセット期間を選択するか、カスタム期間を設定できます。
12. 追加を選択します。クライアントシークレット値は、作成直後にのみ表示できます。ページを離れる前に、必ずシークレットを安全な場所に保存してください。

必要なアクセス許可

OAuth アプリケーションには以下のアクセス許可を追加する必要があります。アクセス許可を追加するには、「 Microsoft Entraデベロッパーガイド」の「ウェブ API にアクセスするためのアクセス許可を追加」セクションの指示に従います。

- Microsoft Graph ユーザーアクセス API > User.Read.All (委任タイプを選択)
- Microsoft Graph ユーザーアクセス API > offline_access (委任タイプを選択)
- Azure サービス管理監査ログ API > user_impersonation (委任タイプを選択)

アクセス許可を追加した後、アクセス許可に対する管理者の同意を付与するには、「 Microsoft Entra デベロッパーガイド」の「管理者の同意ボタン」セクションの指示に従います。

アプリ権限

AppFabric は、 Azure Monitorアカウントからのユーザー情報と監査ログの受信をサポートします。から監査ログとユーザーデータの両方を受信するにはAzure Monitor、2 つのアプリケーション認証を作成する必要があります。1 つはアプリケーション認証ドロップダウンリストAzure Monitorで、もう 1 つはアプリケーション認証ドロップダウンリストで Azure Monitor Audit Logs という名前です。両方のアプリ認証には、同じテナント ID、クライアント ID、およびクライアントシークレットを使用できます。から監査ログを受信するには、 Azure Monitorと Azure Monitor Audit Logs アプリ認証の両方Azure Monitorが必要です。ユーザーアクセスツールを単独で使用するには、Azure Monitorアプリ認証のみが必要です。

テナント ID

AppFabric はテナント ID をリクエストします。Azure Monitor でクライアント ID を検索するには、次のステップを実行します。

1. Microsoft Azure ポータル に移動します。
2. Azure Active Directory に移動します。
3. 「アプリ登録」セクションで、以前に作成したアプリを選択します。
4. 概要セクションで、ディレクトリ (テナント) ID フィールドからテナント ID をコピーします。

テナント名

この一意のAzure Monitorサブスクリプションを識別する名前を入力します。 AppFabric は、テナント名を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

> **Note**
> テナント名は、数字、小文字/大文字、およびピリオド (.)、アンダースコア (_)、ダッシュ (-)、空白の特殊文字で構成される最大 2,048 文字にする必要があります。

クライアント ID

AppFabric はクライアント ID をリクエストします。でクライアント ID を検索するには、次の手順を実行しますAzure Monitor。

1. Microsoft Azure ポータル に移動します。
2. Azure Active Directory に移動します。
3. 「アプリ登録」セクションで、以前に作成したアプリを選択します。
4. 概要セクションで、アプリケーション (クライアント) ID フィールドからクライアント ID をコピーします。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。登録された OAuth アプリのクライアントシークレットは、OAuth アプリ作成セクションのステップ 11 で生成したものです。OAuth ア

プリケーションの作成中に生成されたクライアントシークレットを紛失した場合は、OAuth アプリケーション作成セクションのステップ 8 ~ 11 を繰り返して、新しいものを再生成します。

アプリ認証

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されMicrosoft Azure、認証を承認できます。ウィンドウからアカウントにサインインし、許可 を選択して AppFabric 承認を承認します。

Atlassian Confluence

すべての作業を 1 か所で作成、コラボレーション、整理できます。Confluence は、知識とコラボレーションとが融合するチームワークのスペースです。ダイナミックページでは、チームは、あらゆるプロジェクトやアイデアを作成、記録し、コラボレーションすることができます。スペースでは、チームは、作業を構築、整理、共有することができ、チームメンバー全員が組織内の情報を把握したり仕事で最善を尽くすために必要な情報にアクセスしたりできます。セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しConfluence、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Atlassian Confluence
- Atlassian Confluence アカウント AppFabric への接続

AppFabric のサポート Atlassian Confluence

AppFabric は、 からの監査ログの受信をサポートしますAtlassian Confluence。

前提条件

AppFabric を使用して からサポートされている宛先Atlassian Confluenceに監査ログを転送するには、次の要件を満たす必要があります。

- 監査ログにアクセスするには、スタンダード、プレミアム、エンタープライズのいずれかのアカウントが必要です。該当する Confluence プランタイプを作成またはアップグレードする際の詳細については、Atlassian のウェブサイトの「Confluence Pricing」を参照してください。
- 監査ログにアクセスするには、お使いのアカウントの、管理者のアクセス許可が必要になります。ロールの詳細については、Atlassian Support Webサイトの「ユーザーに管理者権限を付与する」を参照してください。

レート制限に関する考慮事項

Confluence は、Atlassian Confluence API にレート制限を課します。 AppFabric と既存の Atlassian Confluence API アプリケーションの組み合わせAtlassian Confluenceが の制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Atlassian Confluence アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますAtlassian Confluence。Atlassian Confluence で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth Atlassian Confluenceを使用して と統合します。Atlassian Confluence で OAuth アプリケーションを作成するには、以下の手順に従います。

1. Atlassian 開発者コンソールに移動します。
2. 右上にあるプロフィールアイコンを選択し、[開発者コンソール] を選択します。
3. [マイアプリ] の横にある [作成]、[OAuth 2.0 統合] を選択します。
4. 左側のナビゲーションペインで [アクセス権限] を選択し、Confluence API の横にある [追加] を選択します。
5. [クラシックスコープ] で、[ユーザーの読み取り] (`read:confluence-user`) を選択します。
6. [詳細スコープ] で [監査記録を表示] (`read:audit-log:confluence`) を選択します。
7. 左側のナビゲーションペインで [承認] を選択し、[OAuth 2.0 (3LO)] の横にある [追加] を選択します。
8. [コールバック URL] テキストボックスに、リダイレクト URL を以下の形式で入力し、[変更を保存] を選択します。

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

この URL AWS リージョン では、*<region>* は AppFabric アプリバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://us-east-1.console.aws.amazon.com/appfabric/oauth2` です。

必要範囲

Atlassian Confluence OAuth アプリケーションに次のスコープのいずれか 1 つを入力する必要があります。スコープに関する詳細は、Atlassian 開発者ウェブサイトの「Scopes for OAuth 2.0 (3LO) and Forge apps」を参照してください。可能な場合はクラシックスコープを使用します。

- クラシックスコープ:
  - `read:confluence-user`
- 詳細なスコープ:
  - `read:audit-log:confluence`

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はAtlassian Confluence、インスタンスのサブドメイン です。Atlassian Confluenceインスタンスのサブドメインは、ブラウザのアドレスバーのhttps:// と.atlassian.netとの間にあります。

テナント名

この一意の Atlassian Confluence 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。Atlassian Confluenceでクライアント ID を検索するには以下の手順を使用してください。

1. Atlassian 開発者コンソールに移動します。
2. 右上にあるプロフィールアイコンを選択し、[開発者コンソール]、[自分のアプリケーション] の順に選択します。

3. の接続に使用する OAuth アプリケーションを選択します AppFabric。
4. 「設定」ページのクライアント ID を のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。以下の手順でAtlassian Confluenceのクライアント シークレット を検索してください。

1. Atlassian 開発者コンソールに移動します。
2. 右上にあるプロフィールアイコンを選択し、[開発者コンソール]、[自分のアプリケーション] の順に選択します。
3. の接続に使用する OAuth アプリケーションを選択します AppFabric。
4. 設定ページから のクライアントシークレットフィールドにシークレットを入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されAtlassian Confluence、承認が承認されます。 AppFabric 承認を承認するには、許可 を選択します。

Atlassian Jira suite

Atlassianはすべてのチームの可能性を解き放ちます。アジャイルおよび DevOps、IT サービス管理および作業管理ソフトウェアは、チームが共有作業を整理、議論、完了するのに役立ちます。フォーチュン500企業の過半数や、NASA、、などを含む世界中のあらゆる規模の24万社を超える企業がKivaDeutsche Bank、チームの連携を強化しSalesforce、Atlassian質の高い結果を予定通りに達成するためのソリューションに頼っています。Jira Software, Confluence, Jira Service Management, Trello, Bitbucket, および Jira AlignなどのAtlassian製品について詳しくはAtlassianをご覧ください。

セキュリティ AWS AppFabric のために を使用すると、 Jira suite (以外) から監査ログとユーザーデータを受信しJira Align、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric の サポート Jira suite
- Jira アカウント AppFabric への接続

AppFabric の サポート Jira suite

AppFabric は、 を除きJira suite、 からのユーザー情報と監査ログの受信をサポートしますJira Align。

前提条件

AppFabric を使用して からサポートされている宛先Jira suiteに監査ログを転送するには、次の要件を満たす必要があります。

- Jiraスタンダードプラン以上に加入している必要があります。Jiraプランの機能について詳しくは、Jiraソフトウェア、Jiraサービス管理、Jiraワークマネジメント、Jiraプロダクトディスカバリーの料金ページをご覧ください。
- Jiraアカウントには組織管理ロールを持つユーザーが必要です。ロールの詳細については、Atlassian Support Webサイトの「ユーザーに管理者権限を付与する」を参照してください。

レート制限に関する考慮事項

Jira が、JiraAPI にレート制限を課します。Jira suiteAPI のレート制限について詳しくは、 Web サイトの『Atlassian開発者ガイド』の「レート制限」を参照してください。 AppFabric と既存の Jira API アプリケーションの組み合わせが制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Jira アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますJira。Jira で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は、OAuth Jira suiteを使用して と統合します。Jiraで OAuth アプリケーションを作成するには、以下の手順に従います。

1. Atlassian開発者コンソールに移動します。
2. [マイアプリ] の横にある [作成]、[OAuth 2.0 統合] を選択します。
3. アプリに名前を付け、[作成してください] を選択します。
4. 「認証」セクションに移動し、「OAuth 2.0」の横にある「追加」を選択します。
5. 「コールバック URL」フィールドに以下の形式の URL を入力し、「変更を保存」を選択します。

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

   この URL AWS リージョン では、*<region>* は AppFabric アプリケーションバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://us-east-1.console.aws.amazon.com/appfabric/oauth2` です。
6. 「設定」セクションに移動し、クライアント ID とクライアントシークレットをコピーして保存し、 AppFabric アプリ認証に使用します。

必要範囲

Jira OAuth アプリの[許可]ページに次のスコープを追加する必要があります。

- [クラシックスコープ] で:
  - Jira API > `read:jira-user`
- グラニュラースコープでは:
  - Jira API > `read:audit-log:jira`
  - Jira API > `read:user:jira`

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はJira、インスタンスのサブドメイン です。Jiraインスタンスのサブドメインは、ブラウザのアドレスバーのhttps://と.atlassian.netとの間にあります。

テナント名

この一意のJiraサーバーを識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。以下の手順で、Jiraでクライアント ID を検索してください。

1. Atlassian開発者コンソールに移動します。
2. の接続に使用する OAuth アプリケーションを選択します AppFabric。
3. 「設定」ページのクライアント ID を のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。のクライアントシークレット AppFabric は、 のシークレットですJira。以下の手順でJiraのシークレットを検索してください。

1. Atlassian開発者コンソールに移動します。
2. の接続に使用する OAuth アプリケーションを選択します AppFabric。
3. 設定ページから のクライアントシークレットフィールドにシークレットを入力します AppFabric。

認証を承認します

でアプリケーション認証を作成すると AppFabric 、 からポップアップウィンドウが表示されJira、認証を承認できます。承認を承認する AppFabricには、許可 を選択します。

Box

Box は、主要な Content Cloud です。これは、組織がコンテンツのライフサイクル全体を管理し、どこからでも安全に作業し、 best-of-breed アプリケーション間で統合できるようにする単一のプラットフォームです。

AWS AppFabric を使用して、 から監査ログとユーザーデータを受信しBox、データをオープンサイバーセキュリティスキーマフレームワーク (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric の サポート Box
- Box アカウント AppFabric への接続

AppFabric の サポート Box

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますBox。

前提条件

AppFabric を使用して からサポートされている宛先Boxに監査ログを転送するには、次の要件を満たす必要があります。

- 監査ログにアクセスするには、Business、Business Plus、Enterprise、または Enterprise Plus プランへの有効な有料サブスクリプションが必要です。
- 管理者権限 を持つユーザーが必要です。
- 設定タブからアプリケーションのクライアントシークレットを表示およびコピーするには、Boxアカウントで 2 要素認証が有効になっている必要があります。

レート制限に関する考慮事項

Box は、Box API にレート制限を課します。Box API レート制限 の詳細については、「 Boxデベロッパーガイド」ウェブサイトの「レート制限」を参照してください。と既存のBoxアプリケーションの組み合わせが制限を超える AppFabric と、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが送信先に配信されるまでに最大 30 分の遅延が発生することがあります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできます。サポートが必要な場合は、AWS Support にお問い合わせください。

Box アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますBox。Box で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は、OAuth Boxを使用して と統合します。次の手順を使用して で OAuth アプリケーションを作成します。詳細についてはBox、 Boxウェブサイトの[OAuth アプリケーションの作成](#)」を参照してください。

1. にログインBoxし、[デベロッパーコンソール](#) に移動します。
2. [新しいアプリの作成] を選択します。
3. アプリケーションタイプのリストからカスタムアプリケーションを選択します。次のステップの選択を求めるモーダルが表示されます。
4. アプリ名と説明を入力します。
5. 目的ドロップダウンリストから統合を選択します。
   a. カテゴリドロップダウンリストからセキュリティとコンプライアンスを選択します。
   b. どの外部システムと統合しているかテキストボックスAWS AppFabric Secureに「」と入力します。
6. クライアント ID とクライアントシークレットを使用してアプリケーション ID を検証する場合は、サーバー認証 (クライアント認証情報の付与) を選択します。
7. [Create App (アプリの作成)] を選択します。
8. [設定] タブを選択します。
9. ページの「アプリケーションアクセスレベル」セクションで、「アプリケーション + エンタープライズアクセス」を選択します。
10. ページの「アプリケーションスコープ」セクションで、「ユーザーの管理」と「エンタープライズプロパティの管理」を選択します。
11. [変更の保存] をクリックします。

    Box 管理者は、アプリケーションを使用する前にBox、管理コンソール内でアプリケーションを認証する必要があります。認証をリクエストするには、次のステップを実行します。

    a. [デベロッパーコンソール](#) 内のアプリケーションの認証タブを選択します。
    b. レビューと送信を選択して、Boxエンタープライズ管理者に承認用の E メールを送信します。詳細については、「 Boxガイド」の[「認可](#)」を参照してください。

    > **Note**
    > 送信後に変更があった場合は、アプリを再送信する必要があります。

必要範囲

次のアプリケーションスコープが必要です。スコープの詳細については、 Box ドキュメントウェブサイトの「スコープ」を参照してください。

- エンタープライズプロパティの管理 (`manage_enterprise_properties`)
- ユーザーを管理する (`manage_managed_users`)

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はBoxエンタープライズ ID です。Box エンタープライズ ID は、管理者コンソールの「 アカウントと請求 > アカウント情報 > エンタープライズ ID」にあります。詳細については、Box ドキュメントウェブサイトの「エンタープライズ ID」を参照してください。

テナント名

この一意の Box 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID とクライアントシークレット

1. にログインBoxし、デベロッパーコンソール に移動します。
2. ナビゲーションメニューで「マイアプリ」を選択します。
3. の接続に使用する OAuth アプリケーションを選択します AppFabric。
4. [設定] タブを選択します。
5. ページの「Oauth 2.0 認証情報」セクションまでスクロールします。
6. OAuth クライアント ID のクライアント ID を のクライアント ID フィールドに入力します AppFabric。
7. クライアントシークレットの取得 を選択します。
8. OAuth クライアントシークレットから のクライアントシークレットフィールドにクライアントシークレットを入力します AppFabric。

Cisco Duo

Cisco Duo は、強力な多層防御と革新的な機能を提供する主要なアクセス管理スイートを使用して、正当なユーザーを侵入させ、悪意のある攻撃者を排除する侵害から保護します。侵害を懸念し、迅速にソリューションを必要とする組織にとって、 Cisco Duo はユーザーの生産性を向上させながら、強力なセキュリティを迅速に実現します。セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しCisco Duo、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Cisco Duo
- Cisco Duo アカウント AppFabric に接続する

AppFabric のサポート Cisco Duo

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますCisco Duo。

前提条件

AppFabric を使用して からサポートされている宛先Cisco Duoに監査ログを転送するには、次の要件を満たす必要があります。

- 監査ログにアクセスするには、Duo Essentials、Duo Advantage、または Duo エディションへのアクティブなサブスクリプションが必要です。または、アドバンテージまたはプレミアムトライアルの新規のお客様も にアクセスできます。Cisco Duo エディションの詳細については、「エディションと料金」を参照してください。
- Admin API を作成または変更するには、所有者ロールを持つ管理者である必要があります。
- 管理 API の監査ログにアクセスするには、読み取りログリソースの付与「アクセス許可」を追加する必要があります。

レート制限に関する考慮事項

Cisco Duo は、Cisco Duo API にレート制限を課します。Cisco Duo API レート制限の詳細については、「認証ログ」の「レート制限」を参照してください。 AppFabric と既存の Cisco Duo API アプリケーションの組み合わせCisco Duoが の制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。レート制限の引き上げが必要な場合は、Cisco にお問い合わせください。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Cisco Duo アカウント AppFabric に接続する

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますCisco Duo。Cisco Duo で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

Cisco Duo Admin API アプリケーションを作成する

AppFabric は API サービストークンCisco Duoを使用して と統合します。でアプリケーションを作成するにはCisco Duo、次の手順を実行します。

- Cisco Duo Admin API アプリケーションを作成するには、Admin API の「最初のステップCisco Duo」の手順に従います。

必要なアクセス許可

Cisco Duo アプリケーションには、次のスコープを追加する必要があります。

- 読み取りログの付与
- 読み取りリソースの付与

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。テナント ID はCisco Duoホスト名で確認できます。でホスト名を検索するにはCisco Duo、次の手順に従います。

1. Cisco Duo 管理者ログインページに移動してサインインします。
2. アプリケーション に移動し、アプリケーション の保護 を選択します。
3. アプリケーションリストで管理 API のエントリを見つけ、右端に保護を選択してアプリケーションを設定し、API ホスト名を取得します。

4. API ホスト名は という形式です。ここでapi-*<tenant-id>*.duosecurity.com、 *<tenant-id>*はテナント ID です。

テナント名

この一意の Cisco Duo 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

サービストークン

AppFabric はサービストークンをリクエストします。サービストークンは、コロンで区切られた統合キーとシークレットキーで、次の形式になります。

```
integrationkey:secretkey
```

で統合キーとシークレットキーを検索するにはCisco Duo、次の手順を実行します。

1. Cisco Duo 管理者ログインページに移動し、サインインします。
2. アプリケーション に移動し、アプリケーション の保護 を選択します。
3. 「アプリケーションを保護するをクリックし、アプリケーションリストで管理 API のエントリを見つけます。右端にある Protect をクリックして、アプリケーションを設定します。スコープセクションまでスクロールし、 **Grant read log**と を追加します**Grant read resource**。

Dropbox

Dropbox は、何に取り組んでいるのか、どこで働いているか、どのツールを使っているかに関わらず、従業員が一丸となることで、組織がより良い仕事をより早く成し遂げられるように支援します。ユーザーは、シンプルで安全な方法でコンテンツを共有できるようになるため、イノベーションと効率性を加速することができます。Dropbox は 1 か所で生活を整理し、仕事をスムーズに進められる場所を提供します。180 か国、7 億人以上の登録ユーザーを有する Dropbox は、より賢明な働き方をデザインすることを使命としています。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信し Dropbox、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Dropbox
- Dropbox アカウント AppFabric への接続

AppFabric のサポート Dropbox

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますDropbox。

前提条件

AppFabric を使用して からサポートされている宛先Dropboxに監査ログを転送するには、次の要件を満たす必要があります。

- Dropbox ビジネスアカウントを持っている必要があります。Dropbox ビジネスアカウントの作成またはアップグレードの詳細については、Dropbox ウェブサイトの「Dropboxビジネス」を参照してください。
- Dropbox アカウントには管理者ロールを持つユーザーが必要です。ロールに関する詳細については、「Dropboxヘルプセンター」ウェブサイトの「Dropboxチームの管理者権限を変更する方法」を参照してください。

レート制限に関する考慮事項

Dropbox は、Dropbox API にレート制限を課します。Dropbox API のレート制限に関する詳細については、「Dropboxパフォーマンスガイド」ウェブサイトの「レート制限」を参照してください。AppFabric と既存の Dropbox API アプリケーションの組み合わせが制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Dropbox アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますDropbox。Dropbox で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth Dropboxを使用して と統合します。Dropbox で OAuth アプリケーションを作成するには、以下の手順に従います。

1. https://www.dropbox.com/developers/apps のDropboxアプリコンソールで 「アプリの作成」を選択します。
2. 新しいアプリケーション設定ページで、API の 「範囲指定アクセス」を選択します。
3. 次に、Dropbox アクセスの種類として[Full]を選択します。
4. OAuth アプリケーションに名前を付け、「アプリの作成」を選択して OAuth アプリケーションの初期設定を完了します。
5. アプリケーション情報ページの 「OAuth2 リダイレクト URI」 フィールドに、以下の形式のリダイレクト URL を入力します。

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

   この URL AWS リージョン では、 *<region>*は AppFabric アプリケーションバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2` です。
6. [追加]を選択します。
7. アプリ認証で使用するアプリキーと AppFabric アプリシークレットをコピーして保存します。
8. [設定] タブ以外のフィールドはすべてデフォルト値のままでかまいません。

必要範囲

アプリ情報画面の [許可] タブを使用して、次の範囲を Dropbox アプリに入力します。

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

終了したら、[送信]を選択します。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。チーム名など、Dropbox アカウントを一意に識別する任意の値を入力します。

テナント名

この一意のDropboxアカウントを識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。のクライアント ID AppFabric はDropboxアプリケーションキーです。Dropbox アプリキーを確認するには、以下のステップに従います。

1. https://www.dropbox.com/developers/apps の Dropbox アプリコンソールに移動します。
2. の接続に使用するアプリを見つけます AppFabric。
3. アプリ情報ページの「ステータス」セクションでアプリキーを検索します。
4. アプリケーションのアプリキーDropboxを のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。のクライアントシークレット AppFabric はDropboxアプリシークレットです。Dropbox アプリシークレットを確認するには、以下のステップに従います。

1. https://www.dropbox.com/developers/apps の Dropbox アプリコンソールに移動します。
2. の接続に使用するアプリを見つけます AppFabric。
3. アプリ情報ページの「ステータス」セクションでアプリキーを検索します。
4. アプリケーションのアプリシークレットDropboxを のクライアントシークレットフィールドに入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されDropbox、承認が承認されます。 AppFabric 承認を承認するには、許可 を選択します。

Genesys Cloud

Genesys Cloud は、デジタルチャネルと音声チャネルをまたいでスムーズな会話を、簡単かつ all-in-one インターフェイスで作成します。これにより企業は、従業員と顧客に優れたエクスペリエンスを提供し、導入の迅速化、複雑さの解消、管理の簡素化といった数多くのメリットを享受できます。セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しGenesys Cloud、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Genesys Cloud
- Genesys Cloud アカウント AppFabric への接続

AppFabric のサポート Genesys Cloud

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますGenesys Cloud。

前提条件

AppFabric を使用して からサポートされている宛先Genesys Cloudに監査ログを転送するには、次の要件を満たす必要があります。

- Genesys Cloud アカウントが必要です。
- Genesys Cloudアカウントには管理者ロールを持つユーザーが必要です。

レート制限に関する考慮事項

Genesys Cloud は、Genesys Cloud API にレート制限を課します。Genesys Cloud API のレート制限に関する詳細は、Genesys Cloud Developer ウェブサイトの「Rate limits」を参照してください。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Genesys Cloud アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますGenesys Cloud。Genesys Cloud で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth Genesys Cloudを使用して と統合します。Genesys Cloudで OAuth アプリケーションを作成するには、以下の手順に従います。

1. Genesys Cloud Resource Center ウェブサイトの「Create an OAuth Client」の手順に従います。

   [許可のタイプ] では [コード承認] を選択します。

2. 次の形式のリダイレクト URL を承認済みリダイレクト URL として使用します。

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

   この URL AWS リージョン では、*<region>* は AppFabric アプリバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://us-east-1.console.aws.amazon.com/appfabric/oauth2` です。

3. [スコープ] ボックスを選択すると、アプリケーションで使用できるスコープのリストが表示されます。スコープ `audits:readonly`と を選択しますusers:readonly。スコープの詳細については、「Genesys Cloud Developer Center」の「OAuth Scopes」を参照してください。

4. [保存] をクリックします。Genesys Cloud に、クライアント ID とクライアントシークレット (トークン) が作成されます。

必要範囲

Genesys Cloud OAuth アプリケーションに次の範囲を入力する必要があります。

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

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はGenesys Cloudインスタンス名です。ブラウザのアドレスバーにテナント ID が表示されます。例えば、`usw2.pure.cloud`は次のURL`https://login.usw2.pure.cloud`のテナントIDです。

テナント名

この一意の Genesys Cloud 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。Genesys Cloudでクライアント ID を検索するには以下の手順を使用してください。

1. [管理者] を選択します。
2. [統合] で [OAuth] を選択します。
3. OAuth クライアントを選択し、クライアント ID を取得します。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。以下の手順でGenesys Cloudのクライアント シークレット を検索してください。

1. [管理者] を選択します。
2. [統合] で [OAuth] を選択します。
3. OAuth クライアントを選択し、クライアントシークレットを取得します。

GitHub

GitHubは、Git を使用してソフトウェア開発とバージョン管理を行うためのプラットフォームおよびクラウドベースのサービスで、開発者はコードを保存および管理できます。Git の分散型バージョン管理に加えて、アクセス制御、バグトラッキング、ソフトウェア機能要求、タスク管理、継続的インテグレーション、すべてのプロジェクトの Wiki を提供します。セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しGitHub、データを Open Cybersecurity

Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート GitHub
- GitHub アカウント AppFabric への接続

AppFabric のサポート GitHub

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますGitHub。

前提条件

AppFabric を使用して からサポートされている宛先GitHubに監査ログを転送するには、次の要件を満たす必要があります。

- 監査ログにアクセスするには、エンタープライズアカウントが必要です。
- エンタープライズ監査ログにアクセスするには、エンタープライズアカウントの管理者ロールが必要です。
- 組織から監査ログを取得するには、組織のオーナーである必要があります。

レート制限に関する考慮事項

GitHub は、GitHub API にレート制限を課します。GitHubAPI レート制限の詳細については、GitHub ウェブサイト の「API リクエストの制限と割り当て」を参照してください。 AppFabric と既存の GitHub API アプリケーションの組み合わせがGitHub's制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

GitHub アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますGitHub。GitHub で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は、OAuth GitHubを使用して と統合します。GitHub で OAuth アプリケーションを作成するときは、以下の手順に従います。詳細については、 GitHubウェブサイトの GitHubs 「アプリケーションの作成」を参照してください。

1. ページの右上にある [プロフィール写真] を選択し、[設定] を選択します。
2. 左側のナビゲーションペインの [ディベロッパー設定] を選択します。
3. 左のナビゲーションペインから、[OAuth アプリケーション] を選択します。
4. [新規 OAuth アプリケーション] を選択します。

> **Note**
>
> OAuth アプリをまだ作成していない場合、このボタンには [新規アプリケーションの登録] というラベルが表示されます。

5. [アプリケーション名] テクストボックスにアプリケーションの名前を入力します。
6. 「ホームページ URL」テキストボックスに、アプリケーションインスタンスの完全な URL を入力します。
7. (オプション) [アプリケーションの説明] テキストボックスにアプリの説明を入力します。ユーザーにはこの説明が表示されます。
8. 「承認コールバック URL」テキストボックスに、次の形式の URL を入力します。

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

この URL AWS リージョン では、*<region>* は AppFabric アプリケーションバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://us-east-1.console.aws.amazon.com/appfabric/oauth2` です。

9. OAuth アプリがデバイスフローを使用してユーザーの識別と承認を行う場合は、「デバイスフローを有効にする」を選択します。デバイスフローについて詳しくは、「ウェブサイトでの OAuth アプリの承認」を参照してください。GitHub
10. [アプリケーションの登録] を選択します。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。テナント ID は以下のいずれかの形式で指定する必要があります。

エンタープライズ監査ログ:

エンタープライズアカウントが所有するすべての組織のアクションを集約して知りたい場合は、エンタープライズの監査ログを使用してください。

エンタープライズ監査ログを使用するには、テナント ID がアカウントのエンタープライズ ID です。ブラウザのアドレスバーにエンタープライズ ID が表示されます。例えば、*exampleenterprise*は次のURL`https://github.com/settings/enterprises/`*`examplenterprise`*のエンタープライズIDです。

エンタープライズ監査ログのテナント ID を指定するときは、プレフィックスを付ける必要があります`enterprise:`。そのため、前の例ではと指定します`enterprise:examplenterprise`。

組織監査ログ:

組織のメンバーが実行したアクションを知りたい場合は、組織の監査ログを組織管理者として使用してください。アクションを実行したユーザー、アクション内容、実行日時などの詳細が含まれます。

組織の監査ログを使用するには、テナント ID が組織 ID です。ブラウザのアドレスバーに組織 ID が表示されます。例えば、*exampleorganization*は次のURL`https://github.com/settings/organizations/`*`exampleorganization`*の組織IDです。

組織監査ログのテナント ID を指定するときは、プレフィックスを付ける必要があります`organization:`。そのため、前の例では`organization:exampleorganization`と指定します。

テナント名

この一意のGitHubエンタープライズまたは組織を識別する名前を入力します。 AppFabric は、テナント名を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。GitHubでクライアント ID を検索するには以下の手順を使用してください。

1. ページの右上にある [プロフィール写真] を選択し、[設定] を選択します。
2. 左側のナビゲーションペインの [ディベロッパー設定] を選択します。
3. 左のナビゲーションペインから、[OAuth アプリケーション] を選択します。
4. 特定の OAuth アプリを選択し、クライアントID の値を探します。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。GitHub以下の手順でクライアントシークレット を検索してください。

1. ページの右上にある [プロフィール写真] を選択し、[設定] を選択します。
2. 左側のナビゲーションペインの [ディベロッパー設定] を選択します。
3. 左のナビゲーションペインから、[OAuth アプリケーション] を選択します。
4. 特定の OAuth アプリを選択し、クライアントシークレット の値を探します。既存のクライアントシークレットが見つからない場合は、新しいクライアントシークレットを生成する必要がある場合があります。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されGitHub、承認が承認されます。 AppFabric 承認を承認するには、許可 を選択します。

OAuthアプリ へのアクセス制限が有効になっている場合は、組織が OAuth アプリケーションへのアクセスを許可していることを確認してください。

Google Analytics

Google Analytics は、検索エンジンの最適化 (SEO) とマーケティングの目的で統計と基本的な分析ツールを提供するウェブ分析サービスです。 Google Analytics は、ウェブサイトのパフォーマンス

を追跡し、訪問者のインサイトを収集するために使用されます。これにより、組織はユーザートラフィックのトップソースを決定し、マーケティング活動やキャンペーンの成功を判断し、目標の完了 (購入、カートへの製品の追加など) を追跡し、ユーザーエンゲージメントのパターンや傾向を検出し、属性などの他の訪問者情報を取得できます。小規模および中規模の小売ウェブサイトは、さまざまな顧客行動分析を取得および分析Google Analyticsするために を使用することがよくあります。これは、マーケティングキャンペーンの改善、ウェブサイトトラフィックの促進、訪問者の保持の向上に使用できます。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しAzure Monitor、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Google Analytics
- Google Analytics アカウント AppFabric への接続

AppFabric のサポート Google Analytics

AppFabric は、 からの監査ログの受信をサポートしますGoogle Analytics。

前提条件

AppFabric を使用して からサポートされている宛先Google Analyticsに監査ログを転送するには、次の要件を満たす必要があります。

- Google Analytics アカウントの管理者である必要があります。
- AppFabric がログを配信するには、Google Cloudプロジェクトで Google Analytics Admin API を有効にする必要があります。OAuth Google Analytics アプリケーションを設定するときは、必ず新しいプロジェクトを使用してください。

レート制限に関する考慮事項

Google Analytics は、Google Analytics API にレート制限を課します。Google Analytics API レート制限の詳細については、Google Analytics ウェブサイトの「制限とクォータ」を参照してください。AppFabric と既存の Google Analytics API アプリケーションの組み合わせが制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Google Analytics アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますGoogle Analytics。以下の手順を使用して、 Google Analyticsで を認証するために必要な情報を検索します AppFabric。

OAuth アプリケーションの作成

AppFabric は、OAuth Google Analyticsを使用して と統合します。で OAuth アプリケーションを作成するには、次のステップを実行しますGoogle Analytics。

1. OAuth 同意画面を設定するには、Google ウェブサイトの「Google デベロッパーガイド」の OAuth 同意画面を設定する」の手順に従います。
2. ユーザータイプに External を選択する
3. の OAuth 認証情報を設定するには AppFabric、Google デベロッパーガイドの「アクセス認証情報の作成」ページのOAuth クライアント ID 認証情報」セクションの指示に従います。
4. 次の形式のリダイレクト URL を使用します。

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

   そのアドレス AWS リージョン で、 *<region>*は AppFabric アプリバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2` です。

必要範囲

OAuth Google Analytics アプリケーションには、次のスコープを追加する必要があります。

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

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric は、 Google Analyticsアカウント ID です。

1. Google Analytics ホームページ に移動します。
2. ナビゲーションペインで管理者を選択します。
3. アカウント ID は、アカウント > アカウント設定 > アカウントの詳細 > アカウント ID にあります。

テナント名

この一意のGoogle Analytics組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。でクライアント ID を検索するには、次の手順に従いますGoogle Analytics。

1. 認証情報ページ に移動します。
2. OAuth 2.0 クライアント IDs セクションで、作成したクライアント ID を選択します。
3. クライアント ID は、ページの「追加情報」セクションに一覧表示されます。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。でクライアントシークレットを検索するには、次の手順に従いますGoogle Analytics。

1. 認証情報ページ に移動します。
2. OAuth 2.0 クライアント IDsセクションで、クライアント名を選択します。
3. クライアントシークレットは、ページのクライアントシークレットセクションに一覧表示されます。

アプリ認証

でアプリ認証を作成すると AppFabric 、 から承認Google Analyticsのポップアップウィンドウが表示され、承認が承認されます。許可 を選択して AppFabric 承認を承認するには。

Google Workspace

Google Workspace は Google が開発、販売しているクラウドコンピューティング、生産性向上ツール、コラボレーションツール、ソフトウェア、製品のコレクションです。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しGoogle Workspace、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Google Workspace
- Google Workspace アカウント AppFabric への接続

AppFabric のサポート Google Workspace

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますGoogle Workspace。

前提条件

AppFabric を使用して からサポートされている宛先Google Workspaceに監査ログを転送するには、次の要件を満たす必要があります。

- Google Workspace エンタープライズスタンダードプランへの加入が必要です。Google Workspace エンタープライズスタンダードプランの作成またはアップグレードの詳細については、「Google Workspace プラン」ウェブサイトを参照してください。
- Google Workspace には管理者ロールを持つユーザーが必要です。
- がログ AppFabric を配信するには、Google クラウドプロジェクトで Google Admin SDK API を有効にする必要があります。詳細については、「Google Workspaceデベロッパーガイド 」の「Google Workspace API の有効化」を参照してください。

レート制限に関する考慮事項

Google Workspace は、Google Workspace API にレート制限を課します。Google Workspace API レート制限の詳細については、Google Workspace ウェブサイトに掲載されている「Google Workspace管理者ガイド」の「制限とクォータ」を参照してください。 AppFabric と既存の Google Workspace API アプリケーションの組み合わせが制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

ほとんどの監査イベントでは最大 30 分の遅延が発生し、特定の監査イベントが送信先に配信されるまで最大 4 時間の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。詳細については、Google WorkSpace 管理者ヘルプウェブサイトの「データ保持とラグタイム」を参照してください。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、 にお問い合わせくださいAWS Support。

Google Workspace アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますGoogle Workspace。Google Workspace で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth Google Workspaceを使用して と統合します。Google Workspace で OAuth アプリケーションを作成するには、以下の手順に従います。

1. OAuth 同意画面を設定するには、Google Workspace ウェブサイトに掲載されている「Google Workspace デベロッパーガイド」の「OAuth 同意画面の設定」の指示に従ってください。

   ユーザータイプに「内部」を選択します。

2. の OAuth 認証情報を設定するには AppFabric、「 Google Workspace デベロッパーガイド」の「アクセス認証情報の作成」ページのOAuth クライアント ID 認証情報」セクションの指示に従います。

3. 次の形式のリダイレクト URL を使用します。

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

この URL AWS リージョン では、 *<region>*は AppFabric アプリケーションバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは us-east-1 です。そのリージョンのリダイレクト URL は https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2 です。

必要範囲

Google Workspace OAuth アプリケーションに次の範囲を入力する必要があります。

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

これらの範囲が表示されない場合は、Admin SDK API を Google クラウド API ライブラリに追加してください。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はGoogle Workspaceプロジェクト ID です。プロジェクト ID を確認するには、Google API コンソールヘルプウェブサイトの「プロジェクト ID の検索」を参照してください。

テナント名

この一意の Google Workspace を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。クライアント ID を確認するには、以下のステップに従います。

1. 「Google Workspaceデベロッパーガイド」の「認証情報の管理」ページにある「認証情報の表示」セクションの情報を使用してクライアント ID を検索します。
2. OAuth クライアントのクライアント ID を のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。クライアントシークレットを確認するには、以下の手順に従います。

1. 「Google Workspaceデベロッパーガイド」の「認証情報の管理」ページにある「認証情報の表示」セクションの情報を使用してクライアントシークレットを検索します。
2. クライアントシークレットをリセットする必要がある場合は、「Google Workspaceデベロッパーガイド」の「認証情報の管理」ページにある「クライアントシークレットのリセット」セクションの手順に従ってください。
3. のクライアントシークレットフィールドにクライアントシークレットを入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric 、 から承認Google Workspaceのポップアップウィンドウが表示され、承認が承認されます。 AppFabric 承認を承認するには、許可 を選択します。

HubSpot

HubSpot は、マーケティング、営業、コンテンツ管理、カスタマーサービスをつなげるために必要な、ソフトウェア、統合、リソースのすべてを備える顧客プラットフォームです。HubSpot のコネクテッドプラットフォームを使うことで、ユーザーは最も重要なこと、つまり顧客、に焦点を当てることにより、ビジネスをより早く成長させることができます。セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しHubSpot、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート HubSpot
- HubSpot アカウント AppFabric への接続

AppFabric のサポート HubSpot

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますHubSpot。

前提条件

AppFabric を使用して からサポートされている宛先HubSpotに監査ログを転送するには、次の要件を満たす必要があります。

- 監査ログにアクセスするには、HubSpot の Enterprise サブスクリプションのアカウントが必要になります。HubSpot サブスクリプションに関する詳細は、HubSpot のナレッジベースの「Manage your HubSpot subscription」を参照してください。
- デベロッパーアカウントと、そのアカウントに関連付けられたアプリケーションが必要になります。
- アプリケーションを HubSpot アカウントにインストールするには、スーパー管理者であるか、または、App Marketplace Access のアクセス権限と、アプリケーションが要求するスコープを受け入れるためのユーザー権限を持っている必要があります。

