Guide d’administration

AWS AppFabric

AWS AppFabric: Guide d’administration

Table of Contents

Qu'est-ce que c'est AWS AppFabric ?

AWS AppFabric connecte rapidement les applications SaaS (software as a service) au sein de votre organisation, afin que les équipes informatiques et de sécurité puissent facilement gérer et sécuriser les applications à l'aide d'un schéma standard, et que les employés puissent effectuer les tâches quotidiennes plus rapidement grâce à l'IA générative.

Rubriques

Produits

Explorez les deux aspects AWS AppFabric suivants : AppFabric pour la sécurité, conçu pour rationaliser la gestion et la sécurité, et AppFabric pour la productivité (version préliminaire), améliorée grâce à des fonctionnalités d'intelligence artificielle générative. Pour plus d’informations, consultez les rubriques suivantes :

- Qu'est-ce que c'est AWS AppFabric pour la sécurité ?
- Qu'est-ce que c'est AWS AppFabric pour la productivité ?

Avantages

Vous pouvez utiliser AppFabric pour effectuer les opérations suivantes :

- Connectez vos applications en quelques minutes et réduisez les coûts d'exploitation.
- Améliorez la visibilité des données des applications SaaS pour améliorer votre niveau de sécurité.
- Facilitez automatiquement les tâches entre les applications grâce à l'IA générative.