レート制限に関する考慮事項

HubSpot は、HubSpot API にレート制限を課します。HubSpot API のレート制限 (OAuth を使用するアプリケーションの制限を含む) に関する詳細は、HubSpot ウェブサイトの「Rate limits」を参照してください。 AppFabric と既存の HubSpot API アプリケーションの組み合わせHubSpotが の制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

HubSpot アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますHubSpot。HubSpot で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth HubSpotを使用して と統合します。HubSpotで OAuth アプリケーションを作成するには、以下の手順に従います。

1. HubSpot ウェブサイトの「HubSpot ガイド」にある「 Create a public app」のセクションの指示に従います。
2. [認証] タブから、必要範囲 に記載されている 3 つのスコープを追加します。
3. [リダイレクト URL] で、以下の形式のリダイレクト URL を使用します。

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

この URL AWS リージョン では、*<region>* は AppFabric アプリバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://us-east-1.console.aws.amazon.com/appfabric/oauth2` です。

4. [アプリの作成] を選択します。

必要範囲

HubSpot OAuth アプリケーションに次の範囲を入力する必要があります。

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

アプリ権限

テナント ID

この一意の HubSpot 組織を識別する ID を入力します。例えば、HubSpot アカウント ID などです。

テナント名

この一意の HubSpot 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。HubSpotでクライアント ID を検索するには以下の手順を使用してください。

1. HubSpot ログインページに進み、デベロッパーアカウントの認証情報を使用してサインインします。
2. [アプリケーション] メニューで自分のアプリケーションを選択します。
3. [認証] タブで、クライアント ID の値を探します。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。以下の手順でHubSpotのクライアントシークレット を検索してください。

1. HubSpot ログインページに進み、デベロッパーアカウントの認証情報を使用してサインインします。
2. [アプリケーション] メニューで自分のアプリケーションを選択します。
3. [認証] タブで、クライアントシークレットの値を探します。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されHubSpot、承認が承認されます。エンタープライズアカウントの認証情報 (デベロッパーアカウントではない) を使用してアカウントにサインインし、 AppFabric 承認を承認します。[許可] を選択します。

IBM Security® Verify

IBM Security® Verify ファミリーは、アイデンティティガバナンスの管理、ワークフォースとコンシューマーのアイデンティティとアクセスの管理、特権アカウントの制御のための自動化されたクラウドベースのオンプレミス機能を提供します。クラウドまたはオンプレミスのソリューションをデプロイする必要があるかどうかにかかわらず、 IBM Security® Verifyは、信頼を確立し、ワークフォースとコンシューマーの両方に対する内部的な脅威から保護するのに役立ちます。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信し IBM Security® Verify、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric の サポート IBM Security® Verify
- IBM Security® Verify アカウント AppFabric への接続

AppFabric の サポート IBM Security® Verify

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますIBM Security® Verify。

前提条件

AppFabric を使用して からサポートされている宛先IBM Security® Verifyに監査ログを転送するには、次の要件を満たす必要があります。

- 監査ログにアクセスするには、IBM Security® VerifySaaS アカウント が必要です。
- 監査ログにアクセスするには、SaaS IBM Security® Verify アカウントに管理者ロールが必要です。

レート制限に関する考慮事項

IBM Security® Verify は、IBM Security® Verify API にレート制限を課します。IBM Security® Verify API レート制限の詳細については、「IBM 条件」を参照してください。と既存の IBM Security® Verify API アプリケーションの組み合わせがIBM Security® Verify制限を超える AppFabric と、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが宛先に配信されるまでに最大 30 分の遅延が発生することがあります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

IBM Security® Verify アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますIBM Security® Verify。IBM Security® Verify で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は、OAuth IBM Security® Verifyを使用して と統合します。で OAuth アプリケーションを作成するにはIBM Security® Verify、IBM ドキュメントウェブサイトの「API クライアントの作成」を参照してください。

1. 初回ログインには、登録済みの E メールアドレスに送信されたログイン URL と認証情報を使用します。
2. で管理コンソールにアクセスしますhttps://<hostname>.verify.ibm.com/ui/admin/。詳細については、「IBM Security® Verify へのアクセス」を参照してください。

3. 管理コンソールの「セキュリティ < API アクセス < API クライアント」で、「 を追加」を選択します。
4. 次のオプションを選択します。これらは、監査ログとユーザーの詳細を読み取るために必要です。
   - レポートの読み取り
   - ユーザーおよびグループの読み取り
5. クライアント認証メソッド のデフォルトオプションを保持します。

   カスタムスコープフィールドを編集しないでください。
6. [次へ] をクリックします。
7. IP フィルターフィールドを編集しないでください。
8. [次へ] をクリックします。
9. 追加プロパティフィールドを編集しないでください。
10. [次へ] をクリックします。
11. 名前と説明 を指定します。説明はオプションです。
12. API クライアントの作成 を選択します。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。テナント ID は、IBM Security® Verify標準 URL にあります。例えば、`https://hostname.verify.ibm.com/`URL では、テナント ID は より前`.verify.ibm.com` (または以前の`####`を使用している場合`ice.ibmcloud.com`は より前) にあるホスト名です。バニティ URL を使用している場合は、IBM Security® Verifyサポートチームに連絡して標準 URL を取得してください。

テナント名

この一意のIBM Security® Verifyテナントを識別する名前を入力します。 AppFabric は、テナント名を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。IBM Security® Verifyでクライアント ID を検索するには以下の手順を使用してください。

1. 初回ログインには、登録済みの E メールアドレスに送信されたログイン URL と認証情報を使用します。
2. で管理コンソールにアクセスしますhttps://<hostname>.verify.ibm.com/ui/admin/。詳細については、「IBM Security® Verify へのアクセス」を参照してください。
3. 管理コンソールの Security < API Access < API Client で、特定の OAuth アプリの横にある省略記号 (⋮) を選択します。
4. 接続の詳細 を選択します。
5. API 認証情報 でクライアント ID を見つけます。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。以下の手順でIBM Security® Verifyのクライアント シークレット を検索してください。

1. 初回ログインには、登録済みの E メールアドレスに送信されたログイン URL と認証情報を使用します。
2. で管理コンソールにアクセスしますhttps://<hostname>.verify.ibm.com/ui/admin/。詳細については、「IBM Security® Verify へのアクセス」を参照してください。
3. 管理コンソールの Security < API Access < API Client で、特定の OAuth アプリの横にある省略記号 (⋮) を選択します。
4. 接続の詳細 を選択します。
5. API 認証情報 でクライアントシークレットを見つけます。

JumpCloud

JumpCloud Inc. は、アイデンティティ管理用のクラウドベースのディレクトリプラットフォームを提供する米国のエンタープライズソフトウェア会社です。ID 管理を一元化して簡素化することで、ユーザーはプラットフォーム、プロトコル、プロバイダー、場所に関係なく、単一の認証情報セットでシステム、アプリケーション、ネットワーク、ファイルサーバーに安全にアクセスできます。

AWS を使用して、 から監査ログとユーザーデータ AppFabric を受信し JumpCloud、データをオープンサイバーセキュリティスキーマフレームワーク (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Kinesis Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート JumpCloud
- JumpCloud アカウント AppFabric への接続

AppFabric のサポート JumpCloud

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますJumpCloud。

前提条件

AppFabric を使用して からサポートされている宛先JumpCloudに監査ログを転送するには、次の要件を満たす必要があります。

- 有効な有料JumpCloudサブスクリプションプランが必要です。詳細については、 JumpCloudウェブサイトのSelect a package that's right for you「」を参照してください。
- 「Admins with Billing」ロールが必要です。

レート制限に関する考慮事項

JumpCloud はレート制限を公開していません。サポートケースを作成するか、JumpCloudカスタマーチームに連絡する必要があります。AppFabric と既存の JumpCloud API アプリケーションの組み合わせがJumpCloud's制限を超えると、 に表示される監査ログが遅れAppFabricる可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションが利用できる監査イベントの遅延と、データ損失を減らすために講じられた予防策によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

JumpCloud アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますJumpCloud。JumpCloud で を承認するために必要な情報を確認するには AppFabric、次のセクションのステップに従います。

JumpCloud アカウントから Organization トークンを作成する

AppFabric は API JumpCloud キーを使用して と統合します。 で API キーを作成するには JumpCloud、次の手順に従います。

1. 管理者としてアカウントにサインインしますJumpCloud。
2. 管理者ポータルで、右上にあるアカウントのイニシャルを選択し、メニューから My API Key を選択します。
3. 新しい API キーの生成 を選択するか、既存のキーを選択します。

> **Note**
>
> JumpCloud は、アクティブな API キーを 1 つだけ許可します。新しい API キーを生成すると、現在の API キーへのアクセスが取り消されます。これにより、以前の API キーを使用するすべての呼び出しにアクセスできなくなります。以前の API キーを使用する既存の統合は、新しいキー値で更新する必要があります。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。ここで「組織 ID」はテナント ID になります。「Organization Id」を検索するには、次の手順に従います。

1. JumpCloud アカウントにサインインします。
2. ナビゲーションペインで、設定 、組織プロファイル 、一般 を選択します。
3. 「目の」アイコンを選択して、不明瞭なビューを削除します。
4. ID をコピーするには、「ダブルページ」アイコンを選択します。

テナント名

この一意のJumpCloud組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

サービスアカウントトークン

AppFabric はサービスアカウントトークンをリクエストします。では AppFabric、これはこのトピックの前JumpCloud アカウントから Organization トークンを作成する半で で作成した組織 API トークンです。

Microsoft 365

Microsoft 365 は、Microsoft が所有する生産性向上ソフトウェア、コラボレーション、クラウドベースサービスの製品ファミリーです。

セキュリティ AWS AppFabric のために を使用すると、365 Microsoft から監査ログとユーザーデータを受信し、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric 365 Microsoft のサポート
- 365 Microsoft アカウント AppFabric への接続

AppFabric 365 Microsoft のサポート

AppFabric は、365 Microsoft からのユーザー情報と監査ログの受信をサポートします。

前提条件

AppFabric を使用して 365 Microsoft からサポートされている宛先に監査ログを転送するには、次の要件を満たす必要があります。

- Microsoft365 エンタープライズプランのサブスクリプションが必要です。Microsoft 365 エンタープライズプランの作成またはアップグレードについての詳細は、Microsoft ウェブサイトの「Microsoft365 エンタープライズプラン」を参照してください。
- 管理者権限を持つユーザーが含まれている Microsoft 365 アカウントが必要です。
- 組織の監査ログを有効にする必要があります。詳細については、Microsoft ウェブサイトの「監査のオンとオフを切り替える」を参照してください。

レート制限に関する考慮事項

Microsoft 365 は、Microsoft 365 API にレート制限を課しています。Microsoft 365 API のレート制限の詳細については、Microsoft ウェブサイトの MicrosoftGraph 文書の「MicrosoftGraph サービス固有のスロットリング制限」を参照してください。 AppFabric と既存の 365 API Microsoft アプリケーションの組み合わせが制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

365 Microsoft アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、365 Microsoft で を承認 AppFabricする必要があります。で 365 Microsoft を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric はMicrosoft、OAuth を使用して 365 と統合します。Microsoft 365 で OAuth アプリケーションを作成するには、以下の手順に従います。

1. Microsoft ウェブサイトに掲載されている「Azure Active Directory 開発者ガイド」の「アプリケーションの登録」セクションの指示に従ってください。

   「サポートされているアカウントタイプ」の設定では、[この組織ディレクトリのアカウントのみ] を選択します。

2. 「Azure Active Directory 開発者ガイド」の「リダイレクト URI の追加」セクションの指示に従ってください。

   [ウェブプラットフォーム] を選択します。

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

   この URL AWS リージョン では、 *<region>*は AppFabric アプリケーションバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2` です。

   ウェブプラットフォームの他の入力フィールドはスキップできます。

3. 「Azure Active Directory 開発者ガイド」の「クライアントシークレットの追加」セクションの指示に従ってください。

必要なアクセス許可

OAuth アプリケーションには以下のアクセス許可を追加する必要があります。許可を追加するには、「Azure Active Directory 開発者ガイド」の「ウェブ API にアクセスするためのアクセス許可を追加する」セクションの指示に従ってください。

- `Microsoft Graph API` > `User.Read` (自動的に追加されます)
- `Office 365 Management APIs` > `ActivityFeed.Read` (委任タイプを選択)
- `Office 365 Management APIs` > `ActivityFeed.ReadDlp` (委任タイプを選択)
- `Office 365 Management APIs` > `ServiceHealth.Read` (委任タイプを選択)

アクセス許可の追加後にその許可に対する管理者の同意を付与するには、「Azure Active Directory 開発者ガイド」の「管理者同意ボタン」セクションの指示に従ってください。

アプリ権限

AppFabric は、365 Microsoft アカウントからのユーザー情報と監査ログの受信をサポートします。Microsoft 365 から監査ログとユーザーデータの両方を受信するには、2 つのアプリ認証を作成する必要があります。1 つはアプリ認証ドロップダウンリストで Microsoft365 という名前、もう 1 つはアプリ認証ドロップダウンリストで Microsoft365 監査ログという名前が付いています。両方のアプリ認証には、同じテナント ID、クライアント ID、およびクライアントシークレットを使用できます。Microsoft 365 から監査ログを受信するには、 Microsoft365 および Microsoft365 監査ログの両方のアプリ認証が必要です。ユーザーアクセスツールのみを使用する場合は、Microsoft365 アプリ認証のみが必要です。

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric は、Azure Active Directory のテナント ID です。Azure Active Directory のテナント ID を確認するには、Microsoft ウェブサイトの 「Azure 製品ドキュメント」の「Azure Active Directory テナント ID を確認する方法」を参照してください。

テナント名

この一意の Microsoft 365 アカウントを識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。のクライアント ID AppFabric は 365 Microsoft アプリケーション (クライアント) ID です。Microsoft 365 アプリケーション (クライアント) ID を確認するには、以下の手順に従います。

1. で使用する OAuth アプリケーションの概要ページを開きます AppFabric。
2. アプリケーション (クライアント) ID が Essentials の下に表示されます。
3. OAuth クライアントのアプリケーション (クライアント) ID を のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。365 Microsoft は、OAuth アプリケーションのクライアントシークレットを最初に作成した場合にのみ、この値を提供します。まだ行っていない場合に新しいクライアントシークレットを生成するには、以下の手順に従います。

1. クライアントシークレットを作成するには、「Azure Active Directory 開発者ガイド」の「クライアントシークレットの追加」セクションの指示に従ってください。
2. の値フィールドの内容を のクライアントシークレットフィールドに入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric、365 Microsoft からポップアップウィンドウが表示され、承認が承認されます。 AppFabric 承認を承認するには、許可 を選択します。

Miro

Miroは、あらゆる規模の分散型チームが次の大きなものを構築できるようにする、イノベーションのためのオンラインワークスペースです。プラットフォームの無限のキャンバスにより、チームは魅力的なワークショップや会議を開催したり、製品をデザインしたり、アイデアをブレインストーミングしたりすることができます。 Miroサンフランシスコとアムステルダムに共同本社を置き、Fortune 100 企業の 99% を含め、世界中で 5,000 万人以上のユーザーにサービスを提供しています。 Miro2011 年に設立され、現在、世界 12 の拠点に 1,500 人以上の従業員を擁しています。詳細については、「Miro」を参照してください。

Miroダイアグラム作成、ワイヤーフレーミング、リアルタイムのデータ視覚化、ワークショップの円滑化、アジャイルプラクティス、ワークショップ、インタラクティブなプレゼンテーションの組み

込みサポートなど、イノベーションのために設計されたコラボレーション機能がすべて含まれています。 Miro最近、Miro AI を活用したマッピングとダイアグラム作成、Miroクラスタリングと要約、コンテンツ生成といった機能を拡張する AI が発表されました。 Miro組織はスタンドアロンツールの数を減らし、情報の断片化とコスト削減を可能にします。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信し Miro、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Miro
- Miro アカウント AppFabric への接続

AppFabric のサポート Miro

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますMiro。

前提条件

AppFabric を使用して からサポートされている宛先Miroに監査ログを転送するには、次の要件を満たす必要があります。

- Miro Enterprise プランが必要です。Miro プランタイプの詳細については、Web Miroサイトの料金ページを参照してください。Miro
- Miroアカウントには会社管理者ロールを持つユーザーが必要です。ロールについて詳しくは、Miro ヘルプセンター Web サイトの「Miro のロール」の「会社レベル」セクションを参照してください。
- Miroアカウントには Enterprise Developer チームが必要です。開発者チームの作成について詳しくは、Miro Help Center Web サイトの「エンタープライズ開発者チーム」を参照してください。

レート制限に関する考慮事項

Miro は、Miro API にレート制限を課します。MiroAPI のレート制限について詳しくは、Miro Web サイトの『Miro開発者ガイド』の「レート制限」を参照してください。 AppFabric と既存の Miro API アプリケーションの組み合わせが制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Miro アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますMiro。Miro で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth Miroを使用して と統合します。Miroで OAuth アプリケーションを作成するには、以下の手順に従います。

1. OAuth アプリケーションを作成するには、Miro Help Center Web サイトのエンタープライズデベロッパーチームの記事の「アプリの作成とインストール」セクションの指示に従ってください。
2. アプリ作成ダイアログで、エンタープライズ組織の開発者チームを選択した後に、「ユーザー認証トークンを期限切れにする」チェックボックスを選択します。

   > **Note**
   >
   > このオプションはアプリの作成後に変更できないため、アプリを作成する前に行う必要があります。

3. アプリページの「OAuth 2.0 用リダイレクト URI」セクションに次の形式の URL を入力します。

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

   この URL AWS リージョン では、*<region>* は AppFabric アプリバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://us-east-1.console.aws.amazon.com/appfabric/oauth2` です。

4. AppFabric アプリケーション認証で使用するクライアント ID とクライアントシークレットをコピーして保存します。

必要範囲

MiroOAuth `Permissions` アプリページのセクションに次のスコープを追加する必要があります。

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

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はMiroチーム ID です。Miro チーム ID の確認方法については、「Miro新しい管理者です」の「よくある質問」セクションを参照してください。 Miroヘルプセンターの Web サイトのどこから始めればいいですか?

テナント名

この一意の Miro 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。クライアント ID を確認するには、以下のステップに従います。

1. Miroプロファイル設定に移動します。
2. 「マイアプリ」タブを選択します。
3. との接続に使用するアプリを選択します AppFabric。
4. アプリ認証情報セクションのクライアント ID を のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。クライアントシークレットを確認するには、以下の手順に従います。

1. Miroプロファイル設定に移動します。
2. 「マイアプリ」タブを選択します。
3. との接続に使用するアプリを選択します AppFabric。
4. アプリ認証情報セクションのクライアントシークレットを、 のクライアントシークレットフィールドに入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されMiro、承認が承認されます。 AppFabric 承認を承認するには、許可 を選択します。

Okta

Oktaは世界のアイデンティティ企業です。Oktaは、独立系の主要なアイデンティティパートナーとして、誰もがどこでも、あらゆるデバイスやアプリであらゆるテクノロジーを安全に使用できるようにします。最も信頼されているブランドは、安全なアクセス、認証、自動化を実現するOktaを信頼しています。Oktaワークフォース ID クラウドとカスタマー ID クラウドの中核をなす柔軟性と中立性により、ビジネスリーダーや開発者は、カスタマイズ可能なソリューションと 7,000 を超える事前構築済みの統合により、イノベーションに注力し、デジタルトランスフォーメーションを加速できます。 Oktaはアイデンティティが自分のものである世界を構築しています。詳細については、okta.com.を参照してください。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信し Okta、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Okta
- Okta アカウント AppFabric への接続

AppFabric のサポート Okta

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますOkta。

前提条件

AppFabric を使用して からサポートされている宛先Oktaに監査ログを転送するには、次の要件を満たす必要があります。

- は、任意のOktaプランタイプ AppFabric で使用できます。
- Oktaアカウントにはスーパー管理者ロールを持つユーザーが必要です。
- でアプリケーション認証を承認するユーザーには、Oktaアカウントでスーパー管理者ロールも AppFabric 必要です。

レート制限に関する考慮事項

Okta は、Okta API にレート制限を課します。OktaAPI のレート制限について詳しくは、Okta Web サイトの『Okta開発者ガイド』の「レート制限」を参照してください。 AppFabric と既存の Okta API アプリケーションの組み合わせOktaが の制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Okta アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますOkta。Okta で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth Oktaを使用して と統合します。と接続する OAuth アプリケーションを作成するには AppFabric、Oktaヘルプセンターウェブサイトの「OIDC アプリケーション統合の作成」の手順に従います。の設定に関する考慮事項を次に示します AppFabric。

1. [アプリケーションタイプ]には 、[Webアプリケーション] を選択します。
2. 「権限付与タイプ」には、「認証コード」と「更新トークン」を選択します。
3. サインインリダイレクト URI とサインアウトリダイレクト URI には、次の形式のリダイレクト URL を使用します。

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

この URL AWS リージョン では、*<region>* は AppFabric アプリバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://us-east-1.console.aws.amazon.com/appfabric/oauth2` です。

4. 信頼できるオリジンの設定は省略できます。
5. 制限付きアクセス設定で、Okta組織内の全員にアクセス権を付与します。

> **Note**
>
> OAuth アプリケーションの初回作成時にこのステップを省略しても、アプリケーション設定ページの「割り当て」タブを使用して、組織内の全員をグループとして割り当てることができます。

6. その他のオプションはすべて、デフォルト値のままにしておくことができます。

必要範囲

Okta OAuth アプリケーションに次の範囲を入力する必要があります。

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

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はOktaドメインです。Oktaドメインの検索について詳しくは、Oktaウェブサイトの『Okta開発者ガイド』の「Oktaドメインを探す」を参照してください。

テナント名

この一意の Okta 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。Oktaでクライアント ID を検索するには以下の手順を使用してください。

1. Okta開発者コンソールに移動します。
2. [アプリケーション] タブを選択します。
3. アプリケーションを選択し、「一般」タブを選択します。
4. 「クライアント認証情報」セクションまでスクロールします。
5. OAuth クライアントのクライアント ID を のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。以下の手順でOktaのクライアントシークレット を検索してください。

1. Okta開発者コンソールに移動します。
2. [アプリケーション] タブを選択します。
3. アプリケーションを選択し、「一般」タブを選択します。
4. 「クライアント認証情報」セクションまでスクロールします。
5. OAuth アプリケーションのクライアントシークレットを のクライアントシークレットフィールドに入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されOkta、承認が承認されます。 AppFabric 承認を承認するには、許可 を選択します。Okta認証を承認するユーザーには、Oktaのスーパー管理者権限が必要です。

OneLogin by One Identity

OneLogin by One Identity は、従業員、顧客、パートナーのすべてのデジタル ID をシームレスに管理する、最新のクラウドベースのアクセス管理ソリューションです。OneLogin は、安全なシングルサインオン (SSO)、多要素認証 (MFA)、適応型認証、デスクトップレベルの MFA、AD や LDAP、G Suite その他外部ディレクトリとの統合、ID ライフサイクル管理など、さまざまな機能を備えていま

す。を使用するとOneLogin、最も一般的な攻撃から組織を保護し、セキュリティの向上、スムーズなユーザーエクスペリエンス、規制要件への準拠を実現できます。 AWS AppFabric を使用して、 から監査ログとユーザーデータを受信しOneLogin、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート OneLogin by One Identity
- OneLogin by One Identity アカウント AppFabric への接続

AppFabric のサポート OneLogin by One Identity

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますOneLogin by One Identity。

前提条件

AppFabric を使用して からサポートされている宛先OneLogin by One Identityに監査ログを転送するには、次の要件を満たす必要があります。

- OneLogin の Advanced または Professional のアカウントが必要です。
- 管理者/委任管理者の権限を持つユーザーが必要です。

レート制限に関する考慮事項

OneLogin by One Identity は、OneLogin API にレート制限を課します。OneLogin API レート制限の詳細については、「OneLogin API Reference」の「Get Rate Limit」を参照してください。AppFabric と既存の OneLogin API アプリケーションの組み合わせOneLoginが の制限を超えると、に表示される監査ログが遅れ AppFabric る可能性があります。ただし、OneLogin レート制限は増やすことができます。サポートが必要な場合は OneLogin by One Identity アカウントマネージャー、または One Identity にお問い合わせください。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

OneLogin by One Identity アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますOneLogin by One Identity。OneLogin で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth OneLogin by One Identityを使用して と統合します。OneLoginで OAuth アプリケーションを作成するには、以下の手順に従います。

1. OneLogin のログインページに進み、サインインします。
2. [デベロッパー] メニューから [API 認証情報] を選択します。
3. [新しい認証情報] を選択し、新しい認証情報の名前を入力して、[すべて読み取る] を選択します。
4. [保存] をクリックします。OneLogin に、クライアント ID とクライアントシークレットが作成されます。

必要範囲

OneLogin by One Identity OAuth アプリケーションに次の範囲を入力する必要があります。

- すべて読み取ります。スコープとクライアント認証情報の詳細については、「OneLogin API Reference」の「Working with API Credentials」を参照してください。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はインスタンスのサブドメインです。ブラウザのアドレスバーにテナント ID が表示されます。例えば、subdomainは次のURLhttps://*subdomain*.onelogin.comのテナントIDです。

テナント名

この一意の OneLogin by One Identity 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。OneLogin by One Identityでクライアント ID を検索するには以下の手順を使用してください。

1. OneLogin のログインページに進み、サインインします。
2. [デベロッパー] メニューから [API 認証情報] を選択します。
3. API 認証情報を選択してクライアント ID を取得します。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。以下の手順でOneLogin by One Identityのクライアント シークレット を検索してください。

1. OneLogin のログインページに進み、サインインします。
2. [デベロッパー] メニューから [API 認証情報] を選択します。
3. API 認証情報を選択してクライアントシークレットを取得します。

クライアントアプリケーションの認証

で AppFabric、テナント ID と名前、クライアント ID と名前を使用してアプリ認証を作成します。[接続] を選択して認証を有効にします。

PagerDuty

PagerDuty は、兆候を発見したらすぐ行動に移すことで、顧客に影響がおよぶ問題を最小限に抑え、すばやい問題解決と業務効率の向上につなげる、デジタルオペレーション管理プラットフォームです。CloudWatch、GuardDuty、CloudTrail、Personal Health Dashboard と統合します。セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信し PagerDuty、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート PagerDuty
- PagerDuty アカウント AppFabric への接続

AppFabric のサポート PagerDuty

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますPagerDuty。

前提条件

AppFabric を使用して からサポートされている宛先PagerDutyに監査ログを転送するには、次の要件を満たす必要があります。

- 監査ログにアクセスするには、PagerDuty のビジネスプランまたはデジタルオペレーションプランに加入している必要があります。
- ユーザーは、PagerDuty アカウントのグローバル管理者かアカウントオーナーである必要があります。

レート制限に関する考慮事項

PagerDuty は、PagerDuty API にレート制限を課します。PagerDuty API のレート制限の詳細については、「PagerDuty デベロッパープラットフォーム」の「REST API Rate Limits」を参照してください。 AppFabric と既存の PagerDuty API アプリケーションの組み合わせが PagerDutyの制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

PagerDuty アカウント AppFabric への接続

PagerDuty プラットフォームは API アクセスキーをサポートしています。API アクセスキーを生成するには、次のステップを実行します。

API アクセスキーを作成する

AppFabric は、パブリッククライアントの API アクセスキーPagerDutyを使用して と統合します。PagerDuty で API アクセスキーを生成するには、次のステップを実行します。

1. PagerDuty のログインページに進み、サインインします。
2. [統合]、[API アクセスキー] の順に選択します。

3. [新しい API キーを作成] を選択します。
4. 説明を入力し、[読み取り専用 API キー] を選択します。
5. [Create Key] (キーを作成) を選択します。
6. API キーをコピーし、保存します。これは、 で後ほど必要になります AppFabric。API キーを保存する前にページを閉じる場合は、新しい API キーを生成して保存する必要があります。API PagerDutyレート制限を他の統合と共有しないように AppFabric 、このキーは 専用にする必要があります。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。PagerDuty アカウントのテナント ID は、お使いのアカウントのベース URL です。この情報は、PagerDuty にログインし、ウェブブラウザのアドレスバーからコピーすることで確認できます。テナント ID は、次のいずれかの形式に従っている必要があります。

- 米国のアカウントの場合、*subdomain*.pagerduty.com
- EU のアカウントの場合、*subdomain*.eu.pagerduty.com

テナント名

この一意の PagerDuty 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

サービスアカウントトークン

AppFabric はサービスアカウントトークンをリクエストします。のサービスアカウントトークン AppFabric は、 で作成した API アクセスキーですAPI アクセスキーを作成する。

Ping Identity

Ping Identity で私たちは、すべてのユーザーに安全かつシームレスなデジタル体験を、妥協なく実現することは可能だと考えます。だからこそ Ping Identity は、ユーザーのデジタルインタラクションを保護すると同時にスムーズなユーザーエクスペリエンスを実現するために、フォーチュン 100 企業の半数以上から選ばれているのです。2023 年 8 月 23 日、Ping Identity と ForgeRock は、より多くの選択肢、より深い専門知識、より完全な ID ソリューションをお客様とパートナーにお届けする

ために提携しました。セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しPing Identity、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Ping Identity
- Ping Identity アカウント AppFabric への接続

AppFabric のサポート Ping Identity

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますPing Identity。

前提条件

AppFabric を使用して からサポートされている宛先Ping Identityに監査ログを転送するには、次の要件を満たす必要があります。

- Essential、Plus、Premium Ping Identity のいずれかのアカウントが必要です。該当する Ping Identity プランタイプの作成またはアップグレードの詳細については、「Ping Identity Web サイトのPing Identityすべての機能の価格表」を参照してください。
- Ping Identity アカウントには Identity Data Read Only のロールが必要です。アカウントには、アプリケーションにロールを付与することで、ロールを追加することができます。ロールの詳細については、Ping Identity サポートのウェブサイトの「Roles」を参照してください。

レート制限に関する考慮事項

Ping Identity はレート制限を公開していません。サポートケースを作成するか、Ping Identity カスタマーサクセスチームに連絡してください。 AppFabric と既存の Ping Identity API アプリケーションの組み合わせが Ping Identityの制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Ping Identity アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますPing Identity。Ping Identity で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth Ping Identityを使用して と統合します。Ping Identityで OAuth アプリケーションを作成するには、以下の手順に従います。

1. Ping Identity ウェブサイトの「PingOne for Developers」ガイドにある「Create an application connection」のセクションの指示に従います。
2. アプリケーションを作成したら、付与のタイプをカスタマイズします。
   a. アプリケーションにサインインしたら、[設定] タブを選択し、鉛筆アイコンをクリックして既存の設定を変更します。
   b. [付与タイプ] で [認証コード] を選択します。[PKCE 実行] は [オプション] のままにしておきます。
   c. [更新トークン] を選択し、更新期間を選択します。
3. [リダイレクト URL/コールバック URL] では、次の形式のリダイレクト URL を使用します。

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

   この URL AWS リージョン では、*<region>* は AppFabric アプリバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2` です。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はPing Identityインスタンス名です。ブラウザのアドレスバーにテナント ID が表示されます。例えば *API_PATH*`/v1/environments/`*environmentID* です。ここでは、*API_PATH* は PingOne サーバーのリージョンドメイン (`api.pingone.com` など) を表し、*environmentID* は、アプリケーションの環境プロパ

ティで示された環境 ID を表します。環境プロパティの詳細については、Ping Identity のウェブサイトの「Environment Properties」を参照してください。

テナント名

この一意の Ping Identity 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。Ping Identityでクライアント ID を検索するには以下の手順を使用してください。

1. PingOne の管理コンソールにサインインし、[アプリケーション] を選択します。
2. リストの中からアプリケーションを選択します。
3. [概要] タブを選択し、[クライアント ID] の値を探します。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。以下の手順でPing Identityのクライアント シークレット を検索してください。

1. PingOne の管理コンソールにサインインし、[アプリケーション] を選択します。
2. リストの中からアプリケーションを選択します。
3. [概要] タブを選択し、[クライアントシークレット] の値を探します。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されPing Identity、承認が承認されます。 AppFabric 承認を承認するには、許可 を選択します。

Salesforce

Salesforce は、企業がより多くの見込み客を見つけ、より多くの取引を締結し、優れたサービスで顧客を驚かせるのに役立つように設計されたクラウドベースのソフトウェアを提供します。Salesforce’sCustomer 360 は、一連の製品を提供し、販売、サービス、マーケティング、コマース、IT の各チームを顧客情報に関する単一の共有ビューにまとめ、組織が顧客や従業員との関係を拡大するのに役立ちます。 AWS AppFabric を使用して、 から監査ログとユーザーデータを受信し

Salesforce、データをオープンサイバーセキュリティスキーマフレームワーク (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Salesforce
- Salesforce アカウント AppFabric への接続

AppFabric のサポート Salesforce

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますSalesforce。

前提条件

AppFabric を使用して からサポートされている宛先Salesforceに監査ログを転送するには、次の要件を満たす必要があります。

- Performance、Enterprise、または Unlimited エディションの が必要ですSalesforce。これらのエディションのいずれかにアップグレードするにはSalesforce、 にお問い合わせください。
- からログイベントの完全なセットを含む 1 時間ごとのイベントログファイル AppFabric を転送する場合はSalesforce、 の Shield 機能の一部として Event Monitoring をサブスクライブする必要がありますSalesforce。それ以外の場合、 AppFabric は制限されたイベント (ログイン、ログアウト、API の合計使用量 InsecureExternalAssets、CORS 違反、 HostnameRedirects ELF イベントなど) をSalesforce’s標準の日次ログファイルから転送します。Salesforce アカウントが既に Shield 機能をサブスクライブしているかどうかを確認するには、「セットアップ > イベントマネージャー」を参照してください。19 件以上のイベントが表示された場合、アカウントはイベントモニタリングにサブスクライブされます。Event Monitoring がない場合は、 に連絡してこのアドオンのサブスクリプションを購入できますSalesforce。
- Salesforce 設定でイベントログファイルの生成をオプトインする必要があります。
- システム管理者プロファイルを使用して OAuth アプリケーションを作成し、 の同じ認証情報でログインする必要があります AppFabric。

> **Note**
>
> API の合計使用量、CORS 違反レコード、ホスト名リダイレクト、安全でない外部アセット、ログイン、ログアウトイベントは、 のサポートされているエディションで追加料金なしで利用できますSalesforce。残りのイベントタイプを購入するSalesforceには、 にお問い

合わせください。Salesforce イベントタイプの詳細については、 Salesforceウェブサイトの[EventLogFile 「サポートされているイベントタイプ」](#)を参照してください。AppFabric は、ログファイルインスタンスごとにイベントタイプごとに最大 100,000 個のイベントをサポートできます (Event Monitoring アドオンサブスクリプションに応じて毎日または毎時) 。ログファイルがしきい値を超えると、ログファイル全体が取り込みから除外される可能性があります。

レート制限に関する考慮事項

Salesforce は、Salesforce API にレート制限を課します。Salesforce API レート制限の詳細については、 Salesforceウェブサイトの[「API リクエストの制限と割り当て」](#)を参照してください。と既存の Salesforce API アプリケーションの組み合わせがSalesforce's制限を超える AppFabric と、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが送信先に配信されるには、毎日のログファイルで最大 6 時間の遅延、または 1 時間あたりのログファイルで最大 29 時間の遅延が発生することがあります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、[AWS Support](#) にお問い合わせください。

Salesforce アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますSalesforce。Salesforce で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は、OAuth Salesforceを使用して と統合します。Salesforceで OAuth アプリケーションを作成するには、以下の手順に従います。

1. [Salesforceアカウントにログインします。](#)
2. [Salesforce ドキュメント](#) の説明に従って、セットアップページに移動します。
3. クイック検索で App Manager を検索します。
4. 新しい接続アプリケーション を選択します。
5. フォームフィールドに必要な情報を入力します。

6. OAuth 設定を有効にする を選択します。
7. 必ず以下のオプションをオフにしてください。
   - サポートされている承認フローにコード交換 (PKCE) 拡張機能の証明キーを要求する
   - ウェブサーバーフローにシークレットを要求する
   - 更新トークンフローにシークレットを要求する
8. コールバック URL テキストボックスに次の形式の URL を入力し、変更を保存を選択します。

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

   この URL AWS リージョン では、*<region>* は AppFabric アプリケーションバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://us-east-1.console.aws.amazon.com/appfabric/oauth2` です。
9. 必要に応じてスコープを入力します (次の必要範囲セクションで説明) 。他のすべてのフィールドはデフォルト値のままにすることができます。
10. [保存] を選択します。
11. 次の手順を実行して、新しい OAuth アプリの更新トークンポリシーを確認します。
    a. セットアップページで、接続されたアプリをクイック検索テキストボックスに入力し、接続されたアプリの管理を選択します。
    b. 新しく作成したアプリの横にある編集を選択します。
    c. 取り消されたオプションが選択されるまで、更新トークンが有効であることを確認します。
    d. 変更を保存します。
12. 監査ログが生成されていることを確認するには、次のステップを実行します。
    a. セットアップページで、クイック検索テキストボックスにイベントログファイルを入力し、イベントログファイルブラウザ を選択します。
    b. イベントログがイベントログファイルブラウザ にリストされていることを確認します。
13. 作成したアプリに移動し、ドロップダウンから表示を選択します。
14. [コンシューマーの詳細を管理] を選択します。

    ID を検証する必要がある新しいタブにリダイレクトされます。そのタブで、コンシューマーキーとコンシューマーシークレットの値を書き留めます。サインインするには、後でこれらが必要になります。

必要範囲

Salesforce OAuth アプリケーションに次の範囲を入力する必要があります。

- APIs () を使用してユーザーデータを管理しますAPI。
- リクエストはいつでも実行します (`refresh_token` と `offline_access`) 。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric は、SalesforceMy Domain のサブドメインです。My Domain サブドメインは、ブラウザのアドレスバーで `https://`と の間で確認できます`.my.salesforce.com`。

Salesforce マイドメイン を検索するには、Salesforceホーム画面から以下の手順に従います。

1. Salesforce ドキュメント の説明に従って、セットアップページに移動します。
2. クイック検索で会社設定を検索し、結果でマイドメインを選択します。

テナント名

この一意のSalesforce組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。Salesforceでクライアント ID を検索するには以下の手順を使用してください。

1. セットアップページに移動します。
2. Setup を選択し、App Manager を選択します。
3. 作成したアプリを選択し、ドロップダウンメニューから表示を選択します。
4. [コンシューマーの詳細を管理] を選択します。新しいタブにリダイレクトされます。
5. ID を確認し、コンシューマーキーの値を探します。
6. のクライアント ID フィールドにコンシューマーキーを入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。のクライアントシークレット AppFabric は、 のコンシューマーシークレットですSalesforce。でシークレットを検索するには Salesforce、次のステップに従います。

1. セットアップページに移動します。
2. Setup を選択し、App Manager を選択します。
3. 作成したアプリを選択し、ドロップダウンメニューから表示を選択します。
4. [コンシューマーの詳細を管理] を選択します。新しいタブにリダイレクトされます。
5. ID を確認し、コンシューマーシークレットの値を探します。
6. のクライアントシークレットフィールドにコンシューマーシークレットを入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されSalesforce、承認が承認されます。承認ページで、Salesforceシステム管理者ロール、または承認中にイベントログファイルの表示と API が有効なユーザーのアクセス許可Salesforceを持つユーザーを使用してください。許可 を選択して、承認を承認します AppFabric。

ServiceNow

ServiceNow は、企業の IT 運用を自動化するクラウドベースのサービスの主要プロバイダーです。ServiceNowの ITOM は、仮想化インフラストラクチャやクラウドインフラストラクチャなど、IT 環境全体の完全な可視性と制御を企業に提供します。サービスのマッピング、提供、保証を簡素化し、ITサービスとインフラストラクチャのデータを単一の記録システムに統合します。また、イベント、インシデント、問題、構成、変更管理などの主要プロセスを自動化および合理化します。セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信し ServiceNow、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート ServiceNow
- データ遅延に関する考慮事項
- ServiceNow アカウント AppFabric への接続

AppFabric のサポート ServiceNow

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますServiceNow。

前提条件

AppFabric を使用して からサポートされている宛先ServiceNowに監査ログを転送するには、次の要件を満たす必要があります。

- は、任意のServiceNowプランタイプ AppFabric で使用できます。
- ServiceNowアカウントには管理者ロールを持つユーザーが必要です。
- ServiceNowインスタンスが必要です。

レート制限に関する考慮事項

ServiceNow は、ServiceNow API にレート制限を課します。API のレート制限について詳しくは、ServiceNow Web サイトのインバウンドREST API レート制限 を参照してください。 AppFabric と既存の ServiceNow API アプリケーションの組み合わせが制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

ServiceNow アカウント AppFabric への接続

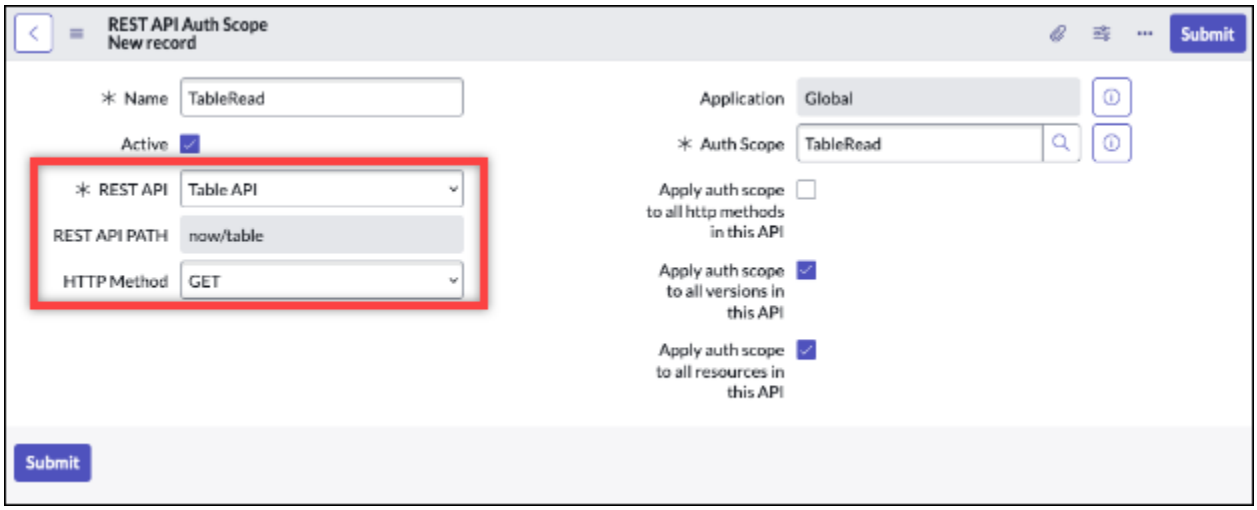
AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますServiceNow。以下の手順を使用して、 ServiceNowで を認証するために必要な情報を検索します AppFabric。

OAuth アプリケーションの作成

Now Platform は、パブリッククライアントがアクセストークンを生成するための OAuth 2.0-認可グラントタイプをサポートしています。

1. OAuth アプリケーションを登録します。この場合、以下の3ステップに従います。これらの手順を完了する方法について詳しくは、Web サイトの「アプリケーションの登録先」を参照してください。ServiceNow ServiceNow

a. アプリを登録し、認証スコープがテーブル API にアクセスできることを確認します。REST API PATH は now/table、HTTP メソッドは GET です。



b. 認可コードを生成します。

c. 認証コードを使用してベアラートークンを生成します。

2. 次の形式のリダイレクト URL を使用します。

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

この URL AWS リージョン では、*<region>* は AppFabric アプリケーションバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2` です。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はインスタンス名です。ブラウザのアドレスバーにテナント ID が表示されます。例えば、*example*は次のURL`https://`*`example`*`.service-now.com`のテナントIDです。

テナント名

この一意のServiceNow組織を識別する名前を入力します。 AppFabric は、テナントの名前を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。ServiceNowでクライアント ID を検索するには以下の手順を使用してください。

1. ServiceNow コンソールに移動します。
2. [システム OAuth] 、[アプリケーションレジストリ] (アプリケーションレジストリ) の順に選択します。
3. アプリケーションを選択します。
4. OAuth クライアントのクライアント ID を のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。ServiceNow以下の手順でクライアントシークレット を検索してください。

1. ServiceNow コンソールに移動します。
2. [システム OAuth] 、[アプリケーションレジストリ] (アプリケーションレジストリ) の順に選択します。
3. アプリケーションを選択します。
4. OAuth アプリケーションのクライアントシークレットを のクライアントシークレットフィールドに入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されServiceNow、承認が承認されます。許可 を選択して AppFabric 、承認を承認します。

Singularity Cloud

このSingularity Cloudプラットフォームは、すべての段階で、すべてのカテゴリの脅威から企業を保護します。その特許取得済みの人工知能は、セキュリティを既知の署名やパターンから、ゼロデイ攻撃やランサムウェアなどの最も高度な攻撃にまで拡張します。

AWS AppFabric を使用して、 から監査ログとユーザーデータを受信しSingularity Cloud、データをオープンサイバーセキュリティスキーマフレームワーク (OCSF) 形式に正規化し、Amazon Simple

Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

> **Note**
>
> Singularity Cloud ドキュメントは、Singularity Cloudアカウントにサインインした後にのみアクセスできます。したがって、このドキュメントのSingularity Cloudドキュメントに直接リンクすることはできません。

トピック

- AppFabric のサポート Singularity Cloud
- Singularity Cloud アカウント AppFabric への接続

AppFabric のサポート Singularity Cloud

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますSingularity Cloud。

前提条件

AppFabric を使用して からサポートされている宛先Singularity Cloudに監査ログを転送するには、Singularity Cloudアカウントに管理者ロールが必要です。Singularity Cloud API レート制限の詳細については、Singularity Cloud アカウントにサインインし、ドキュメントセクションを参照し、ロール を検索します。

レート制限に関する考慮事項

Singularity Cloud は、Singularity Cloud API にレート制限を課します。Singularity Cloud API レート制限の詳細については、Singularity Cloud アカウントにサインインし、ドキュメントセクションを参照し、API レート制限 を検索します。

データ遅延に関する考慮事項

監査イベントが宛先に配信されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Singularity Cloud アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますSingularity Cloud。Singularity Cloud で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

の API トークンを作成する Singularity Cloud

サービスユーザーに関連付けられている API トークンを作成するには、次の手順を実行します。API トークンは、特定のコンソールユーザーまたは E メールアドレスにリンクされません。

> **Note**
>
> 新しいユーザーを作成するか、サービスユーザーをコピーして、サービスユーザー API トークンの有効期限が切れる前または後に新しい API トークンを取得します。

1. Singularity Cloud アカウントにサインインします。
2. 設定ツールバーで、ユーザー を選択し、サービスユーザー を選択します。
3. アクション を選択し、新しいサービスユーザーの作成 を選択します。
4. 「新しいサービスユーザーの作成」ページで、サービスユーザーの名前、説明、有効期限を入力します。
5. [次へ] をクリックします。
6. アクセス範囲の選択セクションで、スコープを選択します。
   - アクセスレベルのアカウントを選択します。
   - 監査ログを取得するアカウントを選択します。
7. [ユーザーを作成] をクリックします。

   API トークンが生成されます。ウィンドウが開き、トークンを最後に表示できることを示すメッセージとともにトークン文字列が表示されます。
8. (オプション) API トークンのコピーを選択し、安全な場所に保存します。
9. [閉じる] を選びます。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID は、サービスにサインインする Sentinel Oneウェブサイトアドレスのサブドメイン AppFabric になります。例えば、`example-company-1.sentinelone.net`住所でSingularity Cloudアカウントにサインインすると、テナント ID は になります`example-company-1`。

テナント名

この一意のSingularity Cloud組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

サービスアカウントトークン

このガイドの の API トークンを作成する Singularity Cloudセクションのステップを使用して生成したトークンを使用します。トークンを紛失したり、見つけられない場合は、同じステップを再度実行して新しいトークンを生成できます。

> **Note**
>
> が監査ログを取り込む間に Singularity Cloud コンソールで新しい API AppFabric トークンが生成されると、取り込みは停止します。この場合、新しい API トークンでアプリ認証を更新して、監査ログの取り込みを再開する必要があります。

Slack

Slack は人々のワーキングライフをよりシンプルに、より楽しく、より生産的なものにすることを使命としています。シームレスな検索とナレッジ共有およびコード不要の自動化に加え、チームのつながりを強化して目標達成に向けた協力体制を支援することでパフォーマンスを向上させる、顧客企業向けの生産性プラットフォームです。Salesforce の一部として、Slack は Salesforce Customer 360 に深く統合されているため、営業、サービス、マーケティングの各チーム全体の生産性が大幅に向上します。Slack の詳細を確認して無料で使い始めるには、slack.com をご覧ください。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信し Slack、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Slack
- Slack アカウント AppFabric への接続

AppFabric のサポート Slack

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますSlack。

前提条件

AppFabric を使用して からサポートされている宛先Slackに監査ログを転送するには、次の要件を満たす必要があります。

- Slack でのエンタープライズグリッドプランへの加入が必要です。詳細については、Slack ウェブサイトの「Slackエンタープライズグリッド入門」を参照してください。
- Slack アカウントには組織の所有者ロールを持つユーザーが必要です。ロールの詳細については、Slack ウェブサイトのSlackヘルプセンター にある「ロールの種類Slack 」を参照してください。

レート制限に関する考慮事項

Slack は、Slack API にレート制限を課します。Slack API レート制限の詳細については、Slack ウェブサイトの「SlackAPI 使用ガイド」にある「レート制限」を参照してください。 AppFabric と既存の Slack API アプリケーションの組み合わせが制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Slack アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますSlack。Slack で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth Slackを使用して と統合します。OAuth アプリを作成するには、アプリマニフェストを使用する方法と、ゼロから作成する方法の 2 つがあります。Slack で OAuth アプリケーションを作成するには、以下の手順に従います。

Using an app manifest

1. ブラウザでSlackアプリ管理 UI に移動します。
2. [新しいアプリ の作成] を選択します。
3. [アプリマニフェストから] を選択します。
4. を承認するワークスペースを選択します AppFabric。
5. [以下にアプリマニフェストを入力]ボックスで [JSON] を選択し、既存の JSON を次のものに置き換えます。*<region>* を適切な AWS リージョン (など*us-east-1*) に置き換えます。

```
{
    "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. 「基本情報」ページからクライアント ID とクライアントシークレットをコピーして保存します。

7. `auditLogs:read` の範囲では、アプリのパブリックディストリビューションを有効にする必要があります。詳しくは、「Slack」 ウェブサイトの[パブリックディストリビューションの有効化]を参照してください。

From scratch

1. 「アプリの作成」画面で [ゼロから作成] を選択します。
2. アプリに名前を付け、ワークスペースを選択します。
3. 「基本情報」ページからクライアント ID とクライアントシークレットをコピーして保存します。
4. 「OAuth および許可」ページで、[トークンローテーションによる高度なトークンセキュリティ] オプションを選択します。
5. 「OAuth および許可」ページの「リダイレクト URL」セクションに、次の形式の URL を追加します。

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

   この URL AWS リージョン では、 *<region>*は AppFabric アプリケーションバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2` です。
6. `auditLogs:read` の範囲では、アプリのパブリックディストリビューションを有効にする必要があります。詳しくは、「Slack」 ウェブサイトの[パブリックディストリビューションの有効化]を参照してください。

必要範囲

> **Note**
>
> このセクションは、OAuth アプリをゼロから作成することを選択した場合にのみ適用されます。アプリマニフェストを使用してアプリケーション認証を作成することを選択した場合は、このセクションをスキップしてください。

Slack OAuthアプリケーションの「 OAuth および許可」ページで次のユーザートークンの範囲を追加する必要があります。

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

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はSlackワークスペース ID です。テナント ID を取得するには、Slack ウェブサイトの「Slackヘルプセンター」にある「SlackURLの検索 」の手順に従ってください。Slack ワークスペース URL の形式は、`examplecorp.slack.com` または `examplecorp.enterprise.slack.com` に似ています。必要なテナント ID は、`.slack.com` または `.enterprise.slack.com` が付いていない `examplecorp` です。

テナント名

Slack ワークスペース ID を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリケーション認証とアプリケーション認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric は、OAuth アプリケーションからクライアント ID Slack をリクエストします。クライアント ID を確認するには、以下のステップに従います。

1. ブラウザでSlackアプリ管理 UI に移動します。
2. で使用する OAuth アプリケーションを選択します AppFabric。
3. 「基本情報」ページのクライアント ID を のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric は、OAuth Slack アプリケーションにクライアントシークレットをリクエストします。クライアントシークレット を確認するには、以下の手順に従います。

1. ブラウザでSlackアプリ管理 UI に移動します。
2. で使用する OAuth アプリケーションを選択します AppFabric。

3. 基本情報ページから のクライアントシークレットフィールドにクライアントシークレットを入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されSlack、承認が承認されます。 AppFabric 承認を承認するには、許可 を選択します。

Smartsheet

Smartsheet は、企業全体で仕事、人材、テクノロジーを連携させる上で役立つワークマネジメントプラットフォームです。 Smartsheet は誰もがプロジェクト管理、ワークフローの自動化、大規模なソリューションの迅速な構築を行えるように支援するエンタープライズグレードの堅牢な機能セットを提供し、セキュリティとコンプライアンスを維持しながらイノベーションを実現する環境を作り出します。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信し Smartsheet、データをオープンサイバーセキュリティスキーマフレームワーク (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Smartsheet
- Smartsheet アカウント AppFabric への接続

AppFabric のサポート Smartsheet

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますSmartsheet。

前提条件

AppFabric を使用して からサポートされている宛先Smartsheetに監査ログを転送するには、次の要件を満たす必要があります。

- Smartsheet ビジネス、エンタープライズ、またはアドバンスアカウントが必要です。Smartsheet アカウントの作成またはアップグレードの詳細については、Smartsheet ウェブサイトの「Smartsheet価格設定」または「Smartsheetアドバンス」を参照してください。
- Smartsheet開発者登録プロセスを完了する必要があります。

レート制限に関する考慮事項

Smartsheet は、Smartsheet API にレート制限を課します。Smartsheet API レート制限の詳細については、[Smartsheet ウェブサイトの Smartsheet API リファレンス」の「レート制限」を参照してください。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Smartsheet アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますSmartsheet。Smartsheet で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth Smartsheetを使用して と統合します。Smartsheet で OAuth アプリケーションを作成するには、以下の手順に従います。

1. Smartsheet アカウントの開発者ツールに移動します。
2. 開発者ツールの画面で、[新規アプリの作成] を選択します。
3. [新規アプリの作成] 画面のすべての入力フィールドに入力します。
4. [アプリの URL] と [アプリの連絡先/サポート] には任意の一意の値を使用してください。
5. 次の形式のリダイレクト URL をアプリリダイレクト URL として使用します。

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

   この URL AWS リージョン では、 *<region>*は AppFabric アプリケーションバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://us-east-1.console.aws.amazon.com/appfabric/oauth2` です。
6. [保存] を選択します。
7. アプリクライアント ID およびアプリシークレットをコピーして保存します。

必要範囲

Smartsheet では、OAuth 設定にスコープを明示的に追加する必要はありません。 AppFabric は、Smartsheetアカウントに認証リクエストで次のスコープをリクエストします。

- `READ_EVENTS`
- `READ_USERS`

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric は、 Smartsheetアカウント ID です。

テナント名

AppFabric はテナント ID をリクエストします。Smartsheet アカウントを一意に識別する任意の値を入力します。

クライアント ID

AppFabric はクライアント ID をリクエストします。のクライアント ID AppFabric はSmartsheet、アプリケーションクライアント ID です。Smartsheet でアプリクライアント ID を確認するには、以下の手順に従います。

1. Smartsheet アカウントの開発者ツールに移動します。
2. との接続に使用する OAuth アプリケーションを選択します AppFabric。
3. アプリプロファイル画面のアプリクライアント ID を のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。のクライアントシークレット AppFabric はSmartsheetアプリシークレットです。Smartsheet でアプリシークレットを確認するには、次のステップに従います。

1. Smartsheet アカウントの開発者ツールに移動します。

2. との接続に使用する OAuth アプリケーションを選択します AppFabric。
3. 「」の「アプリプロファイル」画面から「クライアントシークレット」フィールドにアプリシークレットを入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されSmartsheet、承認が承認されます。 AppFabric 承認を承認するには、許可 を選択します。

Terraform Cloud

HashiCorp Terraform Cloud は、世界中で最も広く使用されているマルチクラウドプロビジョニング製品です。Terraform エコシステムには、3,000 を超えるプロバイダー、14,000 のモジュール、2 億 5,000 万ダウンロードがあります。 Terraform CloudはTerraform、 を導入する最も速い方法です。 は、プラクティショナー、チーム、グローバル企業がインフラストラクチャの作成と共同作業を行い、セキュリティ、コンプライアンス、運用上の制約のリスクを管理するために必要なすべてを提供します。セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しTerraform Cloud、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Terraform Cloud
- Terraform Cloud アカウント AppFabric への接続

AppFabric のサポート Terraform Cloud

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますTerraform Cloud。

前提条件

AppFabric を使用して からサポートされている宛先Terraform Cloudに監査ログを転送するには、次の要件を満たす必要があります。

- 監査ログにアクセスするには、 Terraform Cloud Plus Edition プランがあり、組織の所有者である必要があります。Terraform Cloud プランの詳細については、 HashiCorp Terraformウェブサイトの「 のTerraform料金」を参照してください。

- TBD 監査ログは、Terraform Cloudアカウントから作成できる組織で使用できます。

レート制限に関する考慮事項

Terraform Cloud は、Terraform Cloud API にレート制限を課します。Terraform Cloud API レート制限の詳細については、 Terraform Cloudウェブサイトの「デベロッパー管理全般設定」の「API レート制限」を参照してください。 Terraform Cloud AppFabric と既存の Terraform Cloud API アプリケーションの組み合わせTerraform Cloudが の制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Terraform Cloud アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますTerraform Cloud。Terraform Cloud で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

組織 API トークンを作成する

AppFabric は、組織 API トークンTerraform Cloudを使用して と統合します。Terraform Cloud 組織 API トークンの詳細については、「組織 API トークン」を参照してください。組織を作成するには、「Creating Organizations」の手順に従います。で組織 API トークンを作成するにはTerraform Cloud、次のステップに従います。

1. Terraform Cloud サインインページに移動してサインインします。
2. 左側のパネルで組織 、設定 を選択し、API トークン を選択します。
3. 組織トークン で、組織トークンの作成 を選択し、トークンの生成 を選択します。
4. (オプション) トークンの有効期限日または時刻を入力するか、有効期限のないトークンを作成します。
5. トークンをコピーして保存します。これは、 で後ほど必要になります AppFabric。トークンを保存する前にページを閉じる場合は、古いトークンを取り消して新しいトークンを作成する必要があります。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。Terraform Cloud アカウントのテナント ID は、アカウントの現在の組織 URL です。これは、Terraform Cloud組織にログインし、現在の組織の URL をコピーすることで確認できます。テナント ID は、次のいずれかの形式に従っている必要があります。

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

テナント名

この一意の Terraform Cloud 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

サービスアカウントトークン

AppFabric はサービスアカウントトークンをリクエストします。のサービスアカウントトークン AppFabric は、 で作成した組織 API トークンです組織 API トークンを作成する。

Webex by Cisco

Cisco は、インターネットを支えるテクノロジーの世界的リーダーです。Cisco はアプリケーションの新たな概念をもたらし、データを保護し、インフラストラクチャを変革させ、グローバルでインクルーシブな未来に向けてチームを強化することで、新しい可能性を広げます。

Webex by Cisco について

Webex は、ビデオ会議、通話、メッセージング、イベント、コンタクトセンターや専用コラボレーションデバイスなどの顧客体験ソリューションを含む、クラウドベースのコラボレーションソリューションの大手プロバイダーです。Webex は、インクルーシブなコラボレーション体験を重視し、AI と機械学習を活用したイノベーションにより地理、言語、性格、テクノロジーへの精通度といった障壁を排除するイノベーションを推進しています。同社のソリューションは、そのセキュリティとプライバシーバイデザインに支えられています。Webex は、単一のアプリケーションとインターフェースを通じて世界をリードするビジネスアプリや生産性向上アプリとの連携を提供します。詳細については、「webex.com」を参照してください。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信しWebex、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon

Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Webex
- Webex アカウント AppFabric への接続

AppFabric のサポート Webex

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますWebex。

前提条件

AppFabric を使用して からサポートされている宛先Webexに監査ログを転送するには、次の要件を満たす必要があります。

- コラボレーションフレックスプラン、Meet プラン、Call プラン、またはそれ以上が必要です。該当する Webex プランタイプの作成またはアップグレードの詳細については、「Webex Web サイトのWebexすべての機能の価格表」を参照してください。
- いずれかの Cisco AuditLog APIs が提供するセキュリティ監査イベントにアクセスするには、アカウントに Pro Pack ライセンスが必要です。
- 組織管理者 > 完全な管理者権限を持つユーザが必要です。
- 完全な管理者権限を持つ管理者ロールの設定では、コンプライアンスオフィサーオプションが有効になっている必要があります。

レート制限に関する考慮事項

Webex は、Webex API にレート制限を課します。Webex API のレート制限の詳細については、Webex Web サイトの「Webex開発者ガイド」の「レート制限」を参照してください。AppFabric と既存の Webex API アプリケーションの組み合わせが制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Webex アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますWebex。Webex で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth Webexを使用して と統合します。Webex で OAuth アプリケーションを作成するには、以下の手順に従います。

1. 「Webex開発者ガイド」の「統合と認証」ページにある「統合の登録」セクションの指示に従ってください。
2. 次の形式のリダイレクト URL を使用します。

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

   この URL AWS リージョン では、 *<region>*は AppFabric アプリケーションバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2` です。

必要範囲

Webex OAuth アプリケーションに次の範囲を入力する必要があります。

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

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はWebex組織 ID です。Webex 組織 ID を確認する方法については、Webex ヘルプセンターウェブサイトの「CiscoWebexControl Hub で組織 ID を検索する」を参照してください。

テナント名

この一意のWebexインスタンスを識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証と、アプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はWebexクライアント ID をリクエストします。Webex クライアント ID を確認するには、以下のステップに従います。

1. https://developer.webex.com で Webex アカウントにサインインします。
2. 右上のアバターを選択します。
3. [My Webex アプリ] を選択します。
4. に使用する OAuth2 アプリケーションを選択します AppFabric。
5. このページのクライアント ID を のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric はWebexクライアントシークレットをリクエストします。 は、OAuth アプリケーションを最初に作成したときにクライアントシークレットを 1 回Webexだけ提示します。最初のクライアントシークレットを保存しなかった場合に新しいクライアントシークレットを生成するには、以下の手順に従います。

1. https://developer.webex.com で Webex アカウントにサインインします。
2. 右上のアバターを選択します。
3. [My Webex アプリ] を選択します。
4. に使用する OAuth2 アプリケーションを選択します AppFabric。
5. このページで、新しいクライアントシークレットを生成します。
6. 新しいクライアントシークレットを のクライアントシークレットフィールドに入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric 、 からポップアップウィンドウが表示されWebex、承認が承認されます。承認を承認する AppFabricには、 を受け入れるを選択します。

Zendesk

2007 年に世界中のあらゆる企業がカスタマーサービスをオンライン化できるようにすることで、Zendeskがカスタマーエクスペリエンス革命を始めました。現在では、Zendeskは、あらゆる場所ですべての人に優れたサービスを提供し、何十億もの会話を支えています。電話、チャット、電子メール、メッセージング、ソーシャルチャネル、コミュニティ、レビューサイト、ヘルプセンターを通じて、10万を超えるブランドと数億人の顧客をつなげています。 Zendesk製品は愛されるための愛を込めて作られています。同社はデンマークのコペンハーゲンで設立され、カリフォルニアで建設· 栽培され、現在では世界中で6,000人以上の従業員を雇用しています。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信し Zendesk、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Zendesk
- Zendesk アカウント AppFabric への接続

AppFabric のサポート Zendesk

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますZendesk。

前提条件

AppFabric を使用して からサポートされている宛先Zendeskに監査ログを転送するには、次の要件を満たす必要があります。

- ZendeskスイートエンタープライズアカウントエンタープライズプラスアカウントまたはZendeskSupport エンタープライズアカウントが必要です。Zendesk Enterprise アカウントの作成またはアップグレードについて詳しくは、ZendeskZendeskウェブサイトの「プランタイプの確認」を参照してください。
- Zendeskアカウントには管理者ロールを持つユーザーが必要です。ロールの詳細については、Zendeskウェブサイトの「Zendeskサポート ユーザーのロールについて」を参照してください。

レート制限に関する考慮事項

Zendesk は、Zendesk API にレート制限を課します。Zendesk API のレート制限の詳細については、Zendesk Web サイトの「Zendesk開発者ガイド」の「レート制限」を参照してください。AppFabric と既存の Zendesk API アプリケーションの組み合わせが制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に転送されるまでに最大 30 分の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。ただし、これはアカウントレベルでカスタマイズできる場合があります。サポートが必要な場合は、AWS Support にお問い合わせください。

Zendesk アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 で を承認 AppFabricする必要がありますZendesk。Zendesk で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

OAuth アプリケーションの作成

AppFabric は OAuth Zendeskを使用して と統合します。Zendeskでは、以下の設定で OAuth アプリケーションを作成する必要があります。

1. Zendeskサポート ebサイトの「アプリケーションでのOAuth認証の使用」の「WZendeskへのアプリケーションの登録」セクションの指示に従ってください。
2. 次の形式のリダイレクト URL を使用します。

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

   この URL AWS リージョン では、 *<region>*は AppFabric アプリケーションバンドルを設定した のコードです。例えば、米国東部 (バージニア北部) リージョンのコードは `us-east-1` です。そのリージョンのリダイレクト URL は `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2` です。

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はZendeskサブドメインです。Zendeskサブドメインを見つける方法について詳しくは、Zendesk Support Web サイトの「Zendeskサブドメインはどこで見つけられますか？」を参照してください。

テナント名

この一意の Zendesk 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。のクライアント ID AppFabric は Zendesk API の一意の識別子です。Zendesk 固有の識別子を見つけるには、次の手順に従います。

1. Zendeskアカウントの「管理センター」に移動します。
2. [アプリとインテグレーション] を選択します。
3. [API」, Zendesk[API] .を選択します。
4. [OAuth クライアント] タブを選択します。
5. 用に作成した OAuth アプリケーションを選択します AppFabric。
6. OAuth クライアントの一意の識別子を のクライアント ID フィールドに入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。のクライアントシークレット AppFabric はシーZendeskクレットトークンです。 は、OAuth アプリケーションを初めて作成するときに 1 Zendesk 回だけシークレットトークンZendeskを提示します。最初のシークレットトークンを保存しなかった場合に新しいシークレットトークンを生成するには、以下の手順に従います。

1. Zendeskアカウントの「管理センター」に移動します。
2. [アプリとインテグレーション] を選択します。
3. [API」, Zendesk[API] .を選択します。
4. [OAuth クライアント] タブを選択します。
5. 用に作成した OAuth アプリケーションを選択します AppFabric。
6. 「シークレットトークン」フィールドの横にある「再作成」ボタンを選択します。

7. 新しいシークレットトークンを のクライアントシークレットフィールドに入力します AppFabric。

認証を承認します

でアプリ認証を作成すると AppFabric、 からポップアップウィンドウが表示されZendesk、承認が承認されます。 AppFabric 承認を承認するには、許可 を選択します。

Zoom

Zoom は、ビジネスや個人にとってより簡単で、より没入型で、よりダイナミックな接続を可能にする all-in-one インテリジェントなコラボレーションプラットフォームです。 Zoomテクノロジーは、チームチャット、電話、会議、オムニチャネルクラウドコンタクトセンター、スマート録音、ホワイトボードなどのソリューションを通じて、有意義な接続を可能にし、最新のコラボレーションを促進し、人間のイノベーションを促進します。

セキュリティ AWS AppFabric のために を使用すると、 から監査ログとユーザーデータを受信し Zoom、データを Open Cybersecurity Schema Framework (OCSF) 形式に正規化し、Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose ストリームにデータを出力できます。

トピック

- AppFabric のサポート Zoom
- Zoom アカウント AppFabric への接続

AppFabric のサポート Zoom

AppFabric は、 からのユーザー情報と監査ログの受信をサポートしますZoom。

前提条件

AppFabric を使用して からサポートされている宛先Zoomに監査ログを転送するには、次の要件を満たす必要があります。

- Zoom のプロ、ビジネス、エデュケーション、またはエンタープライズプランに加入している必要があります。
- Zoom 管理者ロールには、 server-to-server OAuthアプリケーションを作成するアクセス許可が必要です。 server-to-server OAuth アプリケーションの有効化の詳細については、 Zoomウェブサイ

トの「 デベロッパーガイド」の「サーバー間のOAuthアクセス許可を有効にする」セクションを参照してください。 Zoom

- Zoom管理者ロールには、管理アクティビティログを表示したり、監査アクティビティにサインイン/サインアウトしたりする許可が必要です。監査アクティビティを閲覧する許可を有効にする方法の詳細については、Zoom サポートウェブサイトの「ロール管理の使用」と「管理者アクティビティログの使用」を参照してください。

レート制限に関する考慮事項

Zoom は にレート制限を課しますZoomAPI。Zoom API レート制限の詳細については、「 デベロッパーガイド」の「レート制限」を参照してください。 Zoom AppFabric と既存のZoomアプリケーションの組み合わせが制限を超えると、 に表示される監査ログが遅れ AppFabric る可能性があります。

データ遅延に関する考慮事項

監査イベントが取り込み先に配信されるまでに約 24 時間の遅延が発生する場合があります。これは、アプリケーションで利用できる監査イベントの遅延と、データ損失を減らすための予防措置によるものです。

Zoom アカウント AppFabric への接続

AppFabric サービス内でアプリケーションバンドルを作成したら、 AppFabric で を承認する必要がありますZoom。Zoom で を認証するために必要な情報を見つけるには AppFabric、次のステップに従います。

アプリケーションを作成する server-to-server OAuth

AppFabric は server-to-server OAuth、 と統合するためにアプリケーション認証情報で を使用しますZoom。でアプリケーションを作成するには server-to-server OAuthZoom、「 Zoomデベロッパーガイド」の「サーバー間OAuthアプリケーションの作成 AppFabric 」の手順に従ってください。 はZoomウェブフックをサポートしていません。ウェブフックサブスクリプションを追加するための セクションはスキップできます。

必要範囲

Zoom には、きめ細かなスコープ (新しく作成されたアプリケーションの場合) と従来のスコープ (以前に作成されたアプリケーションの場合) の 2 種類のスコープがあります。

Zoom server-to-server OAuth アプリケーションには、次の詳細なスコープを追加する必要があります。

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

以前に作成したアプリケーションを使用している場合は、次のクラシックスコープを追加する必要があります。

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

アプリ権限

テナント ID

AppFabric はテナント ID をリクエストします。のテナント ID AppFabric はZoomアカウント ID です。Zoom アカウント ID を確認するには、以下のステップに従います。

1. Zoom Marketplace にアクセスします。
2. [管理] を選択します。
3. に使用するアプリケーションを選択します server-to-server OAuth AppFabric。
4. アプリ認証情報ページのアカウント ID を のテナント ID フィールドに入力します AppFabric。

テナント名

この一意の Zoom 組織を識別する名前を入力します。 AppFabric はテナント名を使用して、アプリ認証とアプリ認証から作成された取り込みにラベルを付けます。

クライアント ID

AppFabric はクライアント ID をリクエストします。Zoom クライアント ID を確認するには、以下のステップに従います。

1. Zoom Marketplace にアクセスします。
2. [管理] を選択します。
3. に使用するアプリケーションを選択します server-to-server OAuth AppFabric。

4. アプリ認証情報ページから のクライアント ID フィールドにクライアント ID を入力します AppFabric。

クライアントシークレット

AppFabric はクライアントシークレットをリクエストします。Zoom クライアントシークレットを確認するには、以下のステップに従います。

1. Zoom Marketplace にアクセスします。
2. [管理] を選択します。
3. に使用するアプリケーションを選択します server-to-server OAuth AppFabric。
4. アプリ認証情報ページから のクライアントシークレットフィールドにクライアントシークレットを入力します AppFabric。

監査ログの配信

Zoom は、24 時間APIごとに にアクセスして監査ログを利用できるようにします。で監査ログを表示する場合 AppFabric、 に表示されるデータは前日のアクティビティZoomに関するものです。

互換性のあるセキュリティツールとサービス

AWS AppFabric for security は、以下のセキュリティツールおよびサービスとの統合をサポートしています。セキュリティが AppFabric 接続するように設定する方法の詳細については、サービスの名前を選択してください。

トピック

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

- Singularity Cloud
- Splunk

Barracuda XDR

Barracuda Networks は、ビジネスのジャーニーに合わせて成長し変化する革新的なソリューションにより、E メール、ネットワーク、データ、アプリケーションを保護する、クラウドファーストなセキュリティソリューションを提供している、信頼できるパートナーであり業界をリードするプロバイダーです。Barracuda XDR は、高度なテクノロジーと、セキュリティオペレーションセンター (SOC) のセキュリティアナリストチームとを組み合わせた、オープンな、拡張された、検知および対応ソリューションです。Barracuda XDR のプラットフォームは、40 を超える統合データソースの、一日数十億件に上る未加工のイベントを分析し、MITRE ATT&CK® フレームワークに対応した広範な脅威検出ルールとともに、これまでよりもスピーディに脅威を検出し、より短時間で対応します。

AWS AppFabric 監査ログの取り込みに関する考慮事項

以下のセクションでは、 で使用する AppFabric 出力スキーマ、出力形式、出力先について説明しますBarracuda XDR。

スキーマと形式

Barracuda XDR は、次の AppFabric 出力スキーマと形式をサポートしています。

- OCSF - JSON: Open Cybersecurity Schema Framework (OCSF) を使用してデータを AppFabric 正規化し、データを JSON 形式で出力します。

出力場所

Barracuda XDR は、Amazon Security Lake の監査ログの受信をサポートしています。から AppFabric にデータを送信するにはBarracuda XDR、以下の手順に従います。

1. Amazon Security Lake にデータを送信する: Amazon Data Firehose を介して Amazon Security Lake にデータ AppFabric を送信するように を設定します。詳細については、「Amazon Security Lake」を参照してください。
2. Barracuda XDR にデータを送信する: Amazon Security Lake から監査ログを受信するように Barracuda XDR を設定します。詳細については、「Setting Up and Using Amazon Security Lake」を参照してください。

Dynatrace

は、広範で深いオブザーバビリティと継続的なランタイムアプリケーションセキュリティを高度なAIOps とDynatrace® Platform組み合わせ、データからの回答とインテリジェントな自動化を提供します。これにより、イノベーターはクラウド運用を最新化および自動化し、ソフトウェアをより迅速かつ安全に提供し、完全なデジタルエクスペリエンスを確保できます。

AWS AppFabric 監査ログの取り込みに関する考慮事項

以下のセクションでは、 で使用する AppFabric 出力スキーマ、出力形式、出力先について説明しますDynatrace Platform。

スキーマと形式

は、次の AppFabric 出力スキーマと形式Dynatrace Platformをサポートしています。

- OCSF - JSON: Open Cybersecurity Schema Framework (OCSF) を使用してデータを AppFabric 正規化し、データを JSON 形式で出力します。

出力場所

は、次の AppFabric 出力場所からの監査ログの受信Dynatrace Platformをサポートします。

- Amazon Simple Storage Service (Amazon S3)
  - 監査ログを含む Amazon S3 バケットからデータDynatrace Platformを受信するように を設定するには、 の Dynatrace の S3 Log Forwarder プロジェクトの指示に従いますGitHub。

Logz.io

Logz.io は、オブザーバビリティとセキュリティを高コストで低価値の負担となるものから、より優れたビジネス成果を実現する高価値でコスト効率の高いものに変えることで、クラウドネイティブ企業がLogz.io Open 360 Platformを通して自社の環境を監視し保護できるよう、支援しています。

Logz.io クラウドSIEMは、高速クエリ、多次元検出、カスタマイズ可能で詳細なセキュリティコンテンツを通じて、データ過負荷や遍在するサイバースキルギャップなどの今日の主要なセキュリティ課題に直接対処し、データ量に関わらず、またパフォーマンスを低下させることなく、クラウド環境全体の監視と調査を支援します。

Logz.io ソリューションは、複雑さとコストを抑えながら、高度な脅威分析と調査を実現する目的で構築されました。ノイズが多いデータを減らすことを目的として備えられた専任のセキュリティアナ

リスト、サービスとしての脅威コンテンツ、AIベースの機能を活用することによって、チームは現実の脅威に迅速に対処するための有益な情報に集中できます。

AWS AppFabric 監査ログの取り込みに関する考慮事項

以下のセクションでは、 で使用する AppFabric 出力スキーマ、出力形式、出力先について説明しますLogz.io。

スキーマと形式

Logz.io は、次の AppFabric 出力スキーマと形式をサポートしています。

- Raw - JSON
  - AppFabric は、ソースアプリケーションで使用される元のスキーマのデータを JSON 形式で出力します。
- OCSF - JSON
  - AppFabric は Open Cybersecurity Schema Framework (OCSF) を使用してデータを正規化し、データを JSON 形式で出力します。

出力場所

Logz.io は、次の AppFabric 出力場所をサポートします。

- Amazon Data Firehose
  - Firehose 配信ストリームを設定して にデータを送信するにはLogz.io、「Amazon Data Firehose デベロッパーガイドLogz.io」の「送信先の選択」の手順に従います。
- Amazon Simple Storage Service (Amazon S3)
  - 監査ログを含む Amazon S3 バケットからデータを受信するように Logz.ioを設定するには、Logz.io ウェブサイトの「Amazon S3 バケットの設定」の手順に従ってください。

Netskope

サイバーセキュリティの世界的リーダーであるNetskopeは、組織がゼロトラストの原則を適用してデータを保護できるように、クラウド、データ、ネットワークのセキュリティを再定義しています。Netskope高速で使いやすいこのプラットフォームは、どこにいても、人、デバイス、データに最適なアクセスとゼロトラストセキュリティを提供します。 Netskopeはクラウド、ウェブ、プライベートアプリケーションのアクティビティにおいて、リスクの軽減、パフォーマンスの向

上、比類のない可視化を実現します。進化する脅威、新しいリスク、テクノロジーシフト、組織Netskopeやネットワークの変更、新しい規制要件に対応するために、25 を超えるフォーチュン 100 社を含む何千ものお客様が信頼し、その強力な NewEdge ネットワークを構築しています。お客様が SASE ジャーニーでどのような状況にも対応できるようにNetskope が支援する方法については、netskope.comをご覧ください。

AWS AppFabric 監査ログの取り込みに関する考慮事項

以下のセクションでは、 で使用する AppFabric 出力スキーマ、出力形式、出力先について説明しますNetskope。

スキーマと形式

Netskope は、次の AppFabric 出力スキーマと形式をサポートしています。

- Raw - JSON
  - AppFabric は、ソースアプリケーションで使用される元のスキーマのデータを JSON 形式で出力します。
- OCSF - JSON
  - AppFabric は Open Cybersecurity Schema Framework (OCSF) を使用してデータを正規化し、データを JSON 形式で出力します。

出力場所

Netskope は、次の AppFabric 出力場所をサポートします。

- Amazon Simple Storage Service (Amazon S3)
  - 監査ログを含む Amazon S3 Netskope バケットからデータを受信するように設定するには、Netskopeウェブサイトの「Amazon Web Services S3 のデータ保護」の指示に従ってください。

NetWitness

NetWitness は、Extended Detection and Response (XDR) ソフトウェアの大手開発業者です。セキュリティ意識の高い同社のグローバル顧客層は、巧妙で攻撃的な攻撃者に対する防御に NetWitness XDR を活用しています。デジタル攻撃を検知、調査、対応するための業界で最も完全で統合され、成熟したプラットフォームを備えた NetWitness XDR は、最新かつ効果的な SOC の統一基盤となっています。

高度にモジュール化されたアーキテクチャにより、NetWitness XDR はクラウド、オンプレミス、モバイルワーカーやリモートワーカーなど、発生場所や相手を問わず脅威を検出します。NetWitness Platform XDR は、適用された脅威インテリジェンスとユーザー行動分析を組み合わせて完全な可視性を提供し、脅威の検出、アクティビティの優先順位付け、調査、対応の自動化を可能にします。これらすべてに基づき、セキュリティアナリストはより優れた、より迅速な効率性をもって、ビジネスに影響を及ぼす脅威の先手を打つセキュリティ運用を実行できます。

AWS AppFabric 監査ログの取り込みに関する考慮事項

以下のセクションでは、 で使用する AppFabric 出力スキーマ、出力形式、出力先について説明しますNetWitness。

スキーマと形式

NetWitness は、次の AppFabric 出力スキーマと形式をサポートしています。

- Raw - JSON
  - AppFabric は、ソースアプリケーションで使用される元のスキーマのデータを JSON 形式で出力します。
- OCSF - JSON
  - AppFabric は Open Cybersecurity Schema Framework (OCSF) を使用してデータを正規化し、データを JSON 形式で出力します。

出力場所

NetWitness は、次の AppFabric 出力場所をサポートします。

- Amazon Simple Storage Service (Amazon S3)
  - 監査ログを含む Amazon S3 バケットからデータを受信するように NetWitness を設定するには、NetWitness ウェブサイトのNetWitnessプラットフォーム統合 ページにある S3 ユニバーサルコネクタイベントソースログ設定ガイドの指示に従ってください。

Amazon QuickSight

Amazon は、統合ビジネスインテリジェンス (BI) をハイパースケールで活用して、データ主導型の組織 QuickSight を強化します。を使用すると QuickSight、最新のインタラクティブダッシュボード、ページ分割レポート、埋め込み分析、自然言語クエリを通じて、すべてのユーザーが同じ信頼できるソースからさまざまな分析ニーズを満たすことができます。で AWS AppFabric 監査ログ

データを分析するには QuickSight、セキュリティログ AppFabric の がソースとして保存されている Amazon Simple Storage Service (Amazon S3) バケットを選択します。

AppFabric 監査ログの取り込みに関する考慮事項

以下のセクションでは、Amazon で使用する AppFabric 出力スキーマ、出力形式、出力先について説明します QuickSight。

スキーマと形式

QuickSight は、次の AppFabric 出力スキーマと形式をサポートしています。

- Raw - JSON
  - AppFabric は、ソースアプリケーションで使用される元のスキーマのデータを JSON 形式で出力します。
- OCSF - JSON
  - AppFabric は Open Cybersecurity Schema Framework (OCSF) を使用してデータを正規化し、データを JSON 形式で出力します。

出力場所

QuickSight は、次の AppFabric 出力場所をサポートします。

- Amazon S3
  - Amazon S3 ファイルを使用してデータセットを作成 QuickSight することで、Amazon S3 から に直接データを取り込むことができます。 Amazon S3 ターゲットファイルセットが QuickSight データソースクォータを超えないことを確認するには、Amazon QuickSight ユーザーガイドの「データソースクォータ」を参照してください。
  - ファイルセットが Amazon S3 データソースの QuickSight クォータを超える場合は、Amazon Athena とテーブルを使用して Amazon S3 にデータを取り込むことができます AWS Glue 。QuickSight データセットで Athena を使用すると、追加コストが発生します。Athena料金の詳細については、Athena料金表を参照ください。

    Athena を使用するには:

    1. Athena ユーザーガイド の「AWS Glue を使用してAmazon S3 のデータソースに接続する」の指示に従ってください。
    2. 「Amazon QuickSight ユーザーガイド」の「Athena データを使用したデータセットの作成」の手順に従います。

Rapid7

Rapid7, Inc. は、サイバーセキュリティをよりシンプルかつアクセスしやすいものにすることで、より安全なデジタル世界を構築することをミッションとしています。 は、セキュリティプロフェッショナルが best-in-class テクノロジー、最先端の研究、幅広い戦略的専門知識を通じて最新の攻撃領域を管理Rapid7できるようにします。 Rapid7の包括的なセキュリティソリューションは、10,000人を超える世界中のお客様がクラウドリスク管理と脅威検出を統合できるよう支援し、攻撃領域を減らし、脅威を迅速かつ正確に排除します。

AWS AppFabric 監査ログの取り込みに関する考慮事項

以下のセクションでは、 で使用する AppFabric 出力スキーマ、出力形式、出力先について説明しますRapid7。

スキーマと形式

Rapid7 は、次の AppFabric 出力スキーマと形式をサポートしています。

- Raw - JSON
  - AppFabric は、ソースアプリケーションで使用される元のスキーマのデータを JSON 形式で出力します。
- OCSF - JSON
  - AppFabric は Open Cybersecurity Schema Framework (OCSF) を使用してデータを正規化し、データを JSON 形式で出力します。

出力場所

Rapid7 は、次の AppFabric 出力場所をサポートします。

- Amazon Simple Storage Service (Amazon S3)
  - 監査ログを含む Amazon S3 バケットからデータを受信するように Rapid7 を設定するには、Rapid7 ブログウェブサイトの「InsightIDR で Amazon S3 アクティビティを監視する方法」ブログ投稿の指示に従ってください。

Amazon Security Lake

Amazon Security Lake は、 AWS 環境、Software as a Service (SaaS) プロバイダー、オンプレミス、クラウドソースのセキュリティデータを、 に保存されている専用のデータレイクに自動的に一元化します AWS アカウント。Security Lake を使用すると、組織全体のセキュリティデータをより

完全に把握できます。Security Lake は、オープンソースのセキュリティイベントスキーマであるオープンサイバーセキュリティスキーマフレームワーク (OCSF) を採用しています。OCSF サポートにより、このサービスは からのセキュリティデータと幅広いエンタープライズセキュリティデータソースを正規化 AWS し、組み合わせます。

AppFabric 監査ログの取り込みに関する考慮事項

Security Lake にカスタムソースを追加 AWS アカウント することで、 の Amazon Security Lake に SaaS 監査ログを取得できます。以下のセクションでは、Security AppFabric Lake で使用する出力スキーマ、出力形式、出力先について説明します。

スキーマと形式

Security Lake は、次の AppFabric 出力スキーマと形式をサポートしています。

- OCSF - JSON
  - AppFabric は Open Cybersecurity Schema Framework (OCSF) を使用してデータを正規化し、データを JSON 形式で出力します。

出力場所

Security Lake は、Amazon Data Firehose 配信ストリームを AppFabric 取り込み出力場所 AppFabric として使用して、カスタムソースとして をサポートします。 AWS Glue テーブルと Firehose 配信ストリームを設定し、Security Lake でカスタムソースを設定するには、以下の手順に従います。

AWS Glue テーブルを作成する

1. Amazon Simple Storage Service (Amazon S3) に移動し、任意の名前を付けたバケットを作成します。
2. AWS Glue コンソールに移動します。
3. [データカタログ] の場合は、[テーブル] セクションに移動し、[テーブルの追加] を選択します。
4. このテーブルに任意の名前を付けます。
5. ステップ 1 で作成した Amazon S3 バケットを選択します。
6. データ形式には [JSON] を選択し、[次へ] を選択します。
7. [スキーマの選択または定義] ページで、[スキーマを JSON として編集] を選択します。
8. 次のスキーマを入力し、 AWS Glue テーブル作成プロセスを完了します。

```
[
```

```
    {
        "Name": "activity_id",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "activity_name",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "actor",
        "Type":
"struct<session:struct<created_time:bigint,uid:string,issuer:string>,user:struct<uid:strin
        "Comment": ""
    },
    {
        "Name": "user",
        "Type":
"struct<uid:string,email_addr:string,credential_uid:string,name:string,type:string>",
        "Comment": ""
    },
    {
        "Name": "group",
        "Type":
"struct<uid:string,desc:string,name:string,type:string,privileges:array<string>>",
        "Comment": ""
    },
    {
        "Name": "privileges",
        "Type": "array<string>",
        "Comment": ""
    },
    {
        "Name": "web_resources",
        "Type":
"array<struct<type:string,uid:string,name:string,data:struct<current_value:string,previous
    },
    {
        "Name": "http_request",
        "Type": "struct<http_method:string,user_agent:string,url:string>",
        "Comment": ""
    },
    {
```

```
            "Name": "auth_protocol",
            "Type": "string",
            "Comment": ""
        },
        {
            "Name": "auth_protocol_id",
            "Type": "int",
            "Comment": ""
        },
        {
            "Name": "category_name",
            "Type": "string",
            "Comment": ""
        },
        {
            "Name": "category_uid",
            "Type": "string",
            "Comment": ""
        },
        {
            "Name": "class_name",
            "Type": "string",
            "Comment": ""
        },
        {
            "Name": "class_uid",
            "Type": "string",
            "Comment": ""
        },
        {
            "Name": "is_mfa",
            "Type": "boolean",
            "Comment": ""
        },
        {
            "Name": "raw_data",
            "Type": "string",
            "Comment": ""
        },
        {
            "Name": "severity",
            "Type": "string",
            "Comment": ""
        },
```

```
    {
        "Name": "severity_id",
        "Type": "int",
        "Comment": ""
    },
    {
        "Name": "status",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "status_detail",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "status_id",
        "Type": "int",
        "Comment": ""
    },
    {
        "Name": "time",
        "Type": "bigint",
        "Comment": ""
    },
    {
        "Name": "type_name",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "type_uid",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "description",
        "Type": "string",
        "Comment": ""
    },
    {
        "Name": "metadata",
        "Type":
 "struct<product:struct<uid:string,vendor_name:string,name:string>,processed_time:string,ve
```

```
    },
    {
        "Name": "device",
        "Type":
 "struct<uid:string,hostname:string,ip:string,name:string,region:string,type:string,os:stru
    },
    {
        "Name": "unmapped",
        "Type": "map<string,string>"
    }
]
```

Security Lake でカスタムソースを作成します

1. Amazon Security Lake コンソールに移動します。
2. ナビゲーションペインで [カスタムソース] を選択します。
3. [カスタムソースの作成] を選択します。
4. カスタムソースの名前を入力し、適用可能な OCSF イベントクラスを選択します。

> **Note**
>
> AppFabric は、アカウント変更 、認証 、ユーザーアクセス管理 、グループ管理 、ウェブリソースアクティビティ 、およびウェブリソースアクセスアクティビティイベントクラスを使用します。

5. AWS アカウント ID と外部 ID の両方に ID を入力します AWS アカウント 。続いて、[作成] を選択します。
6. カスタムソースの Amazon S3 の場所を保存します。これを使用して Amazon Data Firehose 配信ストリームを設定します。

Firehose で配信ストリームを作成する

1. Amazon Data Firehose コンソールに移動します。
2. [配信ストリームの作成] を選択します。
3. [ソース] には、[ダイレクト PUT] を選択します。
4. [宛先] には、[S3] を選択します。

5. [レコードの転換と変換] セクションで、[レコード形式の変換を有効にする]を選択し、出力形式として Apache Parquet を選択します。
6. AWS Glue テーブル で、前の手順で作成した AWS Glue テーブルを選択し、最新バージョンを選択します。
7. [宛先の設定] には、 Security Lake カスタムソースで作成した Amazon S3 バケットを選択します。
8. [動的パーティショニング] には、[有効] を選択します。
9. [JSON のインライン解析] には、[有効] を選択します。
   - [キー名] には、`eventDayValue` と入力します。
   - [JQ 式] には、`(.time/1000)|strftime("%Y%m%d")` と入力します。
10. [S3 バケットプレフィックス] には、以下の値を入力します。

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

    <region> と *<account_id>* を AWS リージョン と AWS アカウント ID に置き換えます。
11. [S3 バケットエラー出力プレフィックス] には、以下の値を入力します。

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

12. [再試行時間] には、 300 を選択します。
13. [バッファサイズ] には、 [128 MiB] を選択します。
14. [バッファ間隔] には、 60秒 を選択します。
15. Firehose 配信ストリームの作成プロセスを完了します。

AppFabric 取り込みの作成

Amazon Security Lake にデータを送信するには、前に作成した Firehose 配信ストリームを出力場所として使用する取り込みをコンソールで AppFabric作成する必要があります。Firehose を出力場所として使用する AppFabric ように取り込みを設定する方法の詳細については、「出力場所の作成」を参照してください。

Singularity Cloud

このSingularity Cloudプラットフォームは、すべての段階で、すべてのカテゴリの脅威から企業を保護します。その特許取得済みの AI (人工知能) は、既知のシグネチャやパターンから、ゼロデイ攻撃やランサムウェアなどの最も高度な攻撃にセキュリティを拡張します。

AWS AppFabric 監査ログの取り込みに関する考慮事項

以下のセクションでは、 で使用する AppFabric 出力スキーマ、出力形式、出力先について説明しますSingularity Cloud。

スキーマと形式

Singularity Cloud は、次の AppFabric 出力スキーマと形式をサポートしています。

OCSF - JSON: Open Cybersecurity Schema Framework (OCSF) を使用してデータを AppFabric 正規化し、データを JSON 形式で出力します。

出力場所

Singularity Cloud は、次の AppFabric 出力場所からの監査ログの受信をサポートします。

- Amazon Simple Storage Service (Amazon S3)
  - 監査ログを含む Amazon S3 バケットからデータSingularity Cloudを受信するように を設定するには、 Singularity Cloud’sドキュメントの指示に従います。

Splunk

Splunkは組織のレジリエンスを高めるのに役立ちます。主要組織は、Splunkのセキュリティとオブザーバビリティの統合プラットフォームを使用して、デジタルシステムの安全性と信頼性を維持しています。セキュリティ、インフラストラクチャ、アプリケーションの問題が重大なインシデントになるのを防ぎ、デジタルの混乱による衝撃を吸収し、デジタルトランスフォーメーションを加速するために、組織は Splunk を信頼しています。

AWS AppFabric 監査ログの取り込みに関する考慮事項

以下のセクションでは、 で使用する AppFabric 出力スキーマ、出力形式、出力先について説明しますSplunk。

スキーマと形式

Splunk では、次の AppFabric 出力スキーマと形式がサポートされています。

- Raw - JSON
  - AppFabric は、ソースアプリケーションで使用される元のスキーマのデータを JSON 形式で出力します。
- OCSF - JSON
  - AppFabric は Open Cybersecurity Schema Framework (OCSF) を使用してデータを正規化し、データを JSON 形式で出力します。
- OCSF-Parquet
  - AppFabric は、オープンサイバーセキュリティスキーマフレームワーク (OCSF) を使用してデータを正規化し、 Apache Parquet形式でデータを出力します。

出力場所

Splunk は、次の AppFabric 出力場所をサポートします。

- Amazon Data Firehose
  - 監査ログを含む Firehose ストリームから監査ログSplunkを受信するように を設定するには、SplunkウェブサイトのSplunk「Amazon Data Firehose 用アドオン」の手順に従います。
- Amazon Simple Storage Service (Amazon S3)
  - 監査ログを含む Amazon S3 バケットからデータを受信するようにSplunkを設定するには、Splunkウェブサイトの「AWS用SplunkアドオンのSQS ベースの S3 入力の設定」の手順に従ってください。

セキュリティリソース AWS AppFabric の削除

セキュリティ AWS AppFabric のために を引き続き使用しない場合は、追加料金が発生しないように、セットアップ時に作成した出力場所のデータとセキュリティリソース AppFabric の を削除してください。 AppFabric リソースをクリーンアップするには、Software as a Service (SaaS) アプリケーションごとにリソースを作成した逆の順序でリソースを削除する必要があります。取り込み先 > 取り込み先 > アプリ認証 > アプリバンドル

最後のアプリ認証を削除した後、アプリバンドルを削除できます。

トピック

- 取り込み先の削除
- 取り込みの削除

- アプリ認証の削除
- アプリバンドルの削除

取り込み先の削除

取り込みの作成時に出力場所を選択すると、セキュリティ AppFabric 上、 がユーザーに代わって取り込み先を作成します。取り込み先を削除するには、以下の手順に従います。

1. https://console.aws.amazon.com/appfabric/ で AppFabric コンソールを開きます。
2. 「はじめに」ページで、左側のメニューを展開します。
3. 「取り込み」を選択します。
4. アプリ認証を選択します。
5. 削除する取り込み先の横にあるオプションボタンを選択し、[削除] を選択します。
6. 取り込み先ダイアログボックスで、[削除] を選択して確定します。
7. すべての取り込み先で上記の手順を繰り返します。

取り込みの削除

取り込みを削除するには、次の手順に従います。

1. 「はじめに」ページで、左側のメニューを展開します。
2. 「取り込み」を選択します。
3. アプリ認証の横にあるオプションボタンを選択します。
4. [アクション] ドロップダウンメニューを選択します。
5. [削除] を選択します。
6. 取り込みの削除ダイアログボックスで、[削除] を選択して確定します。

アプリ認証の削除

アプリ認証を削除するには、次の手順に従います。

1. 「はじめに」ページで、左側のメニューを展開します。
2. [アプリ認証] を選択します。
3. 削除したいアプリ認証の横にあるオプションボタンを選択します。

4. [アクション] ドロップダウンメニューを選択します。
5. [削除] を選択します。
6. 取り込みの削除ダイアログボックスで、[削除] を選択して確定します。

アプリバンドルの削除

アプリバンドルを削除するには、次の手順に従います。

1. 「はじめに」ページで、左側のメニューを展開します。
2. [アプリバンドル] を選択します。
3. [削除] ボタンを選択します。
4. [delete] と入力して確定し、[削除]を選択します。

for AWS AppFabric productivity とは

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

> **Note**
>
> Amazon Bedrock を搭載: AWS 自動不正使用検出を実装。 AWS AppFabric for productivity は Amazon Bedrock 上に構築されているため、ユーザーは Amazon Bedrock に実装されているコントロールを継承して、AI の安全性、セキュリティ、責任ある使用を強制します。

AWS AppFabric for productivity (プレビュー) は、複数のアプリケーションからコンテキストを使用してインサイトとアクションを生成することで、サードパーティーアプリケーションのエンドユーザーの生産性を再考するのに役立ちます。アプリケーションデベロッパーは、他のアプリケーションのユーザーデータにアクセスすることがアプリケーションの生産性を高めるうえで重要であることを認識していますが、各アプリケーションとの統合を構築して管理することは望んでいません。AppFabric for productivity を使用すると、アプリケーションデベロッパーは、アプリケーション間のデータインサイトとアクションを生成する生成 AI を活用した APIs にアクセスできるため、新規または既存の生成 AI アシスタントを通じてより豊富なエンドユーザーエクスペリエンスを提供できます。 AppFabric for productivity は、複数のアプリケーションのデータを統合するため、デベロッパーが point-to-point 統合を構築または維持する必要がなくなります。アプリケーションデベロッパー

は、生産性 AppFabric 向上のためにアプリケーションの UI に直接埋め込むことができ、エンドユーザーの一貫したエクスペリエンスを維持しながら、他のアプリケーションから関連するコンテキストを表示できます。

AppFabric for productivity はAsana、、、Atlassian Jira Suite、、、Google Workspace、 など Microsoft 365MiroSlackSmartsheet、一般的に使用されるアプリケーションのデータを接続します。AppFabric for productivity を使用すると、アプリデベロッパーは、ユーザーの導入、満足度、ロイヤルティを向上させる、よりパーソナライズされたアプリエクスペリエンスを簡単に構築できます。一方でエンドユーザーは、さまざまなアプリケーションを横断して、必要とするインサイトに作業の流れを止めることなくアクセスできるようになります。

トピック

- 利点
- ユースケース
- for productivity AppFabric へのアクセス
- アプリケーションデベロッパー AppFabric 向けの for productivity (プレビュー) の開始方法
- エンドユーザー AppFabric 向けの for productivity (プレビュー) の開始方法
- AppFabric productivity APIs
- データ処理

利点

AppFabric for productivity を使用すると、アプリケーションデベロッパーは、アプリケーション間のデータインサイトとアクションを生成する APIs にアクセスできるため、新規または既存の生成 AI アシスタントを通じてより豊富なエンドユーザーエクスペリエンスを提供できます。

- クロスアプリケーションユーザーデータの単一ソース: 生産性 AppFabric 向上のため、複数のアプリケーションのデータが統合されるため、デベロッパーが point-to-point 統合を構築または維持する必要がなくなります。SaaS アプリケーションのデータは、異質なデータタイプを、どのアプリケーションにも理解可能な形式に自動的に正規化することで、他のアプリケーションで使用できるように処理されます。これにより、アプリケーションのデベロッパーはより多くのデータを組み込んでエンドユーザーの生産性を高めることができます。
- ユーザーエクスペリエンスの完全制御: 開発者は生産性向上 AppFabric のためにアプリケーションの UI に直接埋め込み、ユーザーエクスペリエンスを完全に制御しながら、アプリケーション全体からのコンテキストを使用して、パーソナライズされたインサイトと推奨アクションをエンドユーザーに提供します。これにより AppFabric 、エンドユーザーが優先する SaaS アプリケーション

で生産性向上を実現でき、タスクの完了を希望するアプリからアクセスできます。それにより、アプリケーションを切り替える手間を省いて時間を節約し、作業の流れを常に把握することが可能になります。

- 市場投入までの時間の短縮: アプリケーションデベロッパーは、モデルを微調整したり、カスタムプロンプトを作成したり、複数のアプリケーションの統合を構築したりすることなく、生成されたユーザーのデータに関するユーザーレベルのインサイトを 1 回の API コールで受け取ることができます。この複雑さ AppFabric を解消して、アプリケーションデベロッパーが生成 AI 機能をより迅速に構築、埋め込み、強化できるようにします。それによりアプリケーションデベロッパーは、最も重要なタスクにリソースを集中させることが可能になります。
- ユーザーの信頼を構築するためのアーティファクトリファレンス: 出力の一部として、生産性 AppFabric 向上のためには、LLM 出力でエンドユーザーの信頼を構築するためのインサイトを生成するために使用される関連するアーティファクトまたはソースファイルが表示されます。
- ユーザーのアクセス許可の簡素化: インサイトの生成に使用されるユーザーアーティファクトは、ユーザーがアクセスできる内容に基づいています。生産性 AppFabric 向上のためには、ISV のアクセス許可とアクセスコントロールが信頼できる情報源として使用されます。

ユースケース

アプリケーションデベロッパーは、生産性 AppFabric 向上のために を使用して、アプリケーション内の生産性を再考できます。 AppFabric for productivity には、エンドユーザーの生産性を高めるために、次のユースケースに焦点を当てた 2 APIs が用意されています。

- 1 日の作業の優先付け
  - 実行可能なインサイト API は、アプリケーション (E メール、カレンダー、メッセージ、タスクなど) を横断してタイムリーにインサイトを表示することで、1 日の業務を効率よく管理することを可能にする API です。さらにユーザーは、メール作成、会議のスケジュール設定、アクションアイテムの作成といったアプリケーションを横断したアクションを、自分が選んだアプリケーションから実行することができます。例えば、夜間にカスタマーエスカレーションを受けた従業員は、夜間の会話の要旨を確認できるだけでなく、推奨されるアクションを確認して、その顧客のアカウントマネージャーとのミーティングを設定することもできます。アクションの必須フィールド (タスク名、所有者、メールの送信者/受信者など) は自動入力され、入力された内容はアクションの実行前に編集することが可能です。
- 次回のミーティングの準備
  - 会議準備の API は、会議の内容を要約したり、E メールやメッセージその他のアプリケーションを横断して関連性の高いアーティファクトを表示したりすることで、会議に向けた準備に役立

つ API です。ユーザーはすぐに会議に向けた準備ができ、コンテンツを見つけるためにアプリケーション間を切り替える手間が省けます。

for productivity AppFabric へのアクセス

AppFabric for productivity は現在プレビュー版としてリリースされており、米国東部 (バージニア北部) で利用可能です。 AWS リージョンの詳細については AWS リージョン、「」のAWS AppFabric「 エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

各リージョンで、次のいずれかの方法で AppFabric for productivity にアクセスできます。

- アプリケーションデベロッパーとして
  - アプリケーションデベロッパー AppFabric 向けの for productivity (プレビュー) の開始方法
- エンドユーザーとして
  - エンドユーザー AppFabric 向けの for productivity (プレビュー) の開始方法

アプリケーションデベロッパー AppFabric 向けの for productivity (プレビュー) の開始方法

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

このセクションでは、アプリデベロッパーが生産性 AWS AppFabric 向上 (プレビュー) のためにアプリケーションに統合するのに役立ちます。生産性 AWS AppFabric 向上のため、デベロッパーは、複数のアプリケーションにわたって E メール、カレンダーイベント、タスク、メッセージなどから AI を活用したインサイトやアクションを生成することで、ユーザーにとってよりリッチなアプリケーションエクスペリエンスを構築できます。サポートされているアプリケーションのリストについては、AWS AppFabric「サポートされているアプリケーション」を参照してください。

AppFabric for productivity は、アプリケーションデベロッパーが安全で制御された環境で構築および実験するためのアクセスを提供します。生産性向上 AppFabric のために を初めて使い始めるときは、 を作成し AppClient 、1 人のテストユーザーを登録します。このアプローチは、アプリケーションと 間の認証と通信の流れを理解してテストするのに役立つように設計されています AppFabric。1 人のユーザーでテストした後、追加のユーザーにアクセスを拡張する前に、検証 AppFabric のためにアプリケーションを に送信できます (「」を参照Step 5. アプリケーションの検証 AppFabric をリクエストする)。 AppFabric は、アプリケーション情報を検証してから、アプリケーションデベ

ロッパー、エンドユーザー、およびそれらのデータを保護するために広範囲に導入できるようにします。これにより、責任ある方法でユーザー導入を拡大する方法が開かれます。

トピック

- 前提条件
- Step 1. for productivity AppFabric を作成する AppClient
- Step 2. アプリケーションを認証し承認する
- ステップ 3。 AppFabric ユーザーポータル URL をアプリケーションに追加する
- ステップ 4。を使用して AppFabric クロスアプリケーションインサイトとアクションを表示する
- Step 5. アプリケーションの検証 AppFabric をリクエストする
- 生産性向上 AppFabric のための の管理 AppClients
- トラブルシューティング

前提条件

開始する前に、 を作成する必要があります AWS アカウント。詳細については、「にサインアップする AWS アカウント」を参照してください。また、以下に示す IAM ポリシーにアクセスできるユーザーを少なくとも "appfabric:CreateAppClient" 1 人作成する必要があります。これにより、ユーザーは にアプリケーションを登録できます AppFabric。for productivity 機能のアクセス許可の付与の詳細については、 AppFabric 「」を参照してくださいAppFabric for productivity IAMポリシーの例。管理ユーザーを作成しておくことは何かと便利ですが、初期設定ではその作成は必須ではありません。詳細については、「管理アクセスを持つユーザーを作成する」を参照してください。

AppFabric for productivity は、プレビュー中に米国東部 (バージニア北部) でのみ使用できます。以下のステップを開始する前に、ご自身の現在地がこの地域であることを確認します。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
```

```
}
```

Step 1. for productivity AppFabric を作成する AppClient

アプリケーション内で生産性に関するインサイト AppFabric を得るには、 を作成する必要があります AppFabric AppClient。 AppClient は基本的に生産性 AppFabric 向上のための へのゲートウェイであり、アプリケーションと 間の安全な通信を可能にする安全な OAuth アプリケーションクライアントとして機能します AppFabric。を作成すると AppClient、 がアプリケーションと で動作していること AppFabric を確実に認識するために重要な一意の識別子である AppClient ID が提供されます AWS アカウント。

AppFabric for productivity は、アプリケーションデベロッパーが安全で制御された環境で構築および実験するためのアクセスを提供します。生産性向上 AppFabric のために を初めて使い始めるときは、 AppClientを作成し、1 人のテストユーザーを登録します。このアプローチは、アプリケーションと 間の認証と通信の流れを理解してテストするのに役立つように設計されています AppFabric。1 人のユーザーでテストした後、追加のユーザーにアクセスを拡張する前に、検証 AppFabric のためにアプリケーションを に送信できます (「」を参照Step 5. アプリケーションの検証 AppFabric をリクエストする)。 AppFabric は、アプリケーション情報を検証してから、アプリケーションデベロッパー、エンドユーザー、およびそれらのデータを保護するために広範囲に導入できるようにします。これにより、責任ある方法でユーザー導入を拡大する方法が開かれます。

を作成するには AppClient、 API オペレーションを使用します AWS AppFabric `CreateAppClient`。 AppClient 後で を更新する必要がある場合は、 `UpdateAppClient` API オペレーションを使用して redirectUrls のみ変更できます。appName や description AppClient など、 に関連付けられている他のパラメータを変更する必要がある場合は、 を削除 AppClient して新しいパラメータを作成する必要があります。詳細については、「CreateAppClient」を参照してください。

Python、Node.js、Java、C#、Go、Rust など、複数のプログラミング言語`CreateAppClient`を使用して API を使用して AWS サービスにアプリケーションを登録できます。詳細については、「IAM ユーザーガイド」の「リクエスト署名の例」を参照してください。この API オペレーションを実行するには、アカウント署名バージョン 4 の認証情報を使用する必要があります。署名バージョン 4 の詳細については、「IAM ユーザーガイド」の AWS 「 API リクエストの署名」を参照してください。

リクエストフィールド

- `appName` - ユーザー AppFabric ポータルの同意ページに表示されるアプリケーションの名前。同意ページでは、アプリケーション内に AppFabric インサイトを表示するアクセス許可をエンド

ユーザーに要求します。同意ページの詳細については、「Step 2. インサイトを表示することをアプリに許可する」を参照してください 。

- `description` - アプリケーションの説明です。
- `redirectUrls` - 承認後にエンドユーザーがリダイレクトされる URI です。redirectUrls は 5 個まで追加できます。例えば、`https://localhost:8080` などです。
- `starterUserEmails` - アプリケーションが検証されるまでの間、インサイトを受け取るためのアクセスが許可されるユーザーの E メールアドレスです。使用できるアドレスは 1 つのみです。例えば、次のようになります: `anyuser@example.com`
- `customerManagedKeyIdentifier` (オプション) - データの暗号化に使用されるカスタマーマネージドキー (KMS が生成) の ARN です。指定しない場合、 AWS AppFabric マネージドキーが使用されます。 AWS 所有のキー およびカスタマーマネージドキーの詳細については、「AWS Key Management Service 開発者ガイド」の「カスタマーキーと AWS キー」を参照してください。

レスポンスフィールド

- `appClientArn` - AppClient ID を含む Amazon リソースネーム (ARN)。例えば、 AppClient ID はです`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。
- `verificationStatus` - AppClient 検証ステータス。
  - `pending_verification` - の検証は AppClientでまだ進行中です AppFabric。が検証されるまで、 を使用できるユーザー (で指定`starterUserEmails`) AppClient は 1 人のみです AppClient。ユーザーは、 で導入された AppFabric ユーザーポータルに通知が表示されステップ 3。 AppFabric ユーザーポータル URL をアプリケーションに追加する、アプリケーションが検証されていないことが示されます。
  - `verified` - 検証プロセスが によって正常に完了 AppFabric し、 AppClient が完全に検証されました。
  - `rejected` - の検証プロセスが によって拒否 AppClient されました AppFabric。検証プロセスが再開され、正常に完了するまでは、 を追加のユーザーが AppClient 使用することはできません。

```
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>"
}'
```

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

```
{
    "appClientConfigSummary": {
        "appClientArn": "arn:aws:appfabric:<region>:<account>:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "verificationStatus": "pending_verification"
    }
}
```

Step 2. アプリケーションを認証し承認する

OAuth 2.0 認証フローを確立することで、アプリケーションが AppFabric インサイトを安全に統合できるようにします。まず認証コードを作成します。このコードがアプリケーションの ID を検証します。詳細については、「承認」を参照してください。次に、この認証コードをアクセストークンと交換します。アクセストークンは、アプリケーション内でインサイトを取得して表示する AppFabricアクセス許可をアプリケーションに付与します。詳細については、「トークン」を参照してください。

アプリケーションを承認するアクセス権限を付与する方法の詳細については、「アプリケーションを承認するためのアクセスを許可する」を参照してください。

1. 認証コードを作成するには、 `oauth2/authorize` API AWS AppFabricオペレーションを使用します。

   リクエストフィールド

   - `app_client_id` (必須) - ステップ 1 で AWS アカウント 作成した の AppClient ID。 を作成します AppClient。例えば `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111` です。
   - `redirect_uri`(必須) - ステップ 1. AppClient の作成 で使用した、認証後にエンドユーザーをリダイレクトする URI です。を作成します AppClient。例えば `https://localhost:8080` です。

- state (必須) - リクエストとコールバック間の状態を維持するための一意の値です。例えば a8904edc-890c-1005-1996-29a757272a44 です。

```
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. 認証後、ユーザーは指定した URI にリダイレクトされ、認証コードがクエリパラメータとして返されます。例えば、code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc です。

```
https://localhost:8080/?code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-
sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-
oampc&state=a8904edc-890c-1005-1996-29a757272a44
```

3. oauth2/token API オペレーションを使用して、この認証コードをアクセストークンと交換します AppFabric。

   このトークンは API リクエストに使用され、 AppClient が検証starterUserEmailsされるまで で最初に有効です。 AppClient が検証されたら、このトークンを任意のユーザーに使用できます。この API オペレーションを実行するには、アカウント署名バージョン 4 の認証情報を使用する必要があります。署名バージョン 4 の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

   リクエストフィールド

   - code (必須) - 最後のステップで認証を行った後にユーザーが受け取る認証コードです。例えば mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc です。
   - app_client_id (必須) - ステップ 1 で AWS アカウント 作成した の AppClient ID。 を作成します AppClient。例えば a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 です。
   - grant_type (必須) - 値は authorization_code でなければなりません。
   - redirect_uri(必須) - ステップ 1. AppClient の作成 で使用した、認証後にユーザーをリダイレクトする URI です。を作成します AppClient。こちらは、認証コードの作成に使用したものと同じリダイレクト URI である必要があります。例えば https://localhost:8080 です。

レスポンスフィールド

- `expires_in` - トークンの有効期限が切れるまでの残り時間です。デフォルトの有効期限は 12 時間です。
- `refresh_token` - 最初の /token リクエストで受け取った更新トークンです。
- `token` - 最初の /token リクエストで受け取ったトークンです。
- `token_type` - この値は `Bearer` になります。
- `appfabric_user_id` - AppFabric ユーザー ID。この値は、リクエストが `authorization_code` グラントタイプを使用している場合のみ返されます。

```
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\"
}"
```

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

```
{
    "expires_in": 43200,
    "refresh_token": "apkaeibaerjr2example",
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "<userId>"
}
```

ステップ 3。 AppFabric ユーザーポータル URL をアプリケーションに追加する

エンドユーザーは、インサイトの生成に使用されるアプリケーションからのデータへのアクセスを AppFabric に許可する必要があります。 は、エンドユーザーがアプリを承認するための専用のユーザーポータル (ポップアップ画面) を構築することで、アプリ開発者がこのプロセスを所有する複雑さ AppFabric を排除します。ユーザーが生産性 AppFabric を高める準備ができたら、ユーザーポータルに移動し、インサイトの生成やクロスアプリケーションアクションに使用されるアプリケーションを接続および管理できるようになります。ログインすると、ユーザーはアプリケーションを に接続して AppFabric 生産性を向上させ、アプリケーションに戻ってインサイトとアクションを調べることができます。アプリケーションを と統合して AppFabric 生産性を高めるには、アプリケーションに特定の AppFabric URL を追加する必要があります。このステップは、ユーザーがアプリケーションから直接 AppFabric ユーザーポータルにアクセスできるようにするために不可欠です。

1. アプリケーションの設定に進み、リダイレクト URL を追加するセクションを探します。
2. 適切な領域を見つけたら、次の AppFabric URL をリダイレクト URL としてアプリケーションに追加します。

```
https://userportal.appfabric.<region>.amazonaws.com/eup_login
```

URL を追加すると、アプリケーションをユーザーポータルに誘導するように AppFabricセットアップされます。ここでは、ユーザーはログインして、生産性に関するインサイト AppFabric の生成に使用されるアプリケーションを接続および管理できます。

ステップ 4。を使用して AppFabric クロスアプリケーションインサイトとアクションを表示する

ユーザーがアプリケーションを接続したら、アプリケーションとコンテキストの切り替えを減らすことで、ユーザーのインサイトを活用して生産性を向上させることができます。 は、ユーザーがアクセス許可を持っているものに基づいて AppFabric のみユーザーのインサイトを生成します。は、ユーザーデータを AWS アカウント が所有する に AppFabric 保存します AppFabric。がデータ AppFabric を使用する方法については、「」を参照してくださいデータ処理。

ユーザーレベルのインサイトとアクションをアプリケーション内で生成して表示するときは、AI を活用した以下の API を使用できます。

- `ListActionableInsights` — 詳細については、以下の「実行可能なインサイト」のセクションを参照してください。

- `ListMeetingInsights` — 詳細については、本ガイドで後述する「会議の準備」のセクションを参照してください。

実行可能なインサイト (**`ListActionableInsights`**)

`ListActionableInsights` は、アプリケーション (E メール、カレンダー、メッセージ、タスクなど) を横断するアクティビティに基づいて実行可能なインサイトを表示する、日々の業務を効率よく管理するのに役立つ API です。表示されるインサイトには、インサイトの生成に使用されたアーティファクトへの埋め込みリンクも含まれているため、ユーザーはインサイトの生成に使用されたデータをすばやく確認できます。さらにこの API は、インサイトに基づく推奨されるアクションを返すことができるため、ユーザーは自分のアプリケーションからクロスアプリケーションアクションを実行することができます。具体的には、この API は Asana、Google Workspace、Microsoft 365、Smartsheet などのプラットフォームと連携し、ユーザーがメール送信、カレンダーイベントの作成、タスクの作成などを行うことを可能にします。大規模言語モデル (LLM) では、推奨されるアクション (メール本文やタスク名など) に自動的に詳細を追加できます。ユーザーはこれを実行前にカスタマイズできるため、意思決定を簡略化し、生産性を高めることができます。エンドユーザーがアプリケーションを認証するエクスペリエンスと同様に、 は同じ専用ポータル AppFabric を使用して、ユーザーがクロスアプリケーションアクションを表示、編集、実行できるようにします。アクションを実行するには、ISVs AppFabric がユーザーを AppFabric ユーザーポータルにリダイレクトし、アクションの詳細を確認して実行する必要があります。によって生成されたすべてのアクションには、一意の URL AppFabric があります。この URL は `ListActionableInsights` API レスポンスのレスポンスで使用できます。

以下は、サポートされているクロスアプリケーションアクションと、どのアプリケーションでサポートされているかをまとめたものです。

- E メールの送信 (Google Workspace、Microsoft 365)
- カレンダーイベントの作成 (Google Workspace、Microsoft 365)
- タスクの作成 (Asana、Smartsheet)

リクエストフィールド

- `nextToken` (オプション) - 次回のインサイトのセットを取得するためのページネーショントークンです。
- `includeActionExecutionStatus` - アクションの実行ステータスのリストを受け入れるフィルターです。これらのアクションは渡されたステータス値に基づいてフィルタリングされます。使用できる値: `NOT_EXECUTED` | `EXECUTED`

リクエストヘッダー

- 承認ヘッダーは `Bearer Token` 値とともに渡す必要があります。

レスポンスフィールド

- `insightId` - 生成されたインサイトの一意の ID です。
- `insightContent` - インサイトの概要と、インサイトの生成に使用されたアーティファクトへの埋め込みリンクを返します。注: こちらは、埋め込みリンク (<a>タグ) を含む HTML コンテンツです。
- `insightTitle` - 生成されたインサイトの件名です。
- `createdAt` - インサイトが生成された日時です。
- `actions` - 生成されたインサイトで推奨されるアクションのリストです。アクションオブジェクト:
  - `actionId` - 生成されたアクションの一意の ID です。
  - `actionIconUrl` - アクションの実行が推奨されているアプリケーションのアイコン URL です。
  - `actionTitle` - 生成されたアクションの件名です。
  - `actionUrl` - の AppFabricユーザーポータルでアクションを表示および実行するエンドユーザーの一意の URL。注: アクションを実行する場合、ISV アプリケーションはこの URL を使用してユーザーを AppFabric ユーザーポータル (ポップアップ画面) にリダイレクトします。
  - `actionExecutionStatus` - アクションのステータスを示す列挙型です。指定できる値は `EXECUTED | NOT_EXECUTED` です。
- `nextToken` (オプション) - 次回のインサイトのセットを取得するためのページネーショントークンです。こちらはオプションのフィールドで、null が返された場合は、ロードするインサイトがそれ以上ないことを意味します。

詳細については、「ActionableInsights」を参照してください。

```
curl -v --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/actionableInsights" \
  --header "Authorization: Bearer <token>"
```

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

```
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
```

```
}
```

会議の準備 (**ListMeetingInsights**)

ListMeetingInsights は、会議の内容を要約したり、E メールやメッセージその他のアプリケーションを横断して関連性の高いアーティファクトを表示したりすることで、今後の会議に向けて準備するのに役立つ API です。ユーザーはすぐに会議に向けた準備ができ、コンテンツを見つけるためにアプリケーション間を切り替える手間が省けます。

リクエストフィールド

- nextToken (オプション) - 次回のインサイトのセットを取得するためのページネーショントークンです。

リクエストヘッダー

- 承認ヘッダーは Bearer Token 値とともに渡す必要があります。

レスポンスフィールド

- insightId - 生成されたインサイトの一意の ID です。
- insightContent - インサイトの説明で、詳細は文字列の形式で強調表示されます。例えば、なぜこのインサイトが重要なのか、など。
- insightTitle - 生成されたインサイトの件名です。
- createdAt - インサイトが生成された日時です。
- calendarEvent - ユーザーが注目すべき重要なカレンダーイベントまたは会議です。カレンダーイベントオブジェクト:
  - startTime - イベントの開始時刻です。
  - endTime - イベントの終了時刻です。
  - eventUrl - ISV アプリケーションのカレンダーイベントの URL です。
- resources - インサイトの生成に関連する他のリソースを含むリストです。リソースオブジェクト:
  - appName - リソースが属するアプリケーションの名前です。
  - resourceTitle - リソースの件名です。
  - resourceType - リソースのタイプです。指定できる値は EMAIL | EVENT | MESSAGE | TASK です。

  - resourceUrl - アプリケーション内のリソース URL です。
  - appIconUrl - リソースが属するアプリケーションの画像 URL です。
- nextToken (オプション) - 次回のインサイトのセットを取得するためのページネーショントークンです。こちらはオプションのフィールドで、null が返された場合は、ロードするインサイトがそれ以上ないことを意味します。

詳細については、「MeetingInsights」を参照してください。

```
curl --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/meetingContexts" \
  --header "Authorization: Bearer <token>"
```

アクションが成功すると、HTTP 201 レスポンスが返されます。

```
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
}
```

インサイトやアクションに関するフィードバックを提供してください。

API AppFabric PutFeedbackオペレーションを使用して、生成されたインサイトとアクションに関するフィードバックを提供します。この機能はアプリに埋め込むと、特定の InsightId または の フィードバック評価 (1～5、評価が高いほど良い) を送信する方法が提供されます ActionId。

リクエストフィールド

- `id` - フィードバックの送信対象となるオブジェクトの識別子です。これは、 InsightId または のいずれかです ActionId。
- `feedbackFor` - フィードバックの送信対象となるリソースタイプです。使用できる値: `ACTIONABLE_INSIGHT` | `MEETING_INSIGHT` | `ACTION`
- `feedbackRating` - 1 から 5 までの評価です。値が大きいほど評価が高いことを意味します。

レスポンスフィールド

- レスポンスフィールドはありません。

詳細については、「PutFeedback」を参照してください。

```
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
}'
```

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 201 レスポンスを返します。

Step 5. アプリケーションの検証 AppFabric をリクエストする

この時点で、アプリケーション UI を更新して AppFabric クロスアプリケーションインサイトとアクションを埋め込み、単一のユーザーに関するインサイトを取得しました。テストに満足し、 AppFabricの豊富なエクスペリエンスを他のユーザーに拡張したい場合は、レビューと検証 AppFabric のために にアプリケーションを送信できます。 AppFabric は、アプリケーションデベロッパー、エンドユーザー、およびそれらのデータを保護するために幅広い導入を可能にする前に、アプリケーション情報を検証します。これにより、責任ある方法でユーザー導入を拡大する方法が開かれます。

検証プロセスの開始

appfabric-appverification@amazon.com にメールを送信し、アプリケーションの検証をリクエストして、検証プロセスを開始します。

E メールの本文には次の情報を含めます。

- AWS アカウント ID
- 検証を依頼するアプリケーションの名称
- AppClient ID
- 自分の連絡先情報

また、可能であれば、以下の情報も含めると、優先順位や影響を評価する際に役立ちます。

- アクセスを許可するユーザー数 (推計)
- リリース日

> **Note**
> AWS アカウント マネージャーまたは AWS パートナー開発マネージャーがいる場合は、E メールでコピーしてください。追加しておくと、検証プロセスをスピーディに進めることができます。

検証基準

検証プロセスを開始する前に、次の基準を満たしている必要があります。

- 生産性 AWS アカウント 向上のために を使用するには、有効な AppFabric を使用する必要があります

また、以下の基準のうち 1 つ以上を満たしている必要があります。

- 組織は、少なくともAWS 「選択」階層 AWS Partner Network を持つ の AWS パートナーです。詳細については、「AWS サービスパートナーティア」を参照してください。
- 組織は、過去 3 年間に AppFabric のサービスに 10,000 USD 以上を費やしているはずです。
- アプリケーションが AWS Marketplaceに掲載されていること。詳細については、「AWS Marketplace」を参照してください。

検証ステータスの更新の待機

アプリケーションの確認後、E メールで応答し、 のステータス AppClient が から `pending_verification`に変わります`verified`。アプリケーションが却下された場合は、検証プロセスを改めて行う必要があります。

生産性向上 AppFabric のための の管理 AppClients

> AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

AppFabric for productivity を管理 AppClients して、認証および認証プロセスの運用とメンテナンスをスムーズに行うことができます。

の詳細を取得する AppClient

API AppFabric `GetAppClient`オペレーションを使用して、 AppClient ステータスの確認など AppClient、 の詳細を表示します。詳細については、「GetAppClient」を参照してください。

の詳細を取得するには AppClient、少なくとも IAM `"appfabric:GetAppClient"` ポリシーのアクセス許可が必要です。詳細については、「の詳細を取得するためのアクセスを許可する AppClients」を参照してください。

リクエストフィールド

- `appClientId` - AppClient ID。

レスポンスフィールド

- `appName` - ユーザー AppFabric ポータルの同意ページに表示されるアプリケーションの名前。
- `customerManagedKeyIdentifier` (オプション) - データの暗号化に使用されるカスタマーマネージドキー (KMS が生成) の ARN です。指定しない場合、 AWS AppFabric マネージドキーが使用されます。
- `description` - アプリケーションの説明です。
- `redirectUrls` - 承認後にエンドユーザーがリダイレクトされる URI です。redirectUrls は 5 個まで追加できます。例えば、`https://localhost:8080` などです。
- `starterUserEmails` - アプリケーションが検証されるまでの間、インサイトを受け取るためのアクセスが許可されるユーザーの E メールアドレスです。使用できるアドレスは 1 つのみです。例えば、`anyuser@example.com` です。

- `verificationStatus` - AppClient 検証ステータス。
  - `pending_verification` - の検証は AppClientでまだ進行中です AppFabric。が検証されるまで、 を使用できるユーザー (で指定`starterUserEmails`) AppClient は 1 人のみです AppClient。
  - `verified` - 検証プロセスが によって正常に完了 AppFabric し、 AppClient が完全に検証されました。
  - `rejected` - の検証プロセスが によって拒否 AppClient されました AppFabric。検証プロセスが再開され、正常に完了するまでは、 を追加のユーザーが AppClient 使用することはできません。

```
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
```

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

```
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"
        }
    }
```

```
}
```

リスト AppClients

API AppFabric `ListAppClients`オペレーションを使用して、 のリストを表示します AppClients。AppClient ごとに 1 つの AppFabric のみを許可します AWS アカウント。この制限は将来変更される可能性があります。詳細については、「ListAppClients」を参照してください。

AppClientsを一覧表示するには、少なくとも IAM `"appfabric:ListAppClients"` ポリシーのアクセス許可が必要です。詳細については、「リストへのアクセスを許可する AppClients」を参照してください。

リクエストフィールド

- 必須フィールドはありません。

レスポンスフィールド

- `appClientARN` - AppClient ID を含む Amazon リソースネーム (ARN)。例えば、 AppClient ID はです`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。
- `verificationStatus` - AppClient 検証ステータス。
  - `pending_verification` - の検証は AppClientでまだ進行中です AppFabric。が検証されるまで、 を使用できるユーザー (で指定`starterUserEmails`) AppClient は 1 人のみです AppClient。
  - `verified` - 検証プロセスが によって正常に完了 AppFabric し、 AppClient が完全に検証されました。
  - `rejected` - の検証プロセスが によって拒否 AppClient されました AppFabric。検証プロセスが再開され、正常に完了するまでは、 を追加のユーザーが AppClient 使用することはできません。

```
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
```

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

```
200 OK

{
    "appClientList": [
        {
            "appClientArn": "arn:aws:appfabric:<region>:111122223333:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "verificationStatus": "pending_verification"
        }
    ]
}
```

の更新 AppClient

API AppFabric `UpdateAppClient`オペレーションを使用して、 にマッピングされた redirectUrls を更新します AppClient。 AppName、、またはその他のパラメータを変更する必要がある場合は starterUserEmails、 を削除 AppClient して新しいパラメータを作成する必要があります。詳細については、「UpdateAppClient」を参照してください。

を更新するには AppClient、少なくとも IAM `"appfabric:UpdateAppClient"` ポリシーのアクセス許可が必要です。詳細については、「更新へのアクセスを許可する AppClients」を参照してください。

リクエストフィールド

- `appClientId` (必須) - redirectUrls を更新する AppClient ID。
- `redirectUrls` (必須) - 更新された redirectUrls のリストです。redirectUrls は 5 個まで追加できます。

レスポンスフィールド

- `appName` - ユーザー AppFabric ポータルの同意ページに表示されるアプリケーションの名前。
- `customerManagedKeyIdentifier` (オプション) - データの暗号化に使用されるカスタマーマネージドキー (KMS が生成) の ARN です。指定しない場合、 AWS AppFabric マネージドキーが使用されます。
- `description` - アプリケーションの説明です。

- `redirectUrls` - 承認後にエンドユーザーがリダイレクトされる URI です。例えば、`https://localhost:8080` です。
- `starterUserEmails` - アプリケーションが検証されるまでの間、インサイトを受け取るためのアクセスが許可されるユーザーの E メールアドレスです。使用できるアドレスは 1 つのみです。例えば、`anyuser@example.com` です。
- `verificationStatus` - AppClient 検証ステータス。
  - `pending_verification` - の検証は AppClientでまだ進行中です AppFabric。が検証されるまで、 を使用できるユーザー (で指定`starterUserEmails`) AppClient は 1 人のみです AppClient。
  - `verified` - 検証プロセスが によって正常に完了 AppFabric し、 AppClient が完全に検証されました。
  - `rejected` - の検証プロセスが によって拒否 AppClient されました AppFabric。検証プロセスが再開され、正常に完了するまでは、 を追加のユーザーが AppClient 使用することはできません。

```
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"]
}'
```

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

```
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"
        }
    }
}
```

を削除する AppClient

API AppFabric `DeleteAppClient`オペレーションを使用して、不要になった AppClients を削除します。詳細については、「DeleteAppClient」を参照してください。

を削除するには AppClient、少なくとも IAM `"appfabric:DeleteAppClient"` ポリシーのアクセス許可が必要です。詳細については、「削除するためのアクセスを許可する AppClients」を参照してください。

リクエストフィールド

- `appClientId` - AppClient ID。

レスポンスフィールド

- レスポンスフィールドはありません。

```
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
```

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 204 レスポンスを返します。

エンドユーザー用トークンを更新する

エンドユーザー用に AppClient 取得したトークンは、有効期限が切れると更新できます。これは トークン API と grant_type `refresh_token` とを組み合わせて使用することで実行できます。grant_type が `authorization_code` である場合は、使用すべき `refresh_token` は、トークン API のレスポンスの一部として返されます。デフォルトの有効期限は 12 時間です。更新 API を呼び出すには、`"appfabric:Token"` IAM ポリシーの許可が必要です。詳細については、「トークン」および「更新へのアクセスを許可する AppClients」を参照してください。

リクエストフィールド

- `refresh_token` (必須) - 最初の `/token` リクエストで受け取った更新トークンです。
- `app_client_id` (必須) - 用に作成された AppClient リソースの ID AWS アカウント。
- `grant_type` (必須) - `refresh_token` でなければなりません。

レスポンスフィールド

- `expires_in` - トークンの有効期限が切れるまでの残り時間です。デフォルトの有効期限は 12 時間です。
- `refresh_token` - 最初の /token リクエストで受け取った更新トークンです。
- `token` - 最初の /token リクエストで受け取ったトークンです。
- `token_type` - この値は `Bearer` になります。
- `appfabric_user_id` - AppFabric ユーザー ID。この値は、リクエストが `authorization_code` グラントタイプを使用している場合のみ返されます。

```
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\"
}"
```

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

```
200 OK

{
    "expires_in": 43200,
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "${UserID}"
}
```

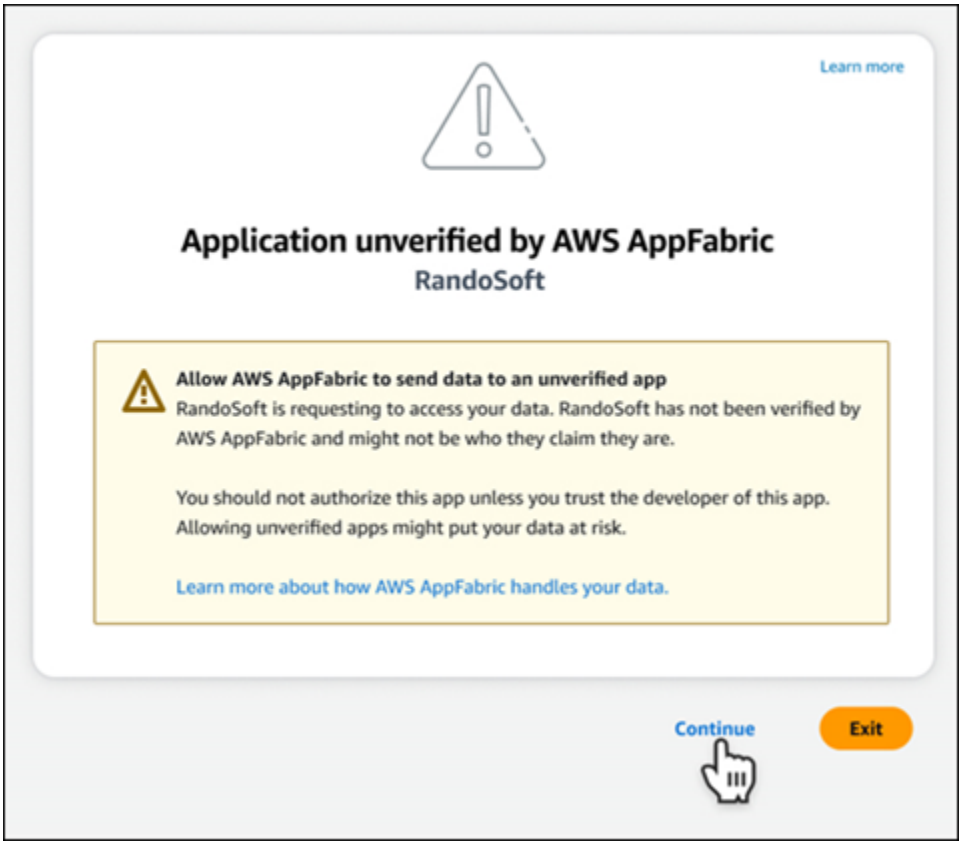
トラブルシューティング

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

このセクションでは、生産性 AppFabric 向上のための一般的なエラーとトラブルシューティングについて説明します。

未検証のアプリケーション

for AppFabric productivity を使用してアプリケーションエクスペリエンスを強化するアプリケーションデベロッパーは、エンドユーザーに機能を起動する前に検証プロセスを実行します。アプリケーションはすべて、未検証の状態からスタートし、検証プロセスが完了した場合のみ、検証済みの状態になります。つまり、 の作成時に`starterUserEmails`使用した AppClient には、このメッセージが表示されます。



`CreateAppClient` エラー

ServiceQuotaExceededException

の作成時に次の例外が発生した場合 AppClient、 ごとに作成 AppClients できる の数を超えました AWS アカウント。上限は 1 です。HTTP ステータスコード: 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` エラー

ResourceNotFoundException

の詳細を取得するときに次の例外が発生した場合は AppClient、正しい AppClient 識別子が入力されていることを確認してください。このエラーは、指定された AppClient が見つからないことを示します。

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
```

```
The specified AppClient is not found. Ensure you’ve entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

DeleteAppClient エラー

ConflictException

の削除時に次の例外が発生した場合 AppClient、別の削除リクエストが進行中です。そちらが完了するまで待機してから、再度お試しください。HTTP ステータスコード: 409

```
ConflictException
Another delete request is in progress. Wait until it completes then try again.
HTTP Status Code: 409
```

ResourceNotFoundException

の削除時に次の例外が発生した場合は AppClient、正しい AppClient 識別子が入力されていることを確認してください。このエラーは、指定された AppClient が見つからないことを示します。

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you’ve entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

UpdateAppClient エラー

ResourceNotFoundException

の更新時に次の例外が発生した場合は AppClient、正しい AppClient 識別子が入力されていることを確認してください。このエラーは、指定された AppClient が見つからないことを示します。

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you’ve entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Authorize エラー

ValidationException

API パラメータのいずれかが、API の仕様で定義されている制限事項を満たしていない場合、以下の例外が発生することがあります。

```
ValidationException
HTTP Status Code: 400
```

理由 1: AppClient ID が指定されていない場合

リクエストにパラメータに `app_client_id` がありません。まだ作成されていない場合は AppClient を作成するか、既存の を使用して`app_client_id`再試行してください。 AppClient ID を検索するには、 ListAppClient API オペレーションを使用します。

理由 2: がカスタマーマネージドキーにアクセス AppFabric できない場合

```
Message: AppFabric couldn't access the customer managed key configured for AppClient.
```

AppFabric は現在、アクセス許可の最近の変更により、カスタマーマネージドキーにアクセスできません。指定されたキーが存在することを確認し、 に適切なアクセス許可 AppFabric が付与されていることを確認します。

理由 3: 指定したリダイレクト URL が無効

```
Message: Redirect url invalid
```

リクエストのリダイレクト URL が正しいことを確認します。を作成または更新したときに指定されたリダイレクト URLs のいずれかと一致する必要があります AppClient。許可されたリダイレクト URLsオペレーションを使用します。 GetAppClient

Token エラー

TokenException

いくつかの理由から、以下のエラーが発生する場合があります。

```
TokenException
HTTP Status Code: 400
```

理由 1: 無効なメールが指定されている

```
Message: Invalid Email used
```

使用している E メールアドレスが、 の作成時に `starterUserEmails` 属性にリストされているものと一致していることを確認します AppClient。一致しない場合は、一致する E メールアドレスに変更してから再度試します。使用された E メールを表示するには、 GetAppClient API オペレーションを使用します。

理由 2: トークンが指定されていない場合、grant_type が refresh_token として返される。

```
Message: refresh_token must be non-null for Refresh Token Grant-type
```

リクエストで指定した更新トークンが null または空です。Token API コールのレスポンスに、受信したアクティブな `refresh_token` を指定します。

ThrottlingException

API が、許可されているクォータを超えるレートで呼び出されると、以下の例外が発生する可能性があります。

```
ThrottlingException
HTTP Status Code: 429
```

`ListActionableInsights`、`ListMeetingInsights`、`PutFeedback` のエラー

ValidationException

API パラメータのいずれかが、API の仕様で定義されている制限事項を満たしていない場合、以下の例外が発生することがあります。

```
ValidationException
HTTP Status Code: 400
```

ThrottlingException

API が、許可されているクォータを超えるレートで呼び出されると、以下の例外が発生する可能性があります。

```
ThrottlingException
```

```
HTTP Status Code: 429
```

エンドユーザー AppFabric 向けの for productivity (プレビュー) の開始方法

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

このセクションは、タスク管理とワークフロー効率を向上させるために生産性向上 (プレビュー) AWS AppFabric を実現したい SaaS アプリケーションのエンドユーザーを対象としています。アプリケーションを接続し、クロスアプリケーションインサイトを表示することを AppFabric に許可し、任意のアプリケーションからのアクション (E メールの送信や会議のスケジュールなど) を完了するのに役立ちます。接続できるアプリケーションは、Asana、Atlassian Jira Suite、Google Workspace、Microsoft 365、Miro、Slack、Smartsheet などです。コンテンツへのアクセスを AppFabric に許可すると、 AppFabric はクロスアプリケーションインサイトとアクションを任意のアプリ内で直接提供し、より効率的に作業し、現在のワークフロー内にとどまるのに役立ちます。

AppFabric for productivity は、Amazon Bedrock を利用した生成 AI を使用します。 AppFabric は、明示的なアクセス許可を受け取った後にのみインサイトとアクションを生成します。個々のアプリケーションが、どのコンテンツが使用されているかを完全に制御できるように許可します。AppFabric は、インサイトの生成に使用される基盤となる大規模言語モデルのトレーニングや改善にデータを使用しません。詳細については、「Amazon Bedrock よくある質問」を参照してください。

トピック

- 前提条件
- Step 1. にサインインする AppFabric
- Step 2. インサイトを表示することをアプリに許可する
- ステップ 3。アプリケーションを接続してインサイトとアクションを生成する
- ステップ 4。自分のアプリケーションでインサイトを確認しクロスアプリケーションアクションを実行する
- IT 管理者とセキュリティ管理者に注意: 生産性 AppFabric 向上のための へのアクセスの管理 (プレビュー) 機能
- トラブルシューティング

前提条件

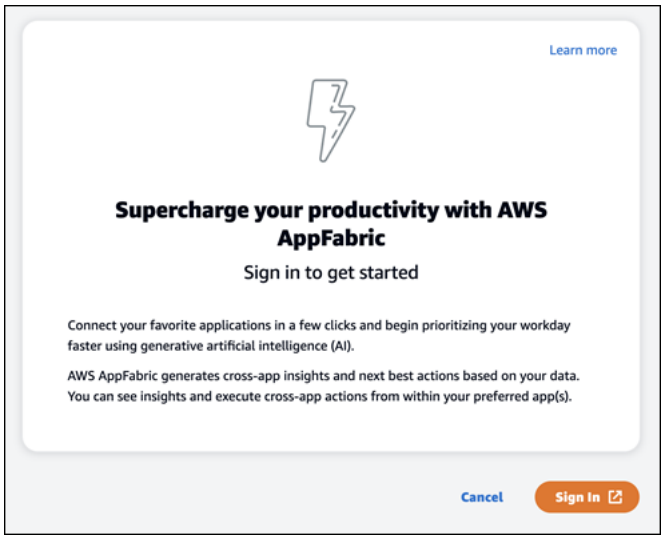
作業を開始する前に、以下の条件がそろっていることを確認します。

- にサインインするための認証情報 AppFabric: 生産性 AppFabric 向上のために の使用を開始するには、、Asana、、Microsoft 365または のいずれかのプロバイダーのフェデレーティッドサインイン認証情報 (ユーザー名とパスワード) Google Workspaceが必要ですSlack。にサインインするとAppFabric 、生産性 AppFabric 向上のために有効にした各アプリケーションのユーザーとして識別できます。サインインすると、お使いのアプリケーションを接続してインサイトの生成を開始できます。
- アプリケーションを接続するための認証情報: クロスアプリケーションのインサイトとアクションは、ユーザーが承認するアプリケーションに基づいてのみ生成されます。サインインの認証情報は (ユーザー名とパスワード) は、認証するアプリケーションごとに、必要になります。サポートされているアプリケーションには、Asana、Atlassian Jira Suite、Google Workspace、Microsoft 365、Miro、Slack、Smartsheet などがあります。

Step 1. にサインインする AppFabric

アプリケーションを に接続 AppFabric して、コンテンツとインサイトを任意のアプリケーションに直接取り込みます。

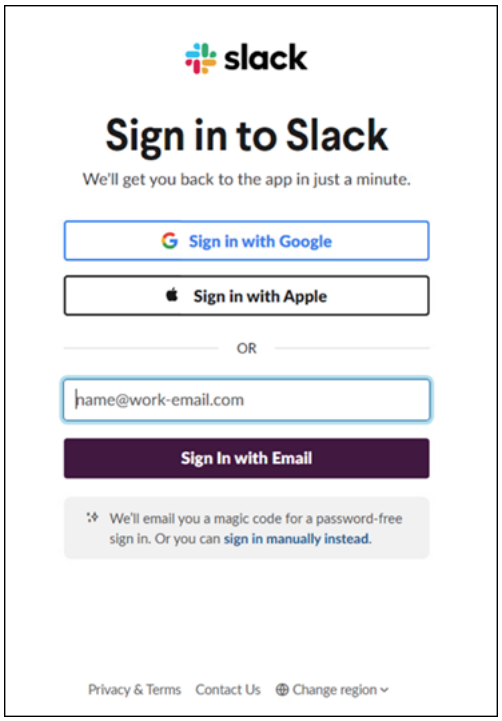
1. すべてのアプリケーションは、さまざまな方法で生産性 AppFabric 向上のために を使用して、より充実したアプリケーションエクスペリエンスを提供します。このため、アプリケーションごとに異なるエントリポイントがあり、以下の for productivity AppFabric のホームページにアクセスできます。ホームページは、有効にするプロセスに関するコンテキストを設定し AppFabric 、最初にサインインするように促します。 AppFabric で有効にするすべてのアプリケーションがこの画面に表示されます。

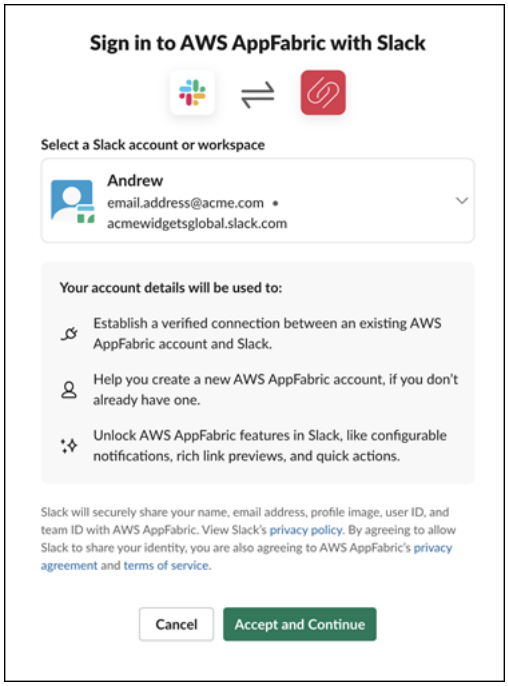


2. Asana、Google Workspace、Microsoft 365、Slack のいずれかのプロバイダーから自分の認証情報を使ってサインインします。最良のエクスペリエンスを得るには、有効にするアプリケー

ションごとに同じプロバイダーを使用して AppFabric サインインすることをお勧めします。例えば、App1 で Google Workspace の認証情報を使用した場合は、App2 でも、また再度サインインする必要がある場合にも、Google Workspace を使用することが推奨されます。別のプロバイダーを使ってサインインする場合は、アプリケーションを接続するプロセスを再度実行する必要があります。

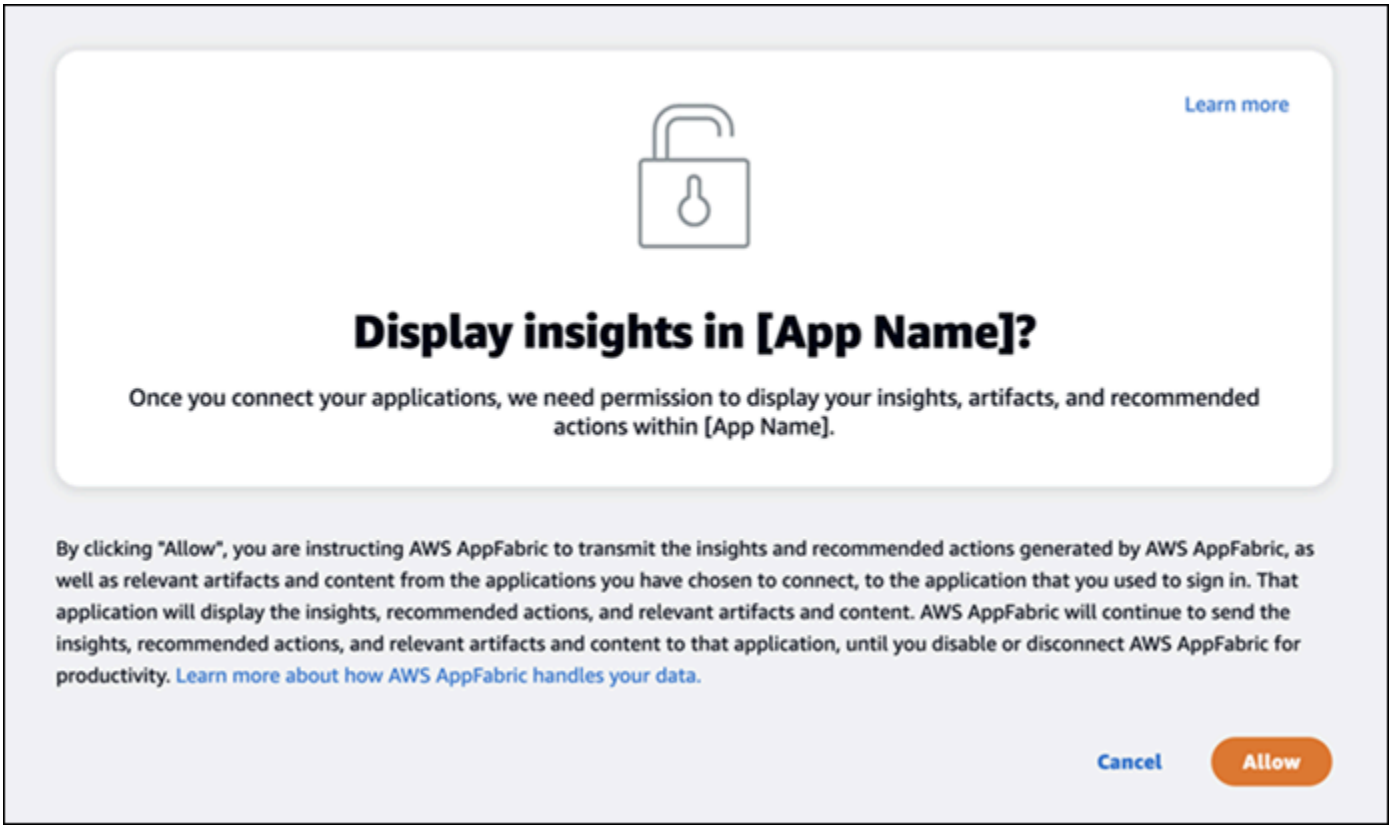
3. プロンプトが表示されたら、サインイン認証情報を入力し、このプロバイダー AppFabric からのサインインを承諾します。





Step 2. インサイトを表示することをアプリに許可する

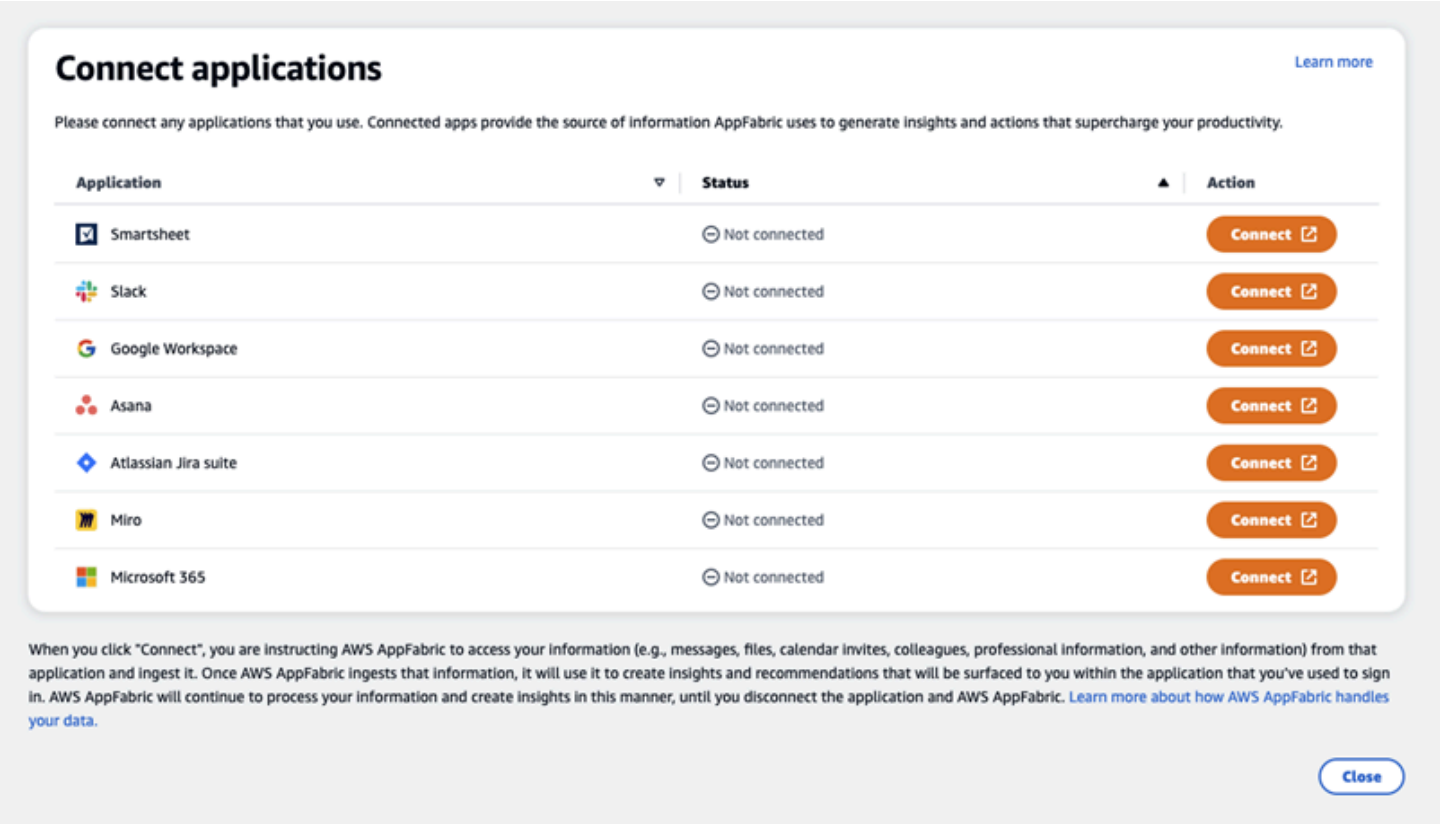
サインインすると、 は、生産性 AppFabric を高めるため AppFabric に有効化しているアプリケーション内でクロスアプリケーションインサイトとアクションを表示できるかどうかを尋ねる同意ページ AppFabric を表示します。例えば、 AppFabric で Google Workspace E メールとカレンダーイベントを受け取り、 に表示することを に許可しますかAsana。この同意ステップは、有効にしたアプリケーションごとに 1 回だけ完了する必要があります AppFabric 。



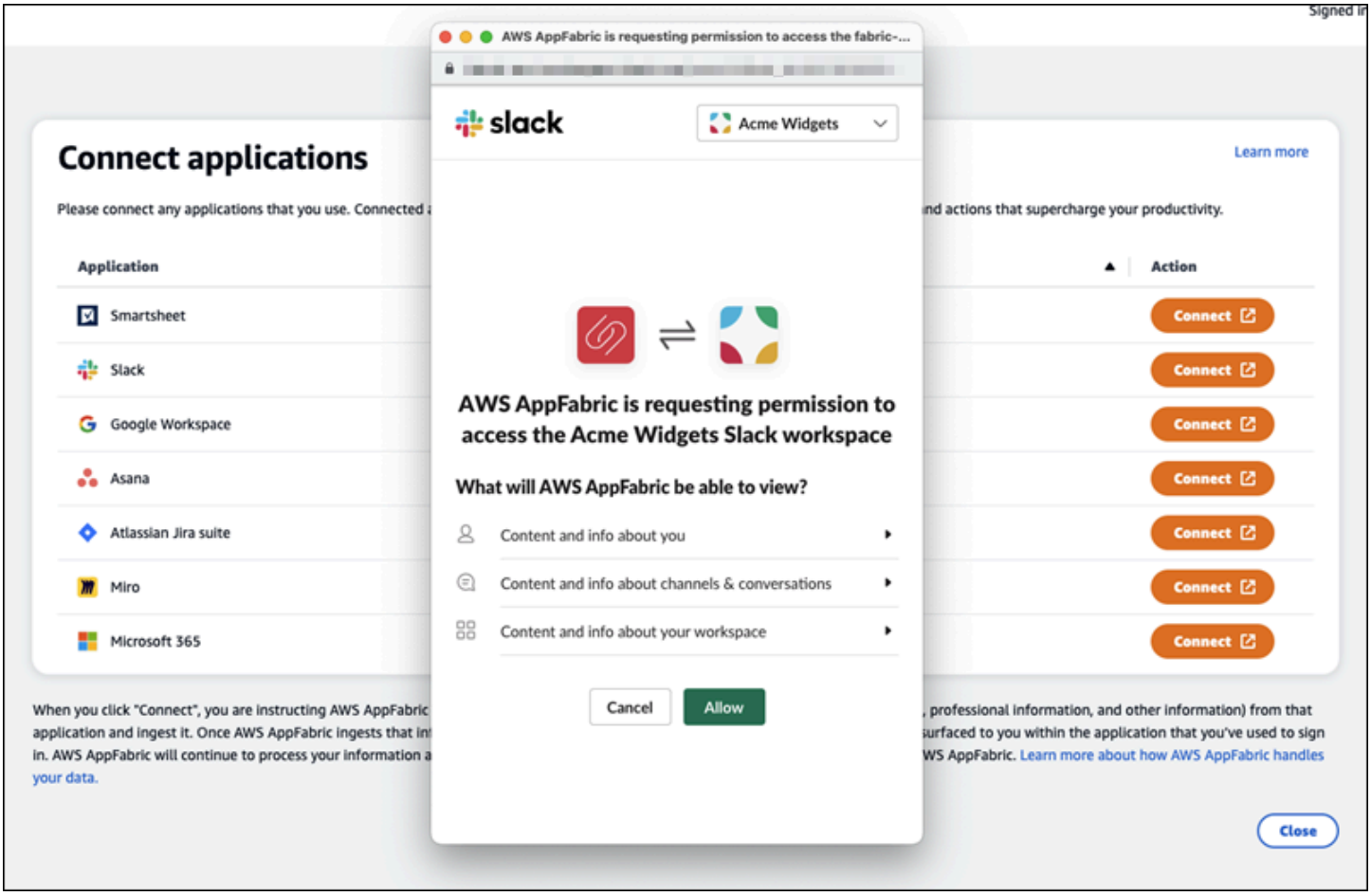
ステップ 3。アプリケーションを接続してインサイトとアクションを生成する

同意のステップを完了すると、[アプリケーションを接続] ページに進みます。ここでは、クロスアプリケーションのインサイトやアクションの生成に使用する個々のアプリケーションの、接続、切断、再接続が行えます。ほとんどの場合、サインインして同意のステップを完了した後は、このページを使って、接続したアプリケーションを管理します。

アプリケーションを接続するには、使用するアプリケーションの横にある [接続] をクリックします。



アプリケーションのサインイン認証情報を提供し、データにアクセスしてインサイトを生成し、アクションを完了するアクセス許可を付与 AppFabricする必要があります。

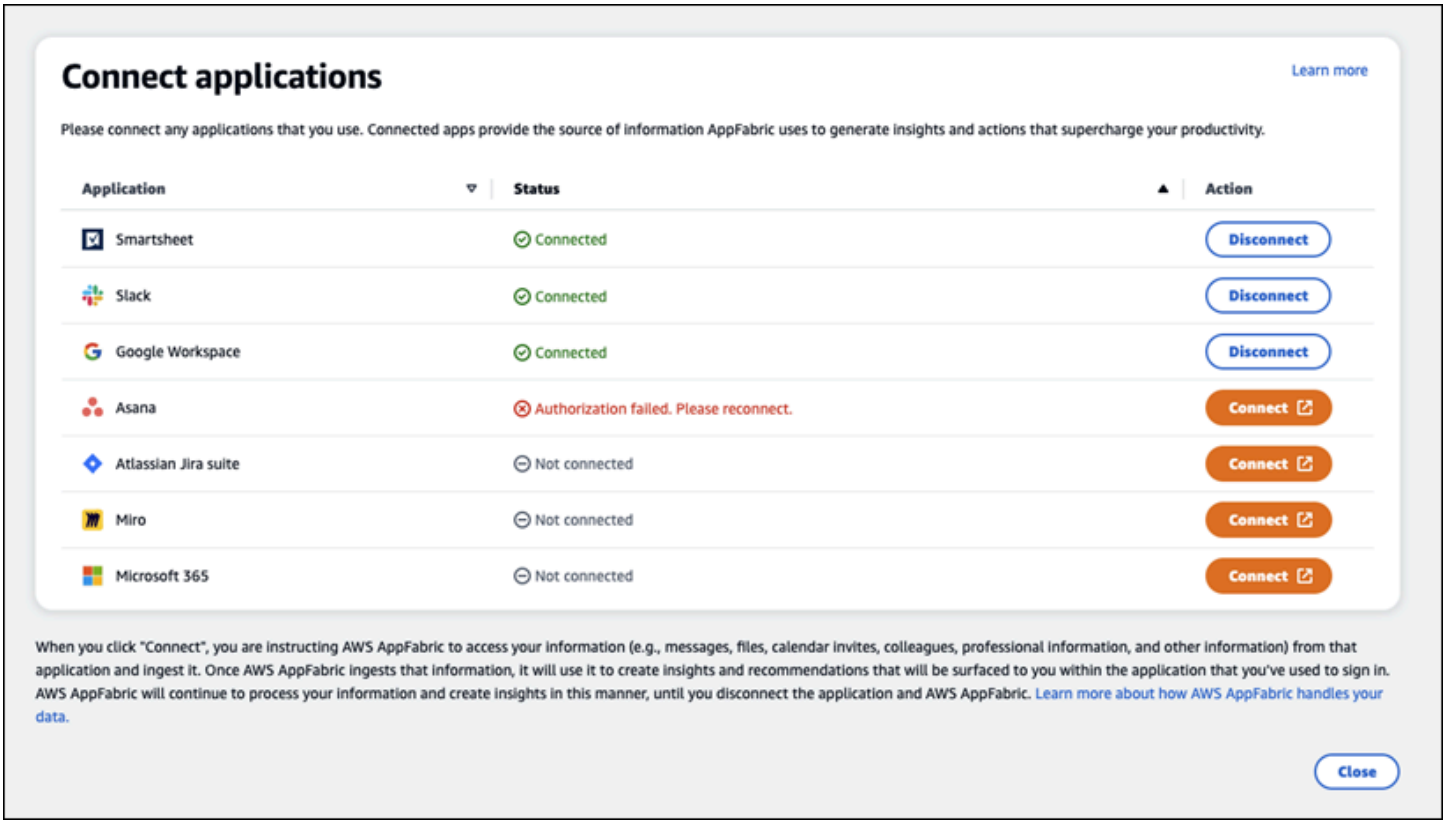


アプリケーションが正常に接続すると、そのアプリケーションのステータスが [未接続] から[接続済み] に変わります。以上の承認ステップは、インサイトやアクションの生成に使用するアプリケーションごとに実行する必要があります。

アプリケーションは、1 度接続すればその状態が永久に続くわけではありません。定期的に接続し直す必要があります。なぜ必要かというと、インサイトを生成するためのアクセス権限が引き続き付与されていることを確認するためです。

アプリケーションのステータスには、以下の状態があります。

- 接続済み - AppFabric 認可されており、このアプリケーションのデータを使用してインサイトを生成しています。
- Not Connected - このアプリケーションのデータを使用してインサイトを生成 AppFabric していません。接続するとインサイトの生成を開始できます。
- 承認に失敗しました。再接続してください。- アプリケーションの認証に失敗した可能性があります。このエラーが表示されたときは、[接続] をクリックして再度アプリケーションを接続します。



セットアップが完了したので、アプリケーションに戻ることができます。アプリケーション内にインサイトが表示されるまで、数時間かかることがあります。

接続済みのアプリケーションを管理するときは、必要に応じてこのページに戻ります。アプリケーションを切断することを選択した場合、 はそのアプリケーションからのデータの使用や新しいデータの収集 AppFabric を停止して、新しいインサイトを生成します。切断したアプリケーションのデータは、7 日以内に、その間アプリケーションをを再度接続しなければ、自動的に削除されます。

ステップ 4。自分のアプリケーションでインサイトを確認しクロスアプリケーションアクションを実行する

アプリケーションを に接続すると AppFabric、貴重なインサイトと、任意のアプリケーションから直接クロスアプリケーションアクションを実行できるようになります。注: この機能は各アプリケーションで保証されるものではなく、アプリケーション開発者がどの AppFabric for productivity 機能を有効にするかに完全に依存します。

クロスアプリケーションインサイト

AppFabric for productivity には、次の 2 種類のインサイトがあります。

- 実用的なインサイト: 接続されたアプリ全体で E メール、カレンダーイベント、タスク、メッセージからの情報を AppFabric 分析し、優先順位を付けることが重要と思われる重要なインサイトを生成します。さらに、 AppFabric 任意のアプリケーションにとどまりながら編集および実行できる推奨アクション (E メールの送信、会議のスケジュール、タスクの作成など) を生成できます。例えば、対処すべきカスタマーエスカレーションがあります、推奨されるアクションはこちらです、といったインサイトを受け取って、顧客とのミーティングをスケジュールする、といったことが行えます。
- 会議の準備に関するインサイト: この機能を使うと、今後の会議に向けて準備することができます。 AppFabric は今後の会議を分析し、会議の目的に関する簡潔な概要を生成します。さらに、接続されているアプリケーションから、関連するアーティファクト (E メール、メッセージ、タスクなど) が表示されます。アプリケーションを切り替えてコンテンツを探す手間が省け、会議の準備を効率的に進めることができます。

クロスアプリケーションアクション

特定のインサイトについては、E メールの送信、会議のスケジュール設定、タスクの作成などの推奨アクションを生成する AppFabric 場合もあります。アクションを生成するときに、接続されたアプリケーションの内容とコンテキストに基づいて、特定のフィールドを AppFabric 事前に入力できます。例えば、インサイトに基づいて推奨される E メールレスポンスやタスク名を生成 AppFabric できます。推奨されるアクションをクリックすると、 AppFabric 所有のユーザーインターフェイスに移動し、アクションを実行する前に事前入力されたコンテンツを編集できます。 AppFabric は、生成 AI と基盤となる大規模言語モデル (LLM) が時折ハルシネーションする可能性があるため、ユーザーによるレビューと入力なしで最初にアクションを実行しません。

> **Note**
>
> AppFabric LLM 出力を検証して確認する責任はお客様にあります。 AppFabric は LLM 出力の正確性や品質を保証しません。詳細については、「AWS Responsible AI Policy」を参照してください。

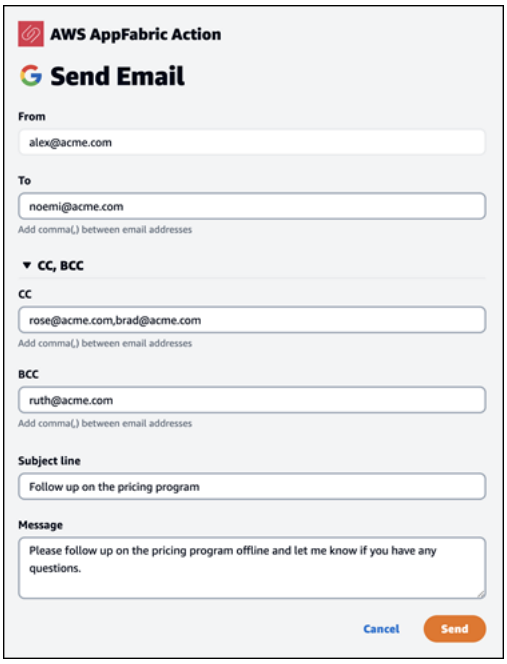
E メールの作成 (Google Workspace、Microsoft 365)

AppFabric を使用すると、任意のアプリケーション内から E メールを編集して送信できます。From、To、Cc/Bcc、E メール件名、E メール本文メッセージなどの基本的な E メールフィールドがサポートされています。 AppFabric は、これらのフィールドにコンテンツを生成して、タスク

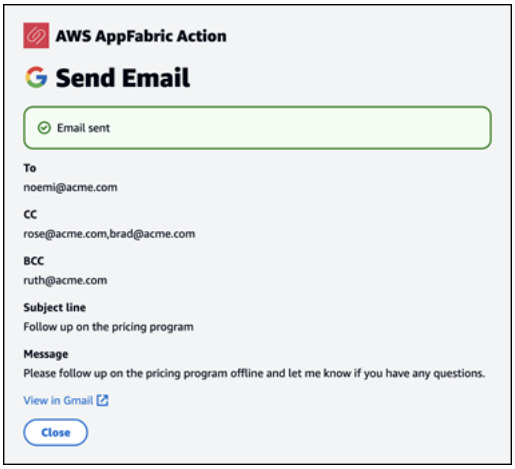
を完了する時間を短縮できます。E メールの編集が完了したら、[送信] を選択して E メールを送信します。

メールを送信するには、以下のフィールドへの入力は必須です。

- 1 つ以上の受信者の E メールアドレス (To、CC、BCC)。有効な E メールアドレスである必要があります。
- 件名と本文のフィールド。



E メールが送信されると、送信されたことを示す確認画面が表示されます。さらに、指定されたアプリケーションで E メールを表示するためのリンクが表示されます。このリンクをクリックするとアプリケーションにすばやく移動でき、メールが送信されたことを確認できます。

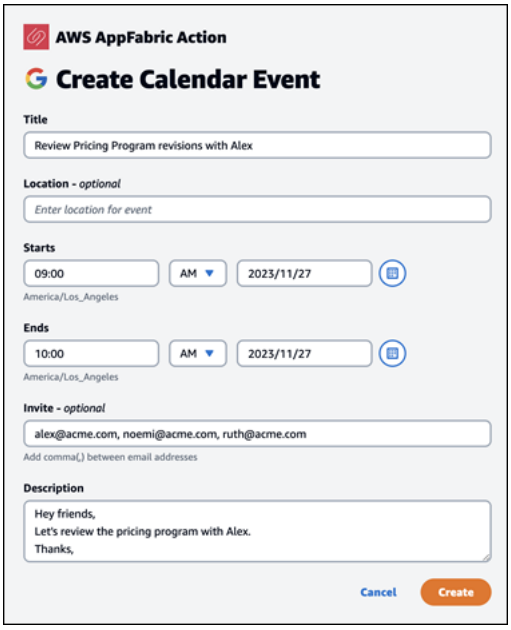


カレンダーイベントの作成 (Google Workspace、Microsoft 365)

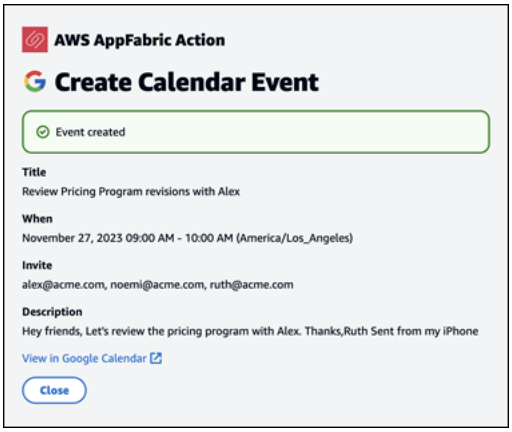
AppFabric では、任意のアプリケーション内からカレンダーイベントを編集および作成できます。イベントタイトル、ロケーション、開始/終了時刻と日付、招待者リスト、イベントの詳細などの基本的なカレンダーイベントフィールドがサポートされています。 AppFabric は、これらのフィールドにコンテンツを生成して、タスクを完了する時間を短縮できます。カレンダーイベントの編集が完了したら、[作成] を選択してイベントを作成します。

カレンダーイベントを作成するときは、以下のフィールドへの入力は必須です。

- タイトル、開始日時、終了日時、イベントの内容。
- 開始日時は終了日時より前にすることはできません。
- 招待フィールドは任意ですが、入力する場合は有効な E メールアドレスを入力する必要があります。



カレンダーイベントを送信すると、イベントが作成されたことを示す確認画面が表示されます。さらに、指定されたアプリケーションでイベントを表示するためのリンクが表示されます。このリンクをクリックするとアプリケーションにすばやく移動でき、イベントが作成されたことを確認できます。

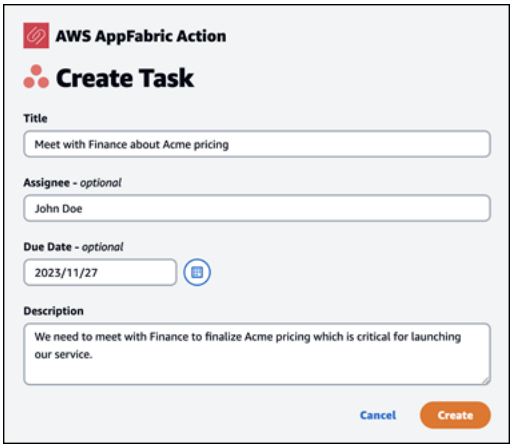


タスクの作成 (Asana)

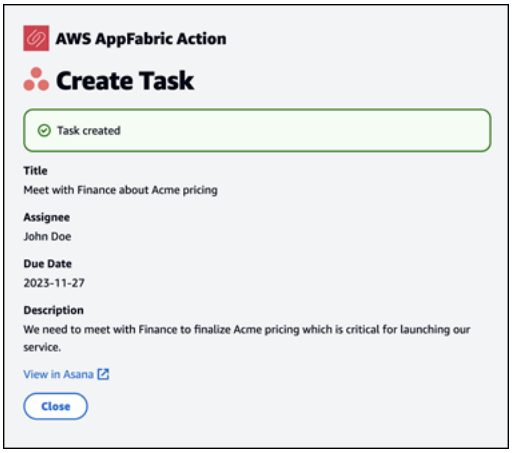
AppFabric では、任意のアプリケーション内Asanaから でタスクを編集および作成できます。タスク名、タスク所有者、期限日、タスク説明などの基本的なタスクフィールドがサポートされています。AppFabric は、これらのフィールドにコンテンツを生成して、タスクの作成時間を短縮できます。タスクの編集が完了したら、[作成] を選択してタスクを作成します。タスクは、LLM の推奨に従って、該当する Asana ワークスペース、プロジェクト、タスクのいずれかに作成されます。

Asana タスクを作成するときは、以下のフィールドへの入力は必須です。

- タイトルと内容。
- 変更された場合、担当者には有効な E メールアドレスを入力しなければなりません。



タスクが作成されると、Asana にタスクが作成されたことを示す確認画面が表示されます。さらに、Asana のタスクを確認できるリンクも表示されます。このリンクをクリックすると、アプリケーションにすばやく移動でき、タスクが作成されたことを確認したり、タスクを該当する Asana ワークスペース、プロジェクト、またはタスクに移動させたりすることができます。

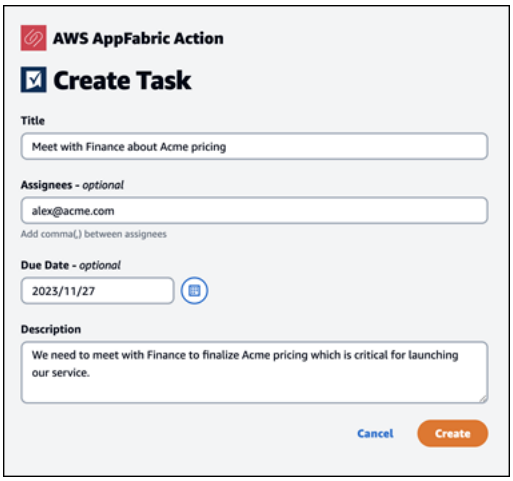


タスクの作成 (Smartsheet)

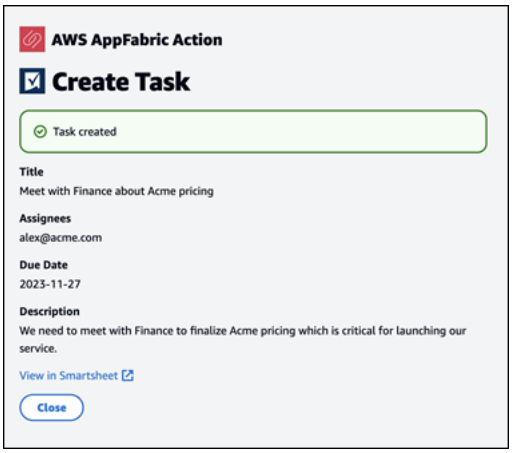
AppFabric では、任意のアプリケーション内Smartsheetから でタスクを編集および作成できます。タスク名、タスク所有者、期限日、タスク説明などの基本的なタスクフィールドがサポートされています。 AppFabric は、これらのフィールドにコンテンツを生成して、タスクの作成時間を短縮できます。タスクの編集が完了したら、[作成] を選択してタスクを作成します。Smartsheet タスクの場合、 AppFabric は新しいプライベートSmartsheetシートを作成し、作成されたタスクを入力します。これは、 AppFabric 生成されたアクションを構造化された方法で 1 か所に一元化するために行われます。

Smartsheet タスクを作成するときは、以下のフィールドへの入力は必須です。

- タイトルと内容。
- 入力された場合、担当者には有効な E メールアドレスを入力しなければなりません。



タスクが作成されると、Smartsheet にタスクが作成されたことを示す確認画面が表示されます。さらに、Smartsheet のタスクを確認できるリンクも表示されます。このリンクをクリックすると、アプリケーションにすばやく移動して、作成された Smartsheet シートにあるタスクを確認できます。今後作成される Smartsheet のタスクは、すべてこのシートに入力されます。シートが削除されると、新しいシート AppFabric が作成されます。



IT 管理者とセキュリティ管理者に注意: 生産性 AppFabric 向上のための へのアクセスの管理 (プレビュー) 機能

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

AppFabric for productivity ユーザーポータルは、 for AppFabric productivity (プレビュー) 機能を と統合している SaaS アプリケーションのすべてのユーザーがパブリックにアクセスできます。こうした生成 AI 機能へのアクセスを組織内で管理したいと考えている IT 管理者の方は、以下の方法を検討できます。

- ID プロバイダー (IdP) ログインを制限する: ID プロバイダー経由のログインアクセスをブロックすることで、生成 AI 機能へのユーザーアクセスを制御できます。
- 特定のアプリケーションの OAuth を無効にする: OAuth を無効にすることで、ダウンストリームで制限を実行できます。このアクションをとると、ユーザーは、OAuth 認証を必要とするアプリケーションを会社のワークスペースに接続できなくなります。

トラブルシューティング

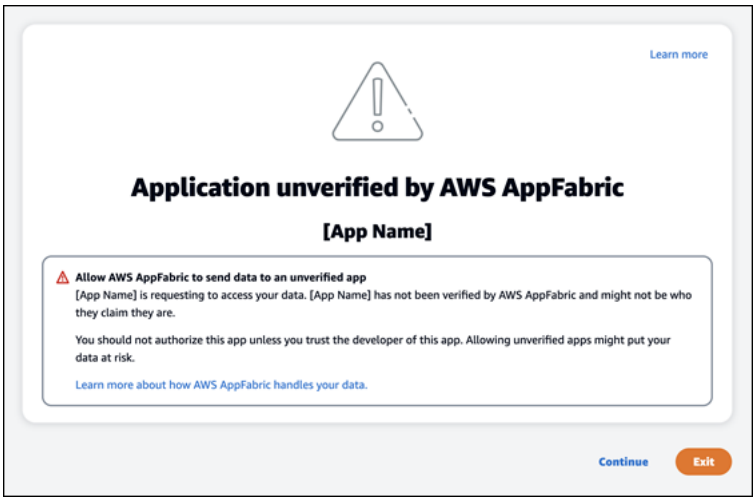
AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

このセクションでは、生産性 AppFabric 向上のための一般的なエラーとトラブルシューティングについて説明します。

未検証のアプリケーション

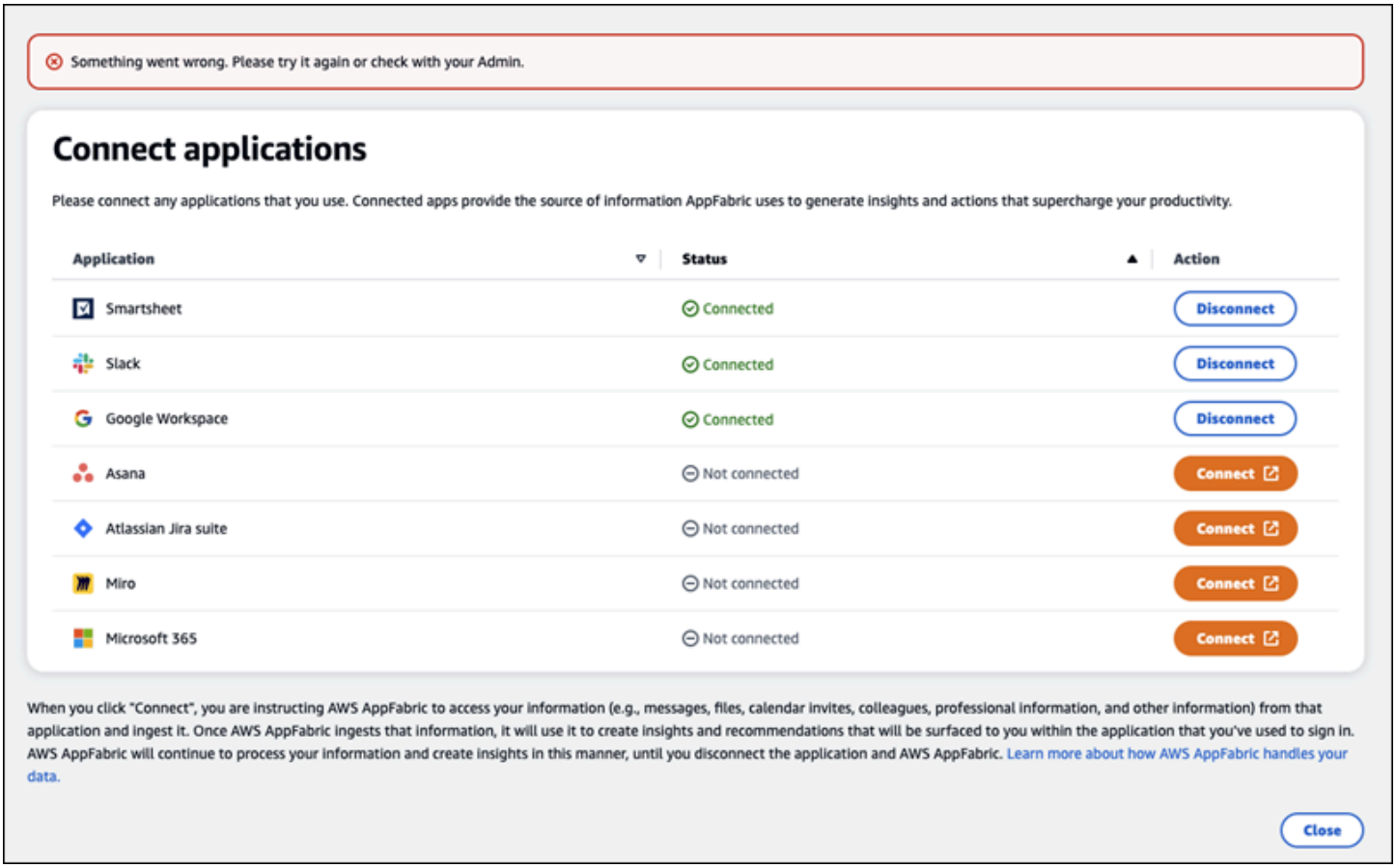
for AppFabric productivity を使用してアプリケーションエクスペリエンスを強化するアプリケーションは、エンドユーザーに機能を起動する前に検証プロセスを実行します。にサインインしようとしたときに「未検証」バナーが表示された場合は AppFabric、アプリケーションが AppFabricの検証プロセスを受けておらず、アプリケーション開発者のアイデンティティとアプリケーションの登録情報の精度が確認されていることを意味します。アプリケーションはすべて、未検証の状態からスタートし、検証プロセスが完了した場合のみ、検証済みの状態になります。

未検証のアプリケーションを使用するときは注意が必要です。アプリケーションの開発者が不明である場合は、ステータスが検証済みに変わってから使用を開始するようにします。



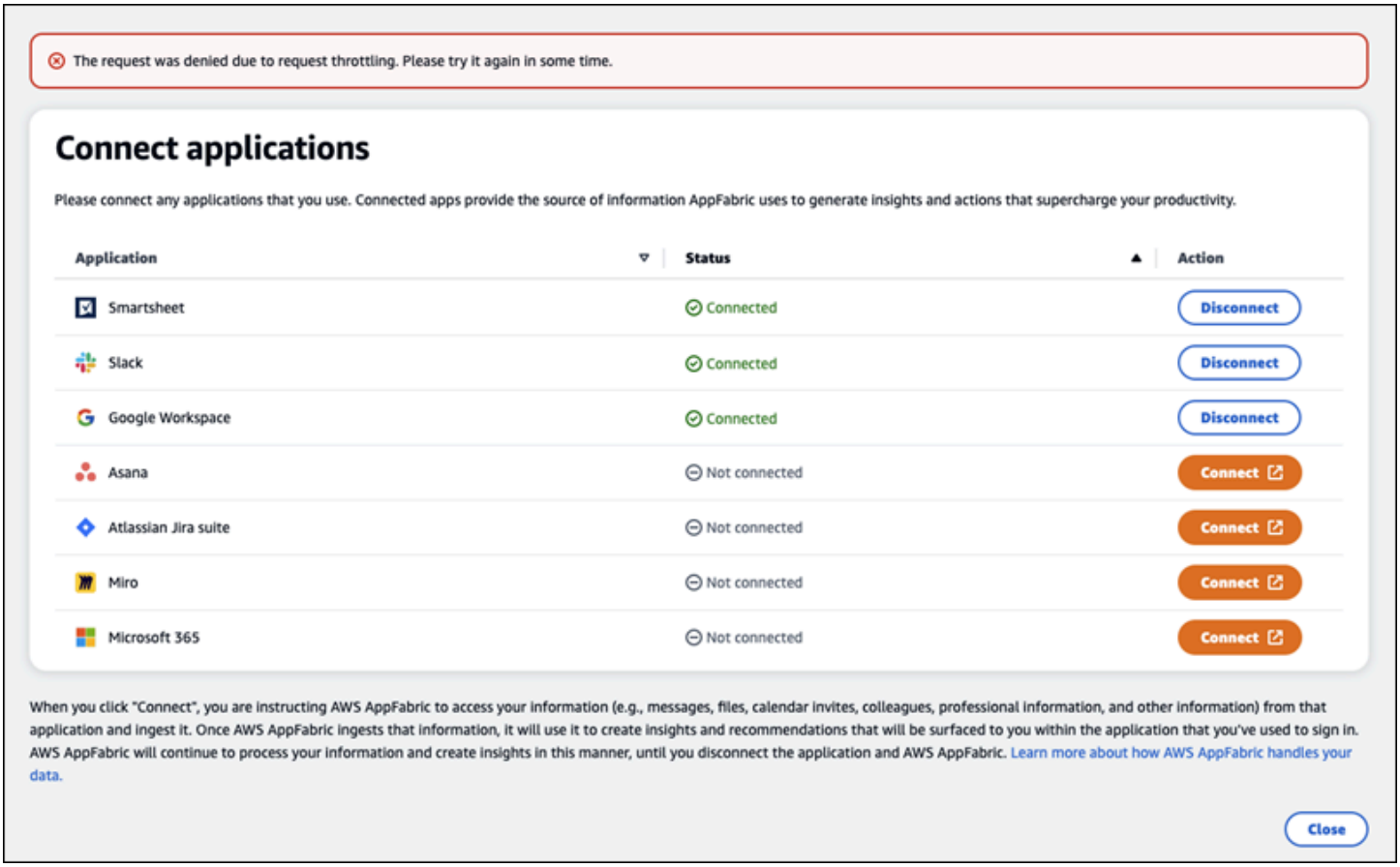
問題が発生しました。もう一度試すか、管理者に確認します (**`InternalServerException`**)。

このメッセージは、不明なエラー、例外、または障害により、 AppFabric ユーザーポータルがアプリケーションを一覧表示できなかったり、アプリケーションを切断したりした場合に表示されることがあります。後ほどもう一度試してください。」



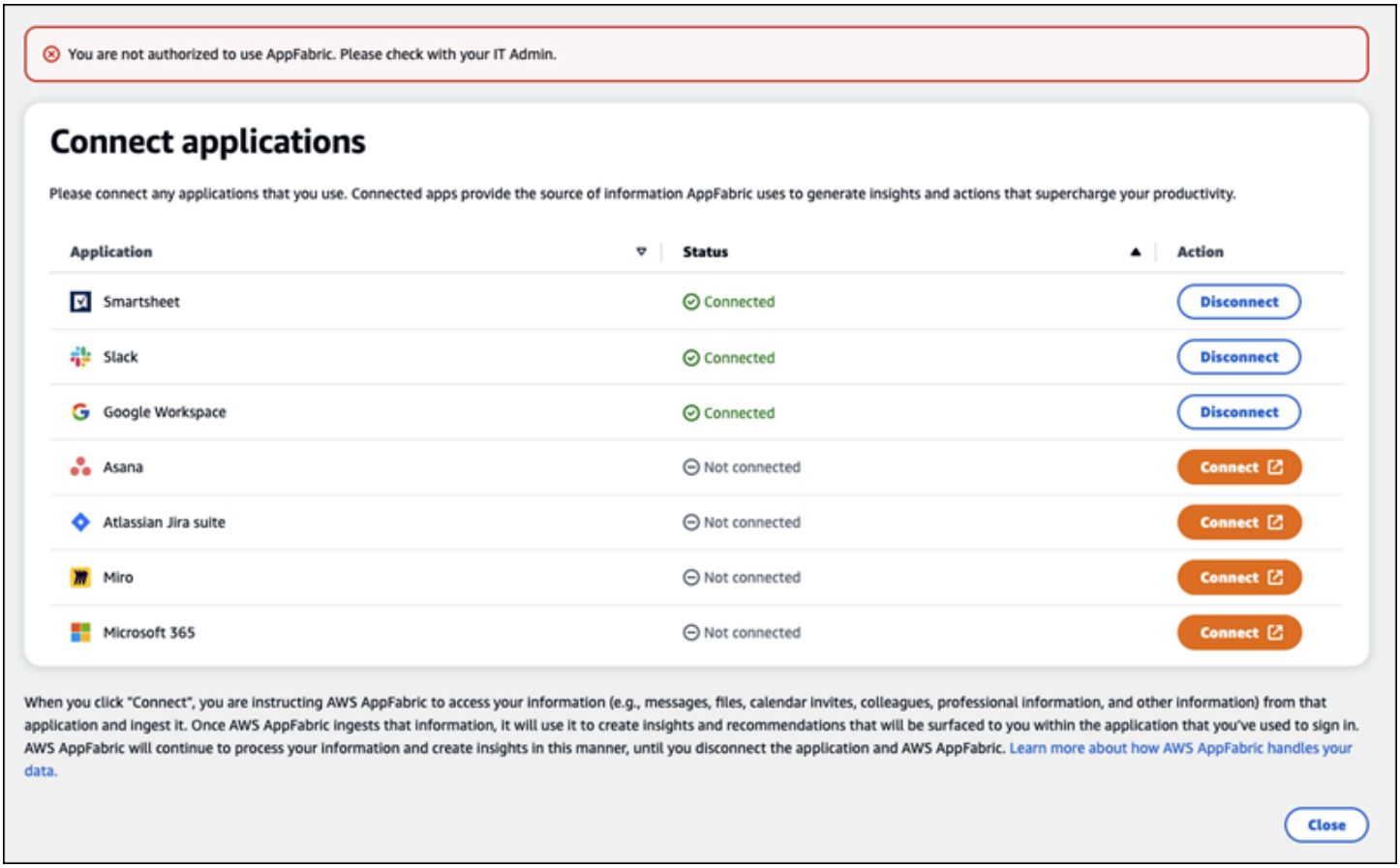
リクエストのスロットリングにより、リクエストが拒否されました。しばらくしてからもう一度試してください (**`ThrottlingException`**)。

このメッセージは、 AppFabric ユーザーポータルがアプリケーションの一覧表示に失敗した場合や、スロットリングの問題によりアプリケーションを切断した場合に表示されることがあります。後ほどもう一度試してください。」



を使用する権限がありません AppFabric。に AppFabric 再度ログインしてください (**`AccessDeniedException`**)

このメッセージは、アクセス拒否の例外により、 AppFabric ユーザーポータルがアプリケーションの一覧表示に失敗したり、アプリケーションを切断したりすると表示されることがあります。に AppFabric 再度サインインします。



AppFabric productivity APIs

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

このセクションでは、生産性向上機能の API オペレーション、データ型、一般的なエラーについて説明します AWS AppFabric。

> **Note**
>
> 他のすべての AppFabric APIsAWS AppFabric リファレンス」を参照してください。

トピック

- アクション
- データ型
- 一般的なエラー

アクション

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

AppFabric 生産性機能では、以下のアクションがサポートされています。

他のすべての AppFabric API アクションについては、AWS AppFabric 「 API アクション」を参照してください。

トピック

- 承認
- CreateAppClient
- DeleteAppClient
- GetAppClient
- ListActionableInsights
- ListAppClients
- ListMeetingInsights
- PutFeedback
- トークン
- UpdateAppClient

承認

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

を承認します AppClient。

トピック

- リクエスト本文

リクエスト本文

リクエストは以下の JSON 形式のデータを受け入れます。

パラメータ	説明
app_client_id	承認 AppClient する の ID。
redirect_uri	承認後にエンドユーザーがリダイレクトされる URI です。
state	リクエストとコールバック間の状態を維持するための一意の値です。

CreateAppClient

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

を作成します AppClient。

トピック

- リクエスト本文
- レスポンス要素

リクエスト本文

リクエストは以下の JSON 形式のデータを受け入れます。

パラメータ	説明
appName	アプリケーションの名前。 型: 文字列 長さの制限：最小長は 1 です。最大長は 255 です。 必須: はい
clientToken	リクエストの冪等性のために割り当てる一意の識別子 (大文字と小文字を区別) を指定します。これにより、同じ操作を誤って 2 度実行することなく、リクエストを安全に再試行できます。操

パラメータ	説明
	作の後半の呼び出しで同じ値を渡す場合は、他のすべてのパラメータにも同じ値を渡す必要があります。UUID タイプの値を使用することが推奨されます。 この値を指定しない場合、 はランダムな値 AWS を生成します。 同じ `ClientToken` を使って、異なるパラメータで操作を再試行すると、再試行は `IdempotentParameterMismatch` のエラーにより失敗します。 型: 文字列 パターン：`[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必須: いいえ
customerManagedKey識別子	によって カスタマー管理キー 生成された の ARN AWS Key Management Service。このキーはデータの暗号化に使用します。 キーが指定されていない場合は、 AWS マネージドキー が使用されます。リソースに割り当てるタグの、キーと値のペアのマップ。 AWS 所有のキー およびカスタマーマネージドキーの詳細については、「 AWS Key Management Service デベロッパーガイド」の「カスタマーキーと AWS キー」を参照してください。 型: 文字列 長さの制限：最小長は 1 です。最大長は 1,011 です。 Pattern: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必須: いいえ

パラメータ	説明
[Description] (説明)	アプリケーションの説明です。 型: 文字列 必須: はい
iconUrl	のアイコンまたはロゴへの URL AppClient。 タイプ: 文字列 必須: いいえ
redirectUrls	承認後にエンドユーザーがリダイレクトされる URI です。redirectUrls は 5 個まで追加できます。例えば、`https://localhost:8080` などです。 タイプ：文字列の配列 配列メンバー: 最小数は 1 項目です。最大数は 5 項目です。 長さの制限：最小長は 1 です。最大長は 2,048 です。 Pattern: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` 必須：はい
starterUserEmails	AppClient が検証されるまでインサイトを受け取るアクセスが許可されているユーザーのスターター E メールアドレス。 タイプ：文字列の配列 配列メンバー: 定数は 1 項目です。 長さの制限: 最小長は 0 です。最大長は 320 です。 Pattern: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` 必須：はい

パラメータ	説明
タグ	リソースに割り当てるタグの、キーと値のペアのマップ。 タイプ: タグオブジェクトの配列 配列メンバー：最小数は 0 項目です。最大数は 50 項目です。 必須: いいえ

レスポンス要素

アクションが成功すると、HTTP 201 レスポンスが返されます。

サービスから以下のデータが JSON 形式で返されます。

パラメータ	説明
appClientSummary	の概要が含まれます AppClient。 タイプ：AppClientSummary オブジェクト

DeleteAppClient

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

アプリケーションクライアントを削除します。

トピック

- リクエスト本文
- レスポンス要素

リクエスト本文

リクエストは以下の JSON 形式のデータを受け入れます。

パラメータ	説明
appClientIdentifier	リクエスト AppClient に使用する の Amazon リソースネーム (ARN) またはユニバーサル一意識別子 (UUID)。 長さの制限：最小長は 1 です。最大長は 1,011 です。 Pattern: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必須：はい

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 204 レスポンスを返します。

GetAppClient

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

に関する情報を返します AppClient。

トピック

- リクエスト本文
- レスポンス要素

リクエスト本文

リクエストは以下の JSON 形式のデータを受け入れます。

パラメータ	説明
appClientIdentifier	リクエスト AppClient に使用する の Amazon リソースネーム (ARN) またはユニバーサル一意識別子 (UUID)。 長さの制限：最小長は 1 です。最大長は 1,011 です。

パラメータ	説明
	Pattern: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必須：はい

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

パラメータ	説明
appClient	に関する情報が含まれます AppClient。 タイプ：AppClient オブジェクト

ListActionableInsights

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

実行可能な E メールメッセージ、タスク、その他の更新の最も重要なものを一覧表示します。

トピック

- リクエスト本文
- レスポンス要素

リクエスト本文

リクエストは以下の JSON 形式のデータを受け入れます。

パラメータ	説明
nextToken	`nextToken` が返された場合、その他にもまだ結果があります。`nextToken` の値は、各ページに固有のページネーション

パラメータ	説明
	トークンです。後続ページを取得するには、返されたトークンを使用して再度呼び出します。他の引数をすべて維持します。各ページネーショントークンの有効期間は 24 時間です。期限切れのページ割りトークンを使用すると、HTTP 400 InvalidToken error が返されます。

レスポンス要素

アクションが成功すると、HTTP 201 レスポンスが返されます。

サービスから以下のデータが JSON 形式で返されます。

パラメータ	説明
ActionableInsightsList	件名、説明、アクション、作成済みのタイムスタンプなど実行可能なインサイトを一覧表示します。詳細については、「ActionableInsights」を参照してください。
nextToken	`nextToken` が返された場合、その他にもまだ結果があります。`nextToken` の値は、各ページに固有のページネーショントークンです。後続ページを取得するには、返されたトークンを使用して再度呼び出します。他の引数をすべて維持します。各ページネーショントークンの有効期間は 24 時間です。期限切れのページ割りトークンを使用すると、HTTP 400 InvalidToken error が返されます。 型: 文字列

ListAppClients

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

すべての のリストを返します AppClients。

トピック

- リクエスト本文
- レスポンス要素

リクエスト本文

リクエストは以下の JSON 形式のデータを受け入れます。

パラメータ	説明
maxResults	コールごとに返される結果の最大数です。`nextToken` を使用すると結果ページをさらに取得できます。 こちらはあくまでも上限です。1 回のコールで返される実際の結果が、指定の最大数より少なくなる場合もあります。 有効範囲: 最小値は 1 です。最大値は 100 です。
nextToken	`nextToken` が返された場合、その他にもまだ結果があります。`nextToken` の値は、各ページに固有のページネーショントークンです。後続ページを取得するには、返されたトークンを使用して再度呼び出します。他の引数をすべて維持します。各ページネーショントークンの有効期間は 24 時間です。期限切れのページ割りトークンを使用すると、HTTP 400 InvalidToken error が返されます。

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

パラメータ	説明
appClientList	AppClient 結果のリストが含まれます。 型: AppClientSummary オブジェクトの配列
nextToken	`nextToken` が返された場合、その他にもまだ結果があります。`nextToken` の値は、各ページに固有のページネーション

パラメータ	説明
	トークンです。後続ページを取得するには、返されたトークンを使用して再度呼び出します。他の引数をすべて維持します。各ページネーショントークンの有効期間は 24 時間です。期限切れのページ割りトークンを使用すると、HTTP 400 InvalidToken error が返されます。 型: 文字列

ListMeetingInsights

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

実行可能なカレンダーイベントの最も重要なものを一覧表示します。

トピック

- リクエスト本文
- レスポンス要素

リクエスト本文

リクエストは以下の JSON 形式のデータを受け入れます。

パラメータ	説明
nextToken	`nextToken` が返された場合、その他にもまだ結果があります。`nextToken` の値は、各ページに固有のページネーショントークンです。後続ページを取得するには、返されたトークンを使用して再度呼び出します。他の引数をすべて維持します。各ページネーショントークンの有効期間は 24 時間です。期限切れのページ割りトークンを使用すると、HTTP 400 InvalidToken error が返されます。

レスポンス要素

アクションが成功すると、HTTP 201 レスポンスが返されます。

サービスから以下のデータが JSON 形式で返されます。

パラメータ	説明
MeetingInsightList	会議に関する実行可能なインサイトを一覧表示します。詳細については、「MeetingInsights」を参照してください。
nextToken	`nextToken` が返された場合、その他にもまだ結果があります。`nextToken` の値は、各ページに固有のページネーショントークンです。後続ページを取得するには、返されたトークンを使用して再度呼び出します。他の引数をすべて維持します。各ページネーショントークンの有効期間は 24 時間です。期限切れのページ割りトークンを使用すると、HTTP 400 InvalidToken error が返されます。 型: 文字列

PutFeedback

> AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

特定のインサイトまたはアクションに関するフィードバックを送ることをユーザーに許可します。

トピック

- リクエスト本文
- レスポンス要素

リクエスト本文

リクエストは以下の JSON 形式のデータを受け入れます。

パラメータ	説明
id	フィードバックの送信対象となるオブジェクトの ID です。これは、 InsightId または のいずれかです ActionId。
feedbackFor	フィードバックの送信対象となるインサイトのタイプです。 使用できる値: `ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION`
feedbackRating	1 から 5 までの評価です。値が大きいほど評価が高いことを意味します。

レスポンス要素

アクションが成功した場合、サービスは空の HTTP 本文を持つ HTTP 201 レスポンスを返します。

トークン

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

が認証コードをアクセストークンと交換 AppClients できるようにする情報が含まれています。

トピック

- リクエスト本文
- レスポンス要素

リクエスト本文

リクエストは以下の JSON 形式のデータを受け入れます。

パラメータ	説明
コード	認証エンドポイントから受信した認証コードです。 型: 文字列

パラメータ	説明
	長さの制限：最小長は 1 です。最大長は 2,048 です。 必須: いいえ
grant_type	トークンの付与のタイプ。`authorization_code` または `refresh_token` である必要があります。 型: 文字列 必須: はい
app_client_id	AppClient の ID。 型: 文字列 Pattern: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必須：はい
redirect_uri	認証エンドポイントに渡されたリダイレクト URI。 タイプ: 文字列 必須: いいえ
refresh_token	最初のトークンリクエストで受け取った更新トークンです。 型: 文字列 長さの制限：最小長は 1 です。最大長は 4,096 です。 必須: いいえ

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

パラメータ	説明
appfabric_user_id	トークン用のユーザーの ID。この値は、リクエストが `authorization_code` グラントタイプを使用している場合のみ返されます。 型: 文字列
expires_in	トークンの有効期限が切れるまでの残りの秒数。 型: 長整数
refresh_token	次のリクエストに使用する更新トークンです。 型: 文字列 長さの制限：最小長は 1 です。最大長は 2,048 です。
token (トークン)	アクセストークンです。 型: 文字列 長さの制限：最小長は 1 です。最大長は 2,048 です。
token_type	トークンのタイプです。 型: 文字列

UpdateAppClient

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

を更新します AppClient。

トピック

- リクエスト本文
- レスポンス要素

リクエスト本文

リクエストは以下の JSON 形式のデータを受け入れます。

パラメータ	説明
appClientIdentifier	リクエスト AppClient に使用する の Amazon リソースネーム (ARN) またはユニバーサル一意識別子 (UUID)。 長さの制限：最小長は 1 です。最大長は 1,011 です。 Pattern: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必須：はい
redirectUrls	承認後にエンドユーザーがリダイレクトされる URI です。redirectUrls は 5 個まで追加できます。例えば、`https://localhost:8080` などです。 タイプ：文字列の配列 配列メンバー: 最小数は 1 項目です。最大数は 5 項目です。 長さの制限：最小長は 1 です。最大長は 2,048 です。 Pattern: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

レスポンス要素

アクションが成功すると、サービスは HTTP 200 レスポンスを返します。

サービスから以下のデータが JSON 形式で返されます。

パラメータ	説明
appClient	に関する情報が含まれます AppClient。 タイプ：AppClient オブジェクト

データ型

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

AppFabric API には、さまざまなアクションが使用する複数のデータ型が含まれています。このセクションでは、 AppFabric 生産性向上機能のデータ型について詳しく説明します。

他のすべての AppFabric API データ型については、AWS AppFabric 「 API データ型」を参照してください。

> **Important**
> データ型構造内の各要素の順序は保証されません。アプリケーションは特定の順序を想定するべきではありません。

トピック

- ActionableInsights
- AppClient
- AppClientSummary
- MeetingInsights
- VerificationDetails

ActionableInsights

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

アプリケーションポートフォリオの E メール、カレンダーの招待、メッセージ、タスクに基づく、ユーザーにとって重要かつ最も適したアクションの概要が含まれます。ユーザーは、すべてのアプリケーションを横断する先を見越したインサイトを確認でき、その日の最適な進め方を確認することができます。これらのインサイトを見れば、ユーザーが、インサイトのサマリーだけでなく、インサイトを生成した、各アプリケーションやアーティファクトなどの参照情報 (埋め込みリンクなど) にも目を向けるべき理由がわかります。

パラメータ	説明
insightId	生成されたインサイトの一意の ID です。
insightContent	インサイトの概要と、インサイトの生成に使用されたアーティファクトへの埋め込みリンクを返します。 こちらは、埋め込みリンク (<a> タグ) を含む HTML コンテンツです。
insightTitle	生成されたインサイトの件名です。
createdAt	インサイトが生成された日時です。
actions	生成されたインサイトで推奨されるアクションのリストです。 アクションオブジェクトには、以下のパラメータが含まれています。 • `actionId` - 生成されたアクションの一意の ID です。 • `actionIconUrl` - アクションの実行が推奨されているアプリケーションのアイコン URL です。 • `actionTitle` - 生成されたアクションの件名です。 • `actionUrl` — のユーザー AppFabricポータルでアクションを表示および実行するエンドユーザーの一意の URL。 アクションを実行する場合、ISV アプリケーションはこの URL を使用してユーザーを AppFabric ユーザーポータル (ポップアップ画面) にリダイレクトします。 • `actionExecutionStatus` - アクションのステータスを示す列挙型です。 指定できる値: `EXECUTED` | `NOT_EXECUTED`

AppClient

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

に関する情報が含まれます AppClient。

パラメータ	説明
appName	アプリケーションの名前。 型: 文字列 必須: はい
arn	の Amazon リソースネーム (ARN) AppClient。 型: 文字列 長さの制限：最小長は 1 です。最大長は 1,011 です。 Pattern: `arn:.+` 必須：はい
[Description] (説明)	アプリケーションの説明です。 型: 文字列 必須: はい
iconUrl	のアイコンまたはロゴへの URL AppClient。 タイプ: 文字列 必須: いいえ
redirectUrls	に許可されるリダイレクト URLs AppClient。 タイプ：文字列の配列 配列メンバー: 最小数は 1 項目です。最大数は 5 項目です。 長さの制限：最小長は 1 です。最大長は 2,048 です。 Pattern: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

パラメータ	説明
	必須：はい
starterUserEmails	AppClient が検証されるまでインサイトを受け取るアクセスが許可されているユーザーのスターター E メールアドレス。 タイプ：文字列の配列 配列メンバー: 定数は 1 項目です。 長さの制限: 最小長は 0 です。最大長は 320 です。 Pattern: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` 必須：はい
verificationDetails	検証のステータスと理由が含まれます AppClient。 型: VerificationDetails オブジェクト 必須: はい
customerManagedKeyArn	AWS Key Management Service の によって生成された の カスタマー管理キー Amazon リソースネーム (ARN) AppClient。 型: 文字列 長さの制限：最小長は 1 です。最大長は 1,011 です。 Pattern: `arn:.+` 必須: いいえ

パラメータ	説明
appClientId	AppClient の ID。app-client の o-auth フローで使用される手段。 型: 文字列 パターン：`[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必須: いいえ

AppClientSummary

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

に関する情報が含まれます AppClient。

パラメータ	説明
arn	の Amazon リソースネーム (ARN) AppClient。 型: 文字列 長さの制限：最小長は 1 です。最大長は 1,011 です。 Pattern: `arn:.+` 必須：はい
verificationStatus	AppClient 検証ステータス。 型: 文字列 有効な値：`pending_verification | verified | rejected` 必須: はい

パラメータ	説明
appClientId	AppClient の ID。app-client の o-auth フローで使用される手段。 型: 文字列 パターン：`[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必須: いいえ

MeetingInsights

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

上位 3 件の会議の概要と、会議の目的、関連するクロスアプリケーションアーティファクト、また、タスク、E メール、メッセージ、カレンダーイベントのアクティビティが含まれます。

パラメータ	説明
insightId	生成されたインサイトの一意の ID です。
insightContent	インサイトの説明で、詳細が文字列の形式で強調表示されています。例えば、なぜこのインサイトが重要なのか、など。
insightTitle	生成されたインサイトの件名です。
createdAt	インサイトが生成された日時です。
calendarEvent	ユーザーが注意すべき重要なカレンダーイベントまたは会議です。 カレンダーイベントオブジェクト: • `startTime` - イベントの開始時刻です。 • `endTime` - イベントの終了時刻です。

パラメータ	説明
	• `eventUrl` - ISV アプリケーションのカレンダーイベントの URL です。
resources	インサイトの生成に関連する他のリソースを含むリストです。 リソースオブジェクト: • `appName` - リソースが属するアプリケーションの名前です。 • `resourceTitle` - リソースの件名です。 • `resourceType` - リソースのタイプです。 指定できる値は以下のとおりです。`EMAIL` | `EVENT` | `MESSAGE` | `TASK` • `resourceUrl` - アプリケーション内のリソース URL です。 • `appIconUrl` - リソースが属するアプリケーションの画像 URL です。
nextToken	次回のインサイトのセットを取得するためのページネーショントークンです。こちらはオプションのフィールドで、null が返された場合は、ロードするインサイトがそれ以上ないことを意味します。

VerificationDetails

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

AppClient 検証のステータスと理由が含まれます。

パラメータ	説明
verificationStatus	AppClient 検証ステータス。 型: 文字列

パラメータ	説明
	有効な値：`pending_verification | verified | rejected` 必須: はい
statusReason	AppClient 検証ステータスの理由。 型: 文字列 長さの制限: 最小長は 1 です。最大長は 1,024 です。 必須: いいえ

一般的なエラー

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

このセクションでは、 AWS AppFabric 生産性向上機能の API アクションに共通するエラーを一覧表示します。

その他の AppFabric 一般的な API エラーについては、「 API リファレンス」のトラブルシューティング「」およびAWS AppFabric 「 API の一般的なエラー」を参照してください。 AWS AppFabric

例外名	説明
TokenException	トークンリクエストは無効です。 HTTP ステータスコード：400

データ処理

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

AppFabric は、ユーザーコンテンツを個別に、 によって管理される Amazon S3 バケットに AppFabric、および個別に保存するステップを実行します。これにより、ユーザー固有のインサイトを確実に生成できます。ユーザーのコンテンツは、保管時および転送中の暗号化を含め、合理的な手段を講じて保護しています。Ingestion から 30 日以内に顧客コンテンツを自動的に削除するようにシステムを設定しました。ユーザーがアクセスできなくなったデータアーティファクトを使用してインサイトは生成 AppFabric されません。例えば、ユーザーがデータソース (アプリ) を切断すると、 はそのアプリからのデータ収集 AppFabric を停止し、切断されたアプリからの残りのアーティファクトを使用してインサイトを生成します。 AppFabricのシステムは、30 日以内にそのようなデータを削除するように設定されています。

AppFabric は、インサイトの生成に使用される基盤となる大規模言語モデルのトレーニングや改善にユーザーコンテンツを使用しません。の生成 AI 機能の詳細については、 AppFabric「Amazon Bedrock のFAQs」を参照してください。

保管中の暗号化

AWS AppFabric は、保管時の暗号化をサポートします。これは、ディスクに保持されているユーザーに関連するすべてのデータを AppFabric 透過的に暗号化し、データにアクセスするときに復号するサーバー側の暗号化機能です。

転送中の暗号化

AppFabric は、TLS 1.2 を使用して転送中のすべてのコンテンツを保護し、 AWS 署名バージョン 4 で AWS サービスの API リクエストに署名します。

用語と概念

このトピックでは、使用開始 AWS AppFabric に役立つ の主要な用語と概念について説明します。

アプリバンドル

AppFabric アプリケーションバンドルには、すべての AppFabric アプリケーション認証と取り込みが保存されます (以下の取り込みの定義を参照) 。 AWS アカウント ごとに 1 つのアプリケーションバンドルを作成できます AWS リージョン。

AppClient （ アプリケーションクライアントとアプリケーションクライアントも ）

データ受信者アプリの OAuth AppClient 。各データ受信者アプリは、 AppFabric データにアクセス AppClient するために を登録する必要があります。デベロッパーユーザーは、 を登録するために AWS アカウントが必要です AppClient。各 AWS アカウントは 1 つの しか登録 AppFabric できません AppClient。 は、 に基づいてアクセストークンを提供します AppClient。 には、この を介してデータにアクセスする AppFabric データ受信者アプリに関する情報 AppClient が含まれます AppClient。

アプリ認証

アプリケーション認証は、アプリケーションに接続して操作する AppFabric アクセス許可を付与します。これにより、OAuth (Open Authorization - アプリケーションにアクセス権を付与するためのアクセス委任のオープン標準) または個人アクセストークン (PAT) 認証情報を使用して、アプリケーションから監査ログを取り込むことができます。アプリバンドルごとに複数のアプリ認証 (最大 50 件) を設定できます。これにより AppFabric 、アプリケーションのテナントごとに必要に応じてアプリケーション認証の作成ステップを繰り返すことで、アプリケーションの複数のテナントから監査ログを取り込むことができます。共有される認証情報は、 AWS Key Management Service （ AWS KMS) の AWS 所有のキー またはカスタマーマネージドキーで暗号化され、 に保存されます AppFabric。

取り込み

AppFabric 取り込みでは、アプリケーション認証を使用して、アプリケーションのパブリック APIs を介してアプリケーションから監査ログを取得します。続いて、監査ログが 1 件以上 (最大 5 件) の取り込み先に転送されます。

クライアント ID

OAuth フローを使用するアプリケーションに接続するためのアプリケーション認証を作成すると、クライアント ID とクライアントシークレットの入力を求められる AppFabric 場合があります。クライアント ID とクライアントシークレットは、アプリケーションの認証アプリにあります。特定の認証アプリ内のクライアント ID を確認する方法については、「サポートされているアプリケーション」を参照してください。共有されるクライアント ID とクライアントシークレットは、AWS 所有のキー またはカスタマーマネージド AWS KMS キーキーで暗号化され、 に保存されます AppFabric。

クライアントシークレット

OAuth フローを使用するアプリケーションに接続するためのアプリケーション認証を作成すると、クライアント ID とクライアントシークレットの入力を求められる AppFabric 場合があります。クライアント ID とクライアントシークレットは、アプリケーションの認証アプリにあります。特定の認証アプリ内のクライアントシークレットを確認する方法については、「サポートされているアプリケーション」を参照してください。共有されるクライアント ID とクライアントシークレットは、AWS 所有のキー またはカスタマーマネージド AWS KMS キーキーで暗号化され、 に保存されます AppFabric。

取り込み先

取り込み先は 、取り込みから取得した監査ログの保存場所を定義します。各取り込みでは、監査ログを 1 つ以上の送信先 (最大 5 つ) に配信できます。送信先は、Amazon Simple Storage Service (Amazon S3) バケットまたは 内の Amazon Data Firehose です AWS アカウント。取り込み先ごとに、ログを raw 形式にするか、オープンサイバーセキュリティスキーマフレームワーク (OCSF) スキーマに正規化するかを定義できます。OCSF スキーマを選択すると、ログの形式 (JSON または Apache Parquet) を定義できます。Apache Parquet 形式は、Amazon S3 が取り込み先として選択されている場合にのみ使用できます。

データ受信者アプリ

から生成されたインサイトを取得 AppFabric するために を呼び出すアプリ AppFabric。

OAuth

OAuth は、ウェブ、モバイル、デスクトップアプリケーションからのシンプルで標準的な方法で安全な認証を可能にするオープンプロトコルです。 は OAuth AppFabric を使用していくつかのアプリケーション認証を作成します。

オープン・ サイバーセキュリティ・ スキーマ・ フレームワーク (OCSF)

オープンサイバーセキュリティスキーマフレームワーク (OCSF) は、ベンダーに依存しないコアセキュリティスキーマと並んで、スキーマを開発するための拡張可能なフレームワークを提供するオープンソースプロジェクトです。ベンダーやその他のデータプロデューサーは、このスキーマを特定のドメインに採用したり拡張したりできます。その目標は、既存のセキュリティ標準やプロセスを補完しながら、あらゆる環境、アプリケーション、ソリューションで採用されるオープン標準を提供することです。 AppFabric はこのスキーマを拡張して、 でサポートされているすべての SaaS アプリケーション監査ログを正規化する Software as a Service (SaaS) 中心のイベント構造を作成 AppFabric しました。詳細については、「オープンサイバーセキュリティスキーマフレームワーク」を参照してください。

個人アクセストークン (PAT)

個人アクセストークン (PAT) は、通常のパスワードの代わりにコンピューターシステムへのアクセスに使用できる文字列です。PAT フローを使用するアプリケーションに接続するためのアプリケーション認証を作成すると、PAT を求められる AppFabric 場合があります。PAT は、アプリケーションの認証アプリにあります。特定の認証アプリで PAT の場所を確認する方法については、「サポートされているアプリケーション」を参照してください。共有されるサービスアカウントトークンは、 AWS 所有のキー またはカスタマーマネージド AWS KMS キーで暗号化され、 に保存されます AppFabric。

サービスアカウントトークン

AppFabric アプリケーションに接続するためのアプリケーション認証を作成する場合、一部のアプリケーションでは、アプリケーション認証用にサービスアカウントを作成する必要があります。アプリケーション認証プロセスの一環として、サービスアカウントトークンを要求する AppFabric 場合があります。特定の認証アプリ内のサービスアカウントトークンの場所については、「サポートされているアプリケーション」を参照してください。共有されるサービスアカウントトークンは、 AWS 所有のキー またはカスタマーマネージド AWS KMS キーで暗号化され、 に保存されます AppFabric。

テナント ID

アプリ認証を作成するときに、アプリのテナント ID とテナント名を尋ねる AppFabric 場合があります。テナント ID は、アプリケーションテナントの一意の識別子です。アプリケーションごとに、Slack の Workspace ID 、または Asana の ドメインID など、テナントに対して使用する用語が異なる場合があります。特定のアプリケーションのテナント ID の場所を確認する方法については、「サポートされているアプリケーション」を参照してください。

テナント名

アプリ認証を作成するときに、アプリのテナント ID とテナント名を尋ねる AppFabric 場合があります。テナント名 はテナント ID に与える一意の名前で、アプリバンドル内で使用されます。この値は、アプリ認証とそれに関連するすべての取り込みを示すために使用されます。

のセキュリティ AWS AppFabric

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS は、 AWS サービス で実行されるインフラストラクチャを保護する責任を担います AWS クラウド。また、 は、お客様が安全に使用できるサービス AWS も提供します。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。に適用されるコンプライアンスプログラムの詳細については AWS AppFabric、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は AWS サービス 、使用する によって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 の使用時に責任共有モデルを適用する方法を理解するのに役立ちます AppFabric。以下のトピックでは、セキュリティおよびコンプライアンスの目的 AppFabric を達成するために を設定する方法を示します。また、 AppFabric リソースのモニタリングや保護 AWS サービス に役立つ他の の使用方法についても説明します。

トピック

- でのデータ保護 AWS AppFabric
- の Identity and Access Management AWS AppFabric
- のコンプライアンス検証 AWS AppFabric
- のセキュリティのベストプラクティス AWS AppFabric
- の耐障害性 AWS AppFabric
- のインフラストラクチャセキュリティ AWS AppFabric
- での設定と脆弱性の分析 AWS AppFabric

でのデータ保護 AWS AppFabric

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS AppFabric。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS サービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシー FAQ」を参照してください。欧州でのデータ保護の詳細については、AWS 「 セキュリティブログ」のAWS 「責任共有モデル」とGDPRブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management () を使用して個々のユーザーを設定することをお勧めしますIAM。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。1TLS.2 が必要で、1.3 TLS をお勧めします。
- を使用して APIとユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS サービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合はAPI、FIPSエンドポイントを使用します。利用可能なFIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、、AppFabric または を使用して または他の AWS サービス を操作する場合API AWS CLIも同様です AWS SDKs。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

> **Note**
>
> セキュリティ上の に適用されるデータ保護の詳細については、 AppFabric 「」を参照してください[データ処理](#)。

保管中の暗号化

AWS AppFabric は、保管時の暗号化をサポートします。これは、アプリケーションバンドルがディスクに保持されているときにアプリケーションバンドルに関連するすべてのデータを透過的に暗号化し、データにアクセスするときに復号するサーバー側の暗号化機能 AppFabricです。デフォルトでは、 は AWS Key Management Service () AWS 所有のキー の を使用してデータを AppFabric 暗号化しますAWS KMS。から独自のカスタマーマネージドキーを使用してデータを暗号化することもできます AWS KMS。

ユーザーを削除すると、そのユーザーのメタデータはすべて、完全に削除されます。

転送中の暗号化

アプリケーションバンドルを設定するときは、 AWS 所有のキー またはカスタマーマネージドキーのいずれかを選択できます。監査ログ取り込みのデータを収集して正規化する場合、 はデータを中間 Amazon Simple Storage Service (Amazon S3) バケットに一時的に AppFabric 保存し、このキーを使用して暗号化します。この中間バケットは、バケットライフサイクルポリシーを使用して 30 日後に削除されます。

AppFabric は 1.2 TLS を使用して転送中のすべてのデータを保護し、署名 V4 を使用して AWS の API AWS サービス リクエストに署名します。

キー管理

AppFabric は、 AWS 所有のキー またはカスタマーマネージドキーによるデータの暗号化をサポートしています。暗号化されたデータを完全に管理できるので、カスタマーマネージドキーを使用することをお勧めします。カスタマーマネージドキーを選択すると、 は、カスタマーマネージドキーへのアクセスを許可するリソースポリシーをカスタマーマネージドキーにア AppFabric タッチします。

カスタマーマネージドキー

カスタマーマネージドキーを作成するには、「 AWS KMS デベロッパーガイド[」の「対称暗号化 KMSキーの作成](#)」の手順に従います。

キーポリシー

キーポリシーは、カスタマーマネージドキーへのアクセスを制御します。すべてのカスタマーマネージドキーには、キーポリシーが 1 つだけ必要です。このポリシーには、そのキーを使用できるユーザーとその使用方法を決定するステートメントが含まれています。カスタマーマネージドキーを作成する際に、キーポリシーを指定することができます。キーポリシーの作成について詳細については、[AWS KMS デベロッパーガイド] の[キーの作成] のポリシー を参照してください。

でカスタマーマネージドキーを使用するには AppFabric、リソースを作成する AWS Identity and Access Management AppFabric (IAM) ユーザーまたはロールに、カスタマーマネージドキーを使用するアクセス許可が必要です。でのみ使用するキーを作成し AppFabric 、 AppFabric ユーザーをキーのユーザーとして追加することをお勧めします。この方法では、データへのアクセス範囲が制限されます。ユーザーが必要とする権限は次のとおりです。

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Decrypt`

AWS KMS コンソールでは、適切なキーポリシーを使用してキーを作成する手順を説明します。キーポリシーの詳細については、「AWS KMS デベロッパーガイド」の「 AWS KMSのキーポリシー」を参照してください。

以下は、それを許可するキーポリシーの例です。

- キーの完全な AWS アカウントのルートユーザー 制御。
- でカスタマーマネージドキー AppFabric の使用を許可されたユーザー AppFabric。
- アプリバンドルのキーポリシーは、でセットアップされます。`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"
                }
            }
        }
    ]
}
```

で 許可 AppFabric を使用する方法 AWS KMS

AppFabric には、カスタマーマネージドキーを使用するための許可が必要です。詳細については、「AWS KMS デベロッパーガイド」の「AWS KMSでの許可」を参照してください。

アプリケーションバンドルを作成すると、 は にCreateGrantリクエストを送信して、ユーザーに代わってグラント AppFabric を作成します AWS KMS。の権限 AWS KMS は、カスタマーアカウン

トの AWS KMS キー AppFabric へのアクセスを許可するために使用されます。 AppFabric では、次の内部オペレーションでカスタマーマネージドキーを使用する権限が必要です。

- カスタマーマネージドキーで暗号化されたデータキーを生成する AWS KMS には、にGenerateDataKeyリクエストを送信します。
- にDecryptリクエストを送信 AWS KMS して、暗号化されたデータキーを復号します。これにより、データの暗号化や転送中のアプリケーションアクセストークンの復号化に使用できます。
- 転送中のアプリケーションアクセストークンを暗号化 AWS KMS するEncryptリクエストを に送信します。

グラントの例を以下に示します。

```
{
  "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"
    }
  }
},
```

アプリバンドルを削除すると、 はカスタマーマネージドキーに対して発行された許可を AppFabric 廃止します。

の暗号化キーのモニタリング AppFabric

で AWS KMS カスタマーマネージドキーを使用する場合 AppFabric、 AWS CloudTrail ログを使用して、 AppFabric が に送信するリクエストを追跡できます AWS KMS。

以下は、 がカスタマーマネージドキー`CreateGrant`に AppFabric を使用するときにログに記録される CloudTrail イベントの例です。

```
{
    "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"
    }
}
```

の Identity and Access Management AWS AppFabric

AWS Identity and Access Management （IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS サービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AppFabric リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は追加料金なしで AWS サービス 使用できる です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- と の AWS AppFabric 連携方法 IAM
- AWS AppFabric のアイデンティティベースのポリシーの例
- AppFabric のサービスにリンクされたロールの使用
- AWS の マネージドポリシー AWS AppFabric
- AWS AppFabric ID とアクセスのトラブルシューティング

対象者

AWS Identity and Access Management （IAM) の使用方法は、 で行う作業によって異なります AppFabric。

サービスユーザー – AppFabric サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの AppFabric 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。の機能にアクセスできない場合は、 AppFabric「」を参照してくださいAWS AppFabric ID とアクセスのトラブルシューティング。

サービス管理者 – 社内の AppFabric リソースを担当している場合は、通常、 へのフルアクセスがあります AppFabric。サービスユーザーがどの AppFabric 機能やリソースにアクセスするかを決めるのは管理者の仕事です。次に、サービスユーザーのアクセス許可を変更するリクエストをIAM管理者に送信する必要があります。このページの情報を確認して、 の基本概念を理解してください IAM。会社で を使用する方法の詳細については、IAM AppFabric「」を参照してくださいと の AWS AppFabric 連携方法 IAM。

IAM 管理者 – IAM管理者の場合は、 へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります AppFabric。で使用できる AppFabric アイデンティティベースのポリシーの例を表示するにはIAM、「」を参照してください[AWS AppFabric のアイデンティティベースのポリシーの例](#)。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAMユーザーとして AWS アカウントのルートユーザー、または IAMロールを引き受けることによって認証（ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center（IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインすると、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の[「 にサインインする方法 AWS アカウント](#)AWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 はソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、「 IAMユーザーガイド」の[AWS API「リクエストの署名](#)」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用することをお勧めします。詳細については、「 AWS IAM Identity Center ユーザーガイド」の[「多要素認証](#)」および[「 ユーザーガイド」の「 での多要素認証 (MFA) AWS](#) IAM の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての AWS サービス およびリソースへの完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行

するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「 IAMユーザーガイド」の「ルートユーザーの認証情報を必要とするタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID プロバイダーとのフェデレーションを使用して一時的な認証情報 AWS サービス を使用して にアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、アイデンティティセンターディレクトリのユーザー、または ID ソースを通じて提供された認証情報 AWS サービス を使用して にアクセスするユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、「 ユーザーガイド」のIAM「Identity Center とはAWS IAM Identity Center 」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能な場合は、パスワードやアクセスキーなどの長期的な認証情報を持つIAMユーザーを作成するのではなく、一時的な認証情報を使用することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「 ユーザーガイド」の「長期的な認証情報を必要とするユースケースでアクセスキーを定期的にローテーションするIAM」を参照してください。

IAM グループは、IAMユーザーのコレクションを指定する ID です。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、という名前のグループを作成しIAMAdmins、そのグループにIAMリソースを管理するアクセス許可を付与できます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユー

ザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「 ユーザーガイド」のIAM「 (ロールの代わりに) ユーザーを作成する場合IAM」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。ユーザーと似ていますがIAM、特定のユーザーに関連付けられていません。IAM ロール を切り替える AWS Management Console ことで、 で ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム を使用しますURL。ロールの使用方法の詳細については、「 ユーザーガイド」のIAM「ロールの使用IAM」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、「 ユーザーガイド」の「サードパーティー ID プロバイダーのロールの作成IAM」を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAMIdentity Center はアクセス許可セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、 IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に引き受けることができます。
- クロスアカウントアクセス – IAMロールを使用して、別のアカウントのユーザー (信頼されたプリンシパル) がアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、ロールを使用することです。ただし、一部の では AWS サービス、 (プロキシとしてロールを使用する代わりに) リソースにポリシーを直接アタッチできます。クロスアカウントアクセスのロールとリソースベースのポリシーの違いについては、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。
- クロスサービスアクセス — 一部の は、他の の機能 AWS サービス を使用します AWS サービス。例えば、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実行EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。

- 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS サービス、ダウンストリームサービス AWS サービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS サービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
- サービスロール – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAMロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 ユーザーガイド」の「 にアクセス許可を委任するロールの作成 AWS サービスIAM」を参照してください。
- サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS サービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

- Amazon で実行されているアプリケーション EC2 – IAMロールを使用して、EC2インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2インスタンス内にアクセスキーを保存するよりも望ましいです。 AWS ロールをEC2インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルには ロールが含まれており、EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「 ユーザーガイド」の「 IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与するIAM」を参照してください。

IAM ロールとIAMユーザーのどちらを使用するかについては、「 ユーザーガイド」の「 IAMロールを作成するタイミング (ユーザーではなく) IAM」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション)

AWS がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーはJSONドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「 ユーザーガイド」のJSON「ポリシーの概要IAM」を参照してください。

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用する方法に関係なく、アクションのアクセス許可を定義します。例えば、`iam:GetRole`アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS からロール情報を取得できますAPI。

アイデンティティベースのポリシー

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。管理ポリシーとインラインポリシーのどちらかを選択する方法については、「 IAM ユーザーガイド」の「管理ポリシーとインラインポリシーの選択」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があり

ます。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS サービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーIAMでは、 の AWS 管理ポリシーを使用できません。

アクセスコントロールリスト (ACLs)

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

Amazon S3、 AWS WAF、および Amazon VPCは、 をサポートするサービスの例ですACLs。の詳細についてはACLs、Amazon Simple Storage Service デベロッパーガイドの「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 – アクセス許可の境界は、アイデンティティベースのポリシーがIAMエンティティ (IAMユーザーまたはロール) に付与できるアクセス許可の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「 IAMユーザーガイド」の「 IAMエンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) に対する最大アクセス許可を指定するJSONポリシーです AWS Organizations。 AWS Organizations は、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCPs) をアカウントの一部またはすべてに適用できます。は、各 を含むメンバーアカウントのエンティティのアクセス許可SCPを制限します AWS アカウントのルートユーザー。Organizations と の詳細についてはSCPs、「 AWS Organizations ユーザーガイド」のSCPs「仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果として

セッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「 ユーザーガイド」の「セッションポリシーIAM」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関係する場合にリクエストを許可するかどうか AWS を決定する方法については、「 ユーザーガイド」の「ポリシー評価ロジックIAM」を参照してください。

と の AWS AppFabric 連携方法 IAM

IAM を使用して へのアクセスを管理する前に AppFabric、 で使用できるIAM機能を確認してください AppFabric。

IAM で使用できる の機能 AWS AppFabric

IAM 機能	AppFabric サポート
アイデンティティベースのポリシー	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	Yes
ポリシー条件キー	なし
ACLs	なし
ABAC (ポリシー内のタグ)	あり
一時的な認証情報	いいえ
プリンシパル権限	あり

IAM 機能	AppFabric サポート
サービスロール	いいえ
サービスリンクロール	あり

AppFabric およびその他の がほとんどの IAM 機能と AWS サービス どのように連携するかの概要を把握するには、IAM「 ユーザーガイド」のAWS 「 と連携する のサービスIAM」を参照してください。

のアイデンティティベースのポリシー AppFabric

アイデンティティベースのポリシーのサポート: あり

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなどの ID にアタッチできるJSONアクセス許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否されたアクションとリソース、およびアクションが許可または拒否される条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「 ユーザーガイド」の「 IAMJSONポリシー要素のリファレンスIAM」を参照してください。

のアイデンティティベースのポリシーの例 AppFabric

AppFabric アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS AppFabric のアイデンティティベースのポリシーの例。

内のリソースベースのポリシー AppFabric

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースにアタッチするJSONポリシードキュメントです。リソースベースのポリシーの例としては、IAMロールの信頼ポリシー や Amazon S3 バケットポリシー などがあります。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスをコントロールできます。ポリシーがアタッチされているリ

ソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS サービス。

クロスアカウントアクセスを有効にするには、リソースベースのポリシーのプリンシパルとして、アカウント全体または別のアカウントのIAMエンティティを指定できます。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントのIAM管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「 ユーザーガイド」の「 でのクロスアカウントリソースアクセスIAMIAM」を参照してください。

のポリシーアクション AppFabric

ポリシーアクションのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

JSON ポリシーの `Action`要素は、ポリシーでアクセスを許可または拒否するために使用できるアクションを記述します。ポリシーアクションの名前は通常、関連する AWS APIオペレーションと同じです。一致するAPIオペレーションを持たないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

AppFabric アクションのリストを確認するには、「サービス認証リファレンス」の「 で定義されるアクション AWS AppFabric」を参照してください。

のポリシーアクションは、アクションの前に次のプレフィックス AppFabric を使用します。

```
appfabric
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "appfabric:action1",
      "appfabric:action2"
         ]
```

ワイルドカード文字 (*) を使用すると、複数のアクションを指定することができます。例えば、List という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

```
"Action": "appfabric:List*"
```

AppFabric アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS AppFabric のアイデンティティベースのポリシーの例。

のポリシーリソース AppFabric

ポリシーリソースのサポート: あり

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

Policy ResourceJSON要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

AppFabric リソースタイプとその のリストを確認するにはARNs、「サービス認証リファレンス」の「 で定義されるリソースタイプ AWS AppFabric」を参照してください。各リソースARNの を指定できるアクションについては、「 で定義されるアクション AWS AppFabric」を参照してください。

AppFabric アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS AppFabric のアイデンティティベースのポリシーの例。

のポリシー条件キー AppFabric

サービス固有のポリシー条件キーをサポート： いいえ

管理者はポリシーを使用して AWS JSON、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

`Condition` 要素 (または `Condition` ブロック) を使用すると、ステートメントが有効な条件を指定できます。`Condition` 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の `Condition` 要素を指定する場合、または 1 つの `Condition` 要素に複数のキーを指定する場合、 AWS では `AND` 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理`OR`オペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば、IAMユーザー名でタグ付けされている場合にのみ、リソースにアクセスするアクセス許可をIAMユーザーに付与できます。詳細については、「 ユーザーガイド」のIAM「ポリシー要素: 変数とタグIAM」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「 ユーザーガイド」のAWS 「 グローバル条件コンテキストキーIAM」を参照してください。

AppFabric 条件キーのリストを確認するには、「サービス認証リファレンス」の「 の条件キー AWS AppFabric」を参照してください。条件キーを使用できるアクションとリソースについては、「 で定義されるアクション AWS AppFabric」を参照してください。

AppFabric アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS AppFabric のアイデンティティベースのポリシーの例。

ACLs の AppFabric

をサポートACLs： いいえ

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs はリソースベースのポリシーに似ていますが、JSONポリシードキュメント形式を使用しません。

ABAC で AppFabric

サポート ABAC (ポリシー内のタグ): はい

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。では AWS、これらの属性はタグ と呼ばれます。タグは、IAMエンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、の最初のステップですABAC。次に、プリンシパルのタグがアクセスしようとしているリソースのタグと一致する場合に、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、ポリシー管理が煩雑になる状況に役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

の詳細についてはABAC、「 ユーザーガイド」の「 とはABACIAM」を参照してください。のセットアップ手順を含むチュートリアルを表示するにはABAC、「 ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用するIAM」を参照してください。

での一時的な認証情報の使用 AppFabric

一時的な認証情報をサポート： いいえ

一部の は、一時的な認証情報を使用してサインインすると機能 AWS サービス しません。一時的な認証情報 AWS サービス を使用する などの詳細については、「 ユーザーガイドAWS サービス 」の「 と連携IAMする IAM 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えの詳細については、「 IAMユーザーガイド」の「ロールへの切り替え (コンソール) 」を参照してください。

一時的な認証情報は、 AWS CLI または を使用して手動で作成できます AWS API。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、長期的なア

クセスキーを使用する代わりに、一時的な認証情報を動的に生成することを推奨しています。詳細については、「」の「一時的なセキュリティ認証情報IAM」を参照してください。

のクロスサービスプリンシパル許可 AppFabric

転送アクセスセッションをサポート (FAS): はい

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS サービス、ダウンストリームサービス AWS サービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS サービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するための権限が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AppFabric のサービスロール

サービスロールをサポート： いいえ

サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける IAM ロールです。IAM 管理者は、 内からサービスロールを作成、変更、削除できますIAM。詳細については、「 ユーザーガイド」の「 にアクセス許可を委任するロールの作成 AWS サービスIAM」を参照してください。

> **Warning**
> サービスロールのアクセス許可を変更すると、 AppFabric 機能が破損する可能性があります。が指示する場合以外 AppFabric は、サービスロールを編集しないでください。

のサービスにリンクされたロール AppFabric

サービスリンクロールのサポート: あり

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS サービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

AppFabric サービスにリンクされたロールの作成または管理の詳細については、「」を参照してください AppFabric のサービスにリンクされたロールの使用。

AWS AppFabric のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールにはリソースを作成または変更 AppFabricするアクセス許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または を使用してタスクを実行することはできません AWS API。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSONポリシーを作成する方法については、「 ユーザーガイド」のIAM「ポリシーの作成IAM」を参照してください。

各リソースタイプの の形式など AppFabric、 で定義されるアクションとリソースタイプの詳細については、「サービス認証リファレンスARNs」の「 のアクション、リソース、および条件キー AWS AppFabric」を参照してください。

目次

- ポリシーのベストプラクティス
- AppFabric コンソールを使用する
- AppFabric セキュリティIAMポリシーの例
  - アプリケーションバンドルへのアクセスを許可する
  - コンテンツに対するアクセス制限
  - 取り込みの削除または停止を制限する
- AppFabric for productivity IAMポリシーの例
  - productivity の機能への読み取り専用アクセスを許可する
  - productivity の機能への完全なアクセスを許可する
  - 作成するためのアクセスを許可する AppClients
  - の詳細を取得するためのアクセスを許可する AppClients
  - リストへのアクセスを許可する AppClients
  - 更新へのアクセスを許可する AppClients
  - 削除するためのアクセスを許可する AppClients
  - アプリケーションを承認するためのアクセスを許可する
- その他のIAMポリシーの例

- 自分の権限の表示をユーザーに許可する

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが AppFabric リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「 ユーザーガイド」の「 AWS 管理ポリシー」または「 ジョブ機能の 管理ポリシーIAM」を参照してください。 AWS
- 最小特権のアクセス許可を適用する – IAMポリシーでアクセス許可を設定する場合は、タスクの実行に必要なアクセス許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用してアクセス許可を適用する方法の詳細については、「 ユーザーガイド」の「 のポリシーとアクセス許可IAMIAM」を参照してください。
- IAM ポリシーの条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションとリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを を使用して送信する必要があることを指定できますSSL。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS サービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「 ユーザーガイド」のIAMJSON「ポリシー要素: 条件IAM」を参照してください。
- IAM Access Analyzer を使用してIAMポリシーを検証し、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されています。詳細については、「 ユーザーガイド」のIAM「Access Analyzer ポリシーの検証IAM」を参照してください。
- 多要素認証を要求する (MFA) – でIAMユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化MFAするために をオンにします。API オペレーションが呼び出されるMFAタイミングを要求するには、ポリシーにMFA条件を追加します。詳細

については、「 IAMユーザーガイド」のMFA「 で保護されたAPIアクセスの設定」を参照してください。

のベストプラクティスの詳細についてはIAM、「 ユーザーガイド」の「 のセキュリティのベストプラクティスIAMIAM」を参照してください。

AppFabric コンソールを使用する

`AWSAppFabricReadOnlyAccess` AWS マネージドポリシーを ID にアタッチして、 IAM のコンソールを含む AppFabric AppFabric サービスへの読み取り専用アクセス許可を付与します AWS Management Console。または、ID IAM に `AWSAppFabricFullAccess` AWS 管理ポリシーをアタッチして、 AppFabric サービスへの完全な管理アクセス許可を付与することもできます。詳細については、「AWS の マネージドポリシー AWS AppFabric」を参照してください。

AppFabric セキュリティIAMポリシーの例

セキュリティ AppFabric 機能の には、次のポリシー例が適用されます。

アプリケーションバンドルへのアクセスを許可する

次のポリシー例では、 サービス内の AppFabricアプリケーションバンドルへのアクセスを許可します。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

コンテンツに対するアクセス制限

次のポリシー例では、 サービス内のアプリケーションバンドルへのアクセスを制限します AppFabric。

```
{
    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

取り込みの削除または停止を制限する

次のポリシー例では、 AppFabric サービス内の取り込みの削除または停止を制限します。

```
{
    "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 for productivity IAMポリシーの例

AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

次のポリシー例は、 for productivity AppFabric の機能に適用されます。

productivity の機能への読み取り専用アクセスを許可する

次のポリシー例では、 AppFabric for productivity 機能への読み取り専用アクセスを許可します。

> **Important**
> このポリシーをIAMコンソールのポリシーJSON工ディタに追加すると、無効なアクションエラーが表示されることがあります。これは、 AppFabric for productivity 機能が現在プレビューされているためです。このエラーは無視し、ポリシーの作成を続けていただいて構いません。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
                "appfabric:ListActionableInsights",
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights"
            ],
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

productivity の機能への完全なアクセスを許可する

次のポリシー例では、 AppFabric for productivity 機能へのフルアクセスを許可します。

> **Important**
>
> このポリシーをIAMコンソールのポリシーJSONエディタに追加すると、無効なアクションエラーが表示されることがあります。これは、 AppFabric for productivity 機能が現在プレビューされているためです。このエラーは無視し、ポリシーの作成を続けていただいて構いません。

```
{
    "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"
}
```

作成するためのアクセスを許可する AppClients

次のポリシー例では、 を作成するためのアクセスを許可します AppClients。詳細については、「Create an for productivity AppFabric AppClient」を参照してください。

> **Important**
>
> このポリシーをIAMコンソールのポリシーJSONエディタに追加すると、無効なアクションエラーが表示されることがあります。これは、 AppFabric for productivity 機能が現在プレビューされているためです。このエラーは無視し、ポリシーの作成を続けていただいて構いません。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

の詳細を取得するためのアクセスを許可する AppClients

次のポリシー例では、 の詳細を取得するためのアクセスを許可します AppClients。詳細については、「 の詳細を取得する AppClient」を参照してください。

> **Important**
>
> このポリシーをIAMコンソールのポリシーJSONエディタに追加すると、無効なアクションエラーが表示されることがあります。これは、 AppFabric for productivity 機能が現在プレビューされているためです。このエラーは無視し、ポリシーの作成を続けていただいて構いません。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

リストへのアクセスを許可する AppClients

次のポリシー例では、 を一覧表示するためのアクセスを許可します AppClients。詳細については、「 の詳細を取得する AppClient」を参照してください。

> **Important**
> このポリシーをIAMコンソールのポリシーJSONエディタに追加すると、無効なアクションエラーが表示されることがあります。これは、 AppFabric for productivity 機能が現在プレビューされているためです。このエラーは無視し、ポリシーの作成を続けていただいて構いません。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:ListAppClients"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

更新へのアクセスを許可する AppClients

次のポリシー例では、 を更新するためのアクセスを許可します AppClients。詳細については、「 の更新 AppClient」を参照してください。

> **Important**
> このポリシーをIAMコンソールのポリシーJSONエディタに追加すると、無効なアクションエラーが表示されることがあります。これは、 AppFabric for productivity 機能が現在プレビューされているためです。このエラーは無視し、ポリシーの作成を続けていただいて構いません。

```
{
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:UpdateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

削除するためのアクセスを許可する AppClients

次のポリシー例では、 を削除するためのアクセスを許可します AppClients。詳細については、「 の更新 AppClient」を参照してください。

> **Important**
>
> このポリシーをIAMコンソールのポリシーJSONエディタに追加すると、無効なアクションエラーが表示されることがあります。これは、 AppFabric for productivity 機能が現在プレビューされているためです。このエラーは無視し、ポリシーの作成を続けていただいて構いません。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:DeleteAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

アプリケーションを承認するためのアクセスを許可する

次のポリシー例では、トークン を使用してアプリケーションを認証するためのアクセスを許可しますAPI。詳細については、「アプリケーションを認証し承認する」を参照してください。

> **Important**
> このポリシーをIAMコンソールのポリシーJSONエディタに追加すると、無効なアクションエラーが表示されることがあります。これは、 AppFabric for productivity 機能が現在プレビューされているためです。このエラーは無視し、ポリシーの作成を続けていただいて構いません。

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:Token"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

その他のIAMポリシーの例

自分の権限の表示をユーザーに許可する

この例では、IAMユーザーがユーザー ID にアタッチされているインラインポリシーと管理ポリシーを表示できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または を使用してプログラムでこのアクションを実行するアクセス許可が含まれています 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": "*"
        }
    ]
}
```

AppFabric のサービスにリンクされたロールの使用

AWS AppFabric は AWS Identity and Access Management（IAM) サービスにリンクされたロール を使用します。サービスにリンクされたロールは、 に直接リンクされた一意のタイプのIAMロールです AppFabric。サービスにリンクされたロールは によって事前定義 AppFabric されており、 AWS サービス ユーザーに代わってサービスから他の を呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、 の設定 AppFabric が簡単になります。 は、サービスにリンクされたロールのアクセス許可 AppFabric を定義し、特に定義されている場合を除き、 のみがそのロールを引き受け AppFabric る

ことができます。定義されたアクセス許可には、信頼ポリシーとアクセス許可ポリシーが含まれ、そのアクセス許可ポリシーを他のIAMエンティティにアタッチすることはできません。

サービスリンクロールは、まずその関連リソースを削除しなければ削除できません。これにより、AppFabric リソースにアクセスするためのアクセス許可を誤って削除することがないため、リソースが保護されます。

サービスにリンクされたロールをサポートする他のサービスの詳細については、「 AWS と連携するのサービスIAM」を参照し、「サービスにリンクされたロール」列で「はい」があるサービスを探します。 そのサービスに関するサービスにリンクされたロールのドキュメントを表示するには、リンクが設定されている Yes] (はい) を選択します。

AppFabric のサービスリンクロールのアクセス許可

AppFabric は、 という名前のサービスにリンクされたロールを使用しますAWSServiceRoleForAppFabric。 AppFabric は、Amazon S3 バケットや Amazon Data Firehose 配信ストリームなどの取り込み先リソースにデータを配置できます。また、 AppFabric は AWS/AppFabric名前空間に CloudWatch メトリクスデータを配置することもできます。

AWSServiceRoleForAppFabric サービスにリンクされたロールは、ロールの引き受けについて以下のサービスを信頼します。

- appfabric.amazonaws.com

という名前のロールアクセス許可ポリシーAWSAppFabricServiceRolePolicyは AppFabric 、 が指定されたリソースに対して次のアクションを実行できるようにします。

- アクション:AWS/AppFabricネームスペース内でcloudwatch:PutMetricData。このアクションは AppFabric 、メトリクスデータを Amazon CloudWatch AWS/AppFabric名前空間に配置するアクセス許可を に付与します。で使用できる AppFabric メトリクスの詳細については、CloudWatch「」を参照してくださいAmazon AWS AppFabric によるモニタリング CloudWatch。
- アクション: Amazon S3 バケットでの s3:PutObject。このアクションは AppFabric 、 が、指定した Amazon S3 バケットに取り込まれたデータを配置するためのアクセス許可を付与します。
- アクション: Amazon Data Firehose 配信ストリームfirehose:PutRecordBatch内。このアクションは AppFabric 、 が、指定した Amazon Data Firehose 配信ストリームに取り込まれたデータを配置するためのアクセス許可を付与します。

詳細については、「 の AWS マネージドポリシー AppFabric」を参照してください。

ユーザー、グループ、ロールなどがサービスにリンクされたロールを作成、編集、削除できるようにするには、アクセス権限を設定する必要があります。詳細については、「 ユーザーガイド」の「サービスにリンクされたロールのアクセス許可IAM」を参照してください。

のサービスにリンクされたロールの作成 AppFabric

サービスリンクロールを手動で作成する必要はありません。、 AWS Management Console、 AWS CLIまたは で AppFabric アプリケーションバンドルを作成すると AWS API、 によってサービスにリンクされたロール AppFabric が自動的に作成されます。

のサービスにリンクされたロールの編集 AppFabric

AppFabric では、`AWSServiceRoleForAppFabric`サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、 を使用してロールの説明を編集することはできますIAM。詳細については、「 IAMユーザーガイド」の「サービスにリンクされたロールの編集」を参照してください。

のサービスにリンクされたロールの削除 AppFabric

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、モニタリングや保守が積極的に行われていない未使用のエンティティを排除できます。ただし、サービスにリンクされたロールを削除する前に、すべての AppFabric アプリケーションバンドルを削除する必要があります。

サービスリンクロールのクリーンアップ

IAM を使用してサービスにリンクされたロールを削除する前に、まずそのロールで使用されているリソースをすべて削除する必要があります。で作成したアプリケーションバンドル AppFabric は、ロールによって使用されます。詳細については、「セキュリティリソース AWS AppFabric の削除」を参照してください。

> **Note**
>
> リソースを削除しようとしたときに AppFabric サービスがロールを使用している場合、削除が失敗する可能性があります。失敗した場合は、数分待ってから操作を再試行してください。

サービスにリンクされたロールを手動で削除する

IAM コンソール、、または AWS API を使用して AWS CLI、`AWSServiceRoleForAppFabric`サービスにリンクされたロールを削除します。詳細については、「 ユーザーガイド」の「サービスにリンクされたロールの削除IAM」を参照してください。

AppFabric サービスにリンクされたロールでサポートされているリージョン

AppFabric は、サービス AWS リージョン が利用可能なすべての でサービスにリンクされたロールの使用をサポートします。詳細については、「」のAppFabric 「 エンドポイントとクォータ」を参照してくださいAWS 全般のリファレンス。

AWS の マネージドポリシー AWS AppFabric

ユーザー、グループ、ロールにアクセス許可を追加するには、自分でポリシーを記述するよりも、AWS 管理ポリシーを使用する方が簡単です。必要なアクセス許可のみをチームに提供するIAMカスタマー管理ポリシーを作成するには、時間と専門知識が必要です。すぐに開始するには、 AWS マネージドポリシーを使用できます。これらのポリシーは、一般的なユースケースをターゲット範囲に含めており、 AWS アカウントで利用できます。 AWS 管理ポリシーの詳細については、「 ユーザーガイド」の「 AWS 管理ポリシーIAM」を参照してください。

AWS サービス AWS 管理ポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可は変更できません。サービスでは、新しい機能を利用できるようにするために、 AWS マネージドポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS マネージドポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が破損することはありません。

さらに、 は、複数の サービスにまたがる職務機能の マネージドポリシー AWS をサポートします。例えば、 ReadOnlyAccess AWS 管理ポリシーは、すべての AWS サービス および リソースへの読み取り専用アクセスを提供します。サービスが新機能を起動すると、 は新しいオペレーションとリソースの読み取り専用アクセス許可 AWS を追加します。職務機能ポリシーのリストと説明については、「 ユーザーガイドAWS 」の「職務機能用の 管理ポリシーIAM」を参照してください。

AWS 管理ポリシー: AWSAppFabricReadOnlyAccess

IAM ID に`AWSAppFabricReadOnlyAccess`ポリシーをアタッチできます。このポリシーは、AppFabric サービスに読み取り専用アクセス許可を付与します。

> **Note**
>
> このAWSAppFabricReadOnlyAccessポリシーは、生産性向上機能 AppFabric のための への読み取り専用アクセスを許可しません。

許可の詳細

このポリシーには、以下の許可が含まれています。

- appfabric— アプリバンドルの取得、アプリバンドルの一覧表示、アプリ承認の取得、アプリ承認のリスト、取り込みの取得、取り込みの一覧表示、取り込み先の取得、取り込み先の取得、取り込み先のリスト、およびリソースタグの一覧表示を行う権限を付与します。

```
{
    "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 マネージドポリシー: AWSAppFabricFullAccess

IAM ID にAWSAppFabricFullAccessポリシーをアタッチできます。このポリシーは AppFabric 、サービスに管理アクセス許可を付与します。

> **Important**
>
> このAWSAppFabricFullAccessポリシーでは、 AppFabric for productivity 機能へのアクセスは許可されません。これは、現在プレビュー中のためです。for productivity 機能へのアクセスの許可の詳細については、 AppFabric 「」を参照してくださいAppFabric for productivity IAMポリシーの例。

許可の詳細

このポリシーには、以下の許可が含まれています。

- appfabric – に完全な管理アクセス許可を付与します AppFabric。
- kms— エイリアスを一覧表示するためのアクセス許可を付与します。
- s3すべての Amazon S3 バケットの権限を付与して、バケット位置を獲得します。
- firehose – Amazon Data Firehose 配信ストリームを一覧表示し、配信ストリームを記述するアクセス許可を付与します。
- iam – AWSServiceRoleForAppFabricのサービスにリンクされたロールを作成するアクセス許可を付与します AppFabric。詳細については、「 AppFabric のサービスにリンクされたロールの使用」を参照してください。

```
{
    "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 管理ポリシー: AWSAppFabricServiceRolePolicy

`AWSAppFabricServiceRolePolicy` ポリシーをIAMエンティティにアタッチすることはできません。このポリシーは、 がユーザーに代わってアクションを実行できるようにするサービスにリンクされたロール AppFabric にアタッチされます。詳細については、「 AppFabric のサービスにリンクされたロールの使用」を参照してください。

許可の詳細

このポリシーには、以下の許可が含まれています。

- `cloudwatch` – メトリクスデータを Amazon CloudWatch `AWS/AppFabric` 名前空間に配置するためのアクセス許可 AppFabric を付与します。で使用できる AppFabric メトリクスの詳細については、 CloudWatch「」を参照してくださいAmazon AWS AppFabric によるモニタリング CloudWatch。

- `s3` – 指定した Amazon S3 バケットに取り込まれたデータを配置するアクセス許可 AppFabric をに付与します。 Amazon S3
- `firehose` – 指定した Amazon Data Firehose 配信ストリームに取り込まれたデータを配置するアクセス許可 AppFabric を に付与します。

```
{
    "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 AWS 管理ポリシーの更新

このサービスがこれらの変更の追跡を開始した AppFabric 以降の の AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートを受け取るには、AppFabric ドキュメント履歴ページのRSSフィードにサブスクライブします。

変更	説明	日付
AWSAppFabricReadOnlyAccess - 新しいポリシー	AppFabric は、 サービスに読み取り専用アクセス許可を付与する新しいポリシーを追加しました AppFabric。	2023 年 6 月 27 日
AWSAppFabricFullAccess - 新しいポリシー	AppFabric は、 AppFabric サービスに管理権限を付与する新しいポリシーを追加しました。	2023 年 6 月 27 日
AWSAppFabricServiceRolePolicy - 新しいポリシー	AppFabric は、`AWSServiceRoleForAppFabric` サービスにリンクされたロールの新しいポリシーを追加しました。	2023 年 6 月 27 日
AppFabric が変更の追跡を開始しました	AppFabric が AWS マネージドポリシーの変更の追跡を開始しました。	2023 年 6 月 27 日

AWS AppFabric ID とアクセスのトラブルシューティング

次の情報は、 および の使用時に発生する可能性がある一般的な問題の診断 AppFabric と修正に役立ちますIAM。

トピック

- でアクションを実行する権限がない AppFabric
- iam:PassRole を実行する権限がない
- 自分の 以外のユーザーに自分の AppFabric リソース AWS アカウント へのアクセスを許可したい

でアクションを実行する権限がない AppFabric

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次の例のエラーは、mateojacksonIAMユーザーが コンソールを使用して架空の*my-example-widget*リソースの詳細を表示しようとしているが、架空のappfabric:*GetWidget*アクセス許可がない場合に発生します。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 appfabric:GetWidget on resource: my-example-widget
```

この場合、appfabric:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がない

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して にロールを渡すことができるようにする必要があります AppFabric。

一部の AWS サービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次の例のエラーは、 というIAMユーザーがコンソールを使用して marymajor でアクションを実行しようする場合に発生します AppFabric。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

自分の 以外のユーザーに自分の AppFabric リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACLs) をサポートするサービスでは、これらのポリシーを使用して、ユーザーにリソースへのアクセスを許可できます。

詳細については、以下を参照してください。

- がこれらの機能 AppFabric をサポートしているかどうかを確認するには、「」を参照してください[と の AWS AppFabric 連携方法 IAM](#)。
- 所有している のリソースへのアクセスを提供する方法については、 AWS アカウント 「 ユーザーガイド」の[「所有 AWS アカウント している別の のIAMユーザーへのアクセスを提供する](#)IAM」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、 IAM ユーザーガイドの[「サードパーティー AWS アカウント が所有する へのアクセス](#)を提供する」を参照してください。
- ID フェデレーションを通じてアクセスを提供する方法については、 IAMユーザーガイドの[「外部認証されたユーザーへのアクセスの提供 (ID フェデレーション)](#)」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、「 ユーザーガイド」の[「 でのクロスアカウントリソースアクセスIAM](#)IAM」を参照してください。

のコンプライアンス検証 AWS AppFabric

AWS サービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラム[AWS サービス による対象範囲内のコンプライアンスプログラム](#)を参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、[AWS 「コンプライアンスプログラム](#)」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、[「 でのレポートのダウンロード AWS Artifact](#)」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS サービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスHIPAAのセキュリティとコンプライアンスのためのアーキテクチャ – このホワイトペーパーでは、企業が AWS を使用して HIPAA対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべての AWS サービス がHIPAA対象となるわけではありません。詳細については、HIPAA「対象サービスリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS サービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST) 、Payment Card Industry Security Standards Council ()、PCI国際標準化機構 (ISO) など) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS サービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS サービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことでDSS、 PCI などのさまざまなコンプライアンス要件に対応するのに役立ちます。
- AWS Audit Manager – これにより AWS サービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

のセキュリティのベストプラクティス AWS AppFabric

AWS AppFabric には、独自のセキュリティポリシーを開発および実装する際に考慮すべきいくつかのセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを提供するものではありません。これらのベストプラクティスはお客様の環境に必ずしも適切または十分でない可能性があるため、処方箋ではなく、あくまで有用な検討事項とお考えください。

管理者アクセスなしでアプリケーションを監視する

読み取り専用 AWS Identity and Access Management（IAM) アクセス許可を使用すると、誰でも Amazon QuickSight および などの他のセキュリティ情報およびイベント管理 (SIEM) ツール AppFabric と統合できますSplunk。アプリケーションのセキュリティをモニタリングするために、データは Amazon Simple Storage Service (Amazon S3) バケットまたは Amazon Data Firehose 配信ストリームに配信されます。

AppFabric イベントのモニタリング

Amazon CloudWatch metrics AppFabric を使用してモニタリングできます。 CloudWatch は 1 分 AppFabric ごとにデータを収集し、メトリクスに処理します。メトリクスが指定したしきい値に一致したときに通知をオフにするアラームを設定できます。詳細については、「Amazon AWS AppFabric によるモニタリング CloudWatch」を参照してください。

の耐障害性 AWS AppFabric

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供し、低レイテンシー、高スループット、高冗長ネットワークで接続されます。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

のインフラストラクチャセキュリティ AWS AppFabric

マネージドサービスである AWS AppFabric は、ホワイトペーパー「Amazon Web Services: セキュリティプロセスの概要」に記載されている AWS グローバルネットワークセキュリティの手順で保護されています。

が AWS 公開したAPI呼び出しを使用して、ネットワーク AppFabric 経由で にアクセスします。クライアントは 1.0 TLS 以降をサポートしている必要があります。1.2 TLS 以降をお勧めします。また、クライアントは、 (Ephemeral Diffie-HellmanPFS) や DHE (Elliptic Curve Ephemeral Diffie-Hellman) などの完全前方秘匿性 ECDHE () を持つ暗号スイートもサポートする必要があります。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、 リクエストは、 IAMプリンシパルに関連付けられたアクセスキー ID とシークレットアクセスキーを使用して署名する必要があります。または、リクエストに署名するための一時的なセキュリティ認証情報を生成するには、AWS Security Token Service (AWS STS) を使用することもできます。

での設定と脆弱性の分析 AWS AppFabric

設定と IT コントロールは、 AWS とお客様の間の責任共有です。詳細については、 AWS 「 責任共有モデル」を参照してください。

モニタリング AWS AppFabric

モニタリングは、 AWS AppFabric およびその他の AWS ソリューションの信頼性、可用性、およびパフォーマンスを維持する上で重要な部分です。 は、 をモニタリングし AppFabric、問題が発生したときに報告し、必要に応じて自動アクションを実行するために、以下のモニタリングツール AWS を提供します。

- Amazon CloudWatch は、 AWS リソースと で実行しているアプリケーションを AWS リアルタイムでモニタリングします。メトリクスを収集および追跡し、カスタマイズされたダッシュボードを作成し、指定されたメトリックが指定したしきい値に達したときに通知またはアクションを実行するアラームを設定できます。例えば、 で Amazon EC2 インスタンスの CPU 使用率やその他のメトリクス CloudWatch を追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。
- Amazon CloudWatch Logs を使用すると、Amazon EC2 インスタンスやその他のソースからログファイルをモニタリング、保存 AWS CloudTrail、およびアクセスできます。 CloudWatch Logs はログファイル内の情報をモニタリングし、特定のしきい値に達したときに通知できます。高い耐久性を備えたストレージにログデータをアーカイブすることもできます。詳細については、「Amazon CloudWatch Logs ユーザーガイド」を参照してください。
- AWS CloudTrail は、 によって、または に代わって行われた API コールおよび関連イベントをキャプチャ AWS アカウント し、指定した Amazon S3 バケットにログファイルを配信します。を呼び出したユーザーとアカウント AWS、呼び出し元のソース IP アドレス、呼び出しが発生した日時を特定できます。詳細については、『AWS CloudTrail ユーザーガイド』を参照してください。

Amazon AWS AppFabric によるモニタリング CloudWatch

raw データを収集し CloudWatch、読み取り可能なほぼリアルタイムのメトリクスに処理する AWS AppFabric を使用してモニタリングできます。これらの統計は 15 か月間保持されるため、履歴情報にアクセスし、ウェブアプリケーションまたはサービスの動作をより的確に把握できます。また、特定のしきい値を監視するアラームを設定し、これらのしきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、「Amazon ユーザーガイド CloudWatch 」を参照してください。

AppFabric サービスは、 `AWS/AppFabric`名前空間で次のメトリクスを報告します。

メトリクス	説明
AppFabric アプリ認証ステータス	アプリ認証のステータス (1接続されている場合は 、その他の0場合は)。
AppFabric データ配信のレイテンシー	が SaaS アプリケーションから監査ログ AppFabric を収集し、設定された送信先 (Amazon S3 または Amazon Data Firehose) に配信するのにかかった時間 (秒単位) 。
取り込み先のステータス	取り込み先のステータス (アクティブな場合は 1、その他の場合は 0)。
全体的なデータ遅延	SaaS アプリケーションでイベントが発生したときと、対応する監査ログが によって設定された送信先 (Amazon S3 または Amazon Data Firehose) に配信されたときの時間差 (秒単位) AppFabric。
取り込まれるデータ量	Amazon Simple Storage Service (Amazon S3) または Amazon Data Firehose に配信されるデータのサイズ。

AppFabric メトリクスでは、次のディメンションがサポートされています。

ディメンション	説明
取り込み先Arn	取り込み先の Amazon リソースネーム (ARN)。

を使用した AWS AppFabric API コールのログ記録 AWS CloudTrail

AWS AppFabric は と統合されています。これは AWS CloudTrail、ユーザー、ロール、または AWS サービス の によって実行されたアクションを記録するサービスです AppFabric。 は、 のすべての API コールをイベント AppFabric として CloudTrail キャプチャします。キャプチャされた呼び出しには、 AppFabric コンソールからの呼び出しと AppFabric API オペレーションへのコード呼び

出しが含まれます。証跡を作成する場合は、 の CloudTrailイベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます AppFabric。証跡を設定しない場合でも、CloudTrail コンソールのイベント履歴 で最新のイベントを表示できます。によって収集された情報を使用して CloudTrail、 に対して行われたリクエスト AppFabric、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

の詳細については CloudTrail、「 AWS CloudTrail ユーザーガイド」を参照してください。

AppFabric の情報 CloudTrail

CloudTrail アカウントを作成する AWS アカウント と、 で が有効になります。でアクティビティが発生すると AppFabric、そのアクティビティは CloudTrail イベント履歴 の他の AWS サービス イベントとともにイベントに記録されます。最近のイベントは、 AWS アカウントで表示、検索、ダウンロードできます。詳細については、「 AWS CloudTrail ユーザーガイド」の「イベント履歴を含む CloudTrail イベントの表示」を参照してください。

のイベントなど AWS アカウント、 のイベントの継続的な記録については AppFabric、証跡を作成します。証跡により CloudTrail 、 はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、 AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、他の を設定 AWS サービス して、CloudTrail ログで収集されたイベントデータをより詳細に分析し、それに基づく対応を行うことができます。詳細については、『AWS CloudTrail ユーザーガイド:』の以下のトピックを参照してください。

- 証跡作成の概要
- CloudTrail がサポートするサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

すべての AppFabric アクションは によってログに記録 CloudTrail され、 AWS AppFabric API リファレンス に記載されています。例えば、`CreateAppBundle`、、および `GetAppBundle`アクションを呼び出すと`UpdateAppBundle`、 CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます:

- リクエストが root または AWS Identity and Access Management (IAM) ユーザーの認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS サービスによって送信されたかどうか。

詳細については、「 ユーザーガイド」の「 CloudTrail userIdentity要素AWS CloudTrail 」を参照してください。

AppFabric ログファイルエントリについて

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントは任意のソースからの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルはパブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 `CreateAppBundle`アクションを示す CloudTrail ログエントリを示しています。

```
{
    "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"
    }
}
```

のクォータ AWS AppFabric

AWS アカウント には、 ごとに、以前は制限と呼ばれていたデフォルトのクォータがあります AWS サービス。特に明記されていない限り、クォータは地域固有です。一部のクォータについては引き上げをリクエストできますが、その他のクォータについては引き上げることはできません。

のクォータを表示するには AppFabric、Service Quotas コンソール を開きます。ナビゲーションペインで、AWS サービスを選択し、 を選択しますAppFabric。

クォータの引き上げをリクエストするには、「Service Quotas ユーザーガイド」の「Requesting a quota increase」(クォータ引き上げリクエスト) を参照してください。Service Quotas でクォータがまだ利用できない場合は、[上限引き上げ] フォームを使用してください。

AppFabric の に関連するクォータを次の表 AWS アカウント に示します。

名前	デフォルト	引き上げ可能	説明
アプリケーションバンドル	サポートされている各リージョン: 1	[いいえ]	現在の AWS リージョンのアカウントで作成できるアプリケーションバンドルの最大数。
アプリケーション権限	サポートされている各リージョン: 50	いいえ	現在の AWS リージョンのアカウントで作成できるアプリケーション認証の最大数。
取り込み	サポートされている各リージョン: 50	いいえ	現在の AWS リージョンのアカウントで作成できる取り込みの最大数。

名前	デフォルト	引き上げ可能	説明
取り込み先	サポートされている各リージョン：5	いいえ	現在の AWS リージョンのアカウントで取り込みごとに作成できる取り込み先の最大数。
AppClient	サポートされている各リージョン: 1	[いいえ]	現在の AWS リージョンのアカウントで作成 AppClients できる の最大数。 AWS AppFabric for productivity 機能はプレビュー版であり、変更される可能性があります。

AppFabric 管理ガイドのドキュメント履歴

次の表に、 のドキュメントリリースを示します AWS AppFabric。

変更	説明	日付
新たにサポートされるアプリケーション	サポートされているアプリケーションJumpCloudとしてを追加しました。詳細については、「 でサポートされているアプリケーション AWS AppFabric」を参照してください。	2024 年 6 月 5 日
新たにサポートされるアプリケーションとセキュリティツール	サポートされているアプリケーションGoogle Analyticsとして Azure Monitorおよびを追加しました。詳細については、「 でサポートされているアプリケーション AWS AppFabric」を参照してください。サポートされているセキュリティツールSingularity Cloudとして を追加しました。詳細については、「互換性のあるセキュリティツール」を参照してください。	2024 年 4 月 30 日
新たにサポートされるアプリケーション	サポートされているアプリケーションSentinelOneとして を追加しました。詳細については、「 でサポートされているアプリケーション AWS AppFabric」を参照してください。	2024 年 4 月 25 日

新たにサポートされるアプリケーション	サポートされているアプリケーション1Passwordとして を追加しました。詳細については、「 でサポートされているアプリケーション AWS AppFabric」を参照してください。	2024 年 4 月 23 日
新たにサポートされるセキュリティツール	互換性のあるセキュリティツールDynatraceとして を追加しました。詳細については、「互換性のあるセキュリティツール」を参照してください。	2024 年 3 月 26 日
新しいメトリクス	AppFabric App Authorization Status メトリクスを追加しました。詳細については、「Amazon CloudWatch Logs AWS AppFabric によるモニタリング」を参照してください。	2024 年 3 月 8 日
新たにサポートされるアプリケーション	サポートされているアプリケーションIBM Security® Verifyとして を追加しました。詳細については、「 でサポートされているアプリケーション AWS AppFabric」を参照してください。	2024 年 3 月 6 日
新たにサポートされるアプリケーション	サポートされているアプリケーションBoxとして を追加しました。詳細については、「 でサポートされているアプリケーション AWS AppFabric」を参照してください。	2024 年 2 月 28 日

新たにサポートされるアプリケーションとメトリクス	サポートされているアプリケーションTerraform CloudとしてCisco Duo、Sales force、、 を追加しました。詳細については、「 でサポートされているアプリケーション AWS AppFabric」を参照してください。 AppFabric データ配信レイテンシーと全体的なデータ遅延メトリクスを追加しました。詳細については、「Amazon CloudWatch Logs によるモニタリング AWS AppFabric」を参照してください。	2024 年 2 月 1 日
サポート対象のアプリケーションとして、Atlassian Confluence、Genesys Cloud、HubSpot、OneLogin by One Identity、PagerDuty、Ping Identity を、互換性のあるセキュリティツールとして Barracuda XDR を追加しました。	サポートされている新しいアプリケーションの詳細については、「 でサポートされているアプリケーション AWS AppFabric」および「互換性のあるセキュリティツール」を参照してください。	2023 年 12 月 15 日
サポート対象のアプリケーションとして、Atlassian Confluence、Genesys Cloud、HubSpot、OneLogin by One Identity、PagerDuty、Ping Identity を、互換性のあるセキュリティツールとして Barracuda XDR を追加しました。	サポートされている新しいアプリケーションの詳細については、「 でサポートされているアプリケーション AWS AppFabric」および「互換性のあるセキュリティツール」を参照してください。	2023 年 12 月 15 日

AWS AppFabric for productivity のプレビュードキュメントを追加しました	for productivity の詳細については、 AppFabric「What is for productivity? AWS AppFabric 」を参照してください。	2023 年 11 月 27 日
サポートされているアプリケーションとして GitHub および ServiceNow を追加しました。	新たにサポートされるアプリケーションの詳細については、「サポートされているアプリケーション」を参照してください。	2023 年 10 月 31 日
の管理 AWS ポリシーの追跡を開始しました AWS AppFabric	の AWS 管理ポリシーの詳細については AppFabric、「 の AWS 管理ポリシー AWS AppFabric」を参照してください。	2023 年 6 月 27 日
初回リリース	AWS AppFabric 管理ガイドの初回リリース。	2023 年 6 月 27 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。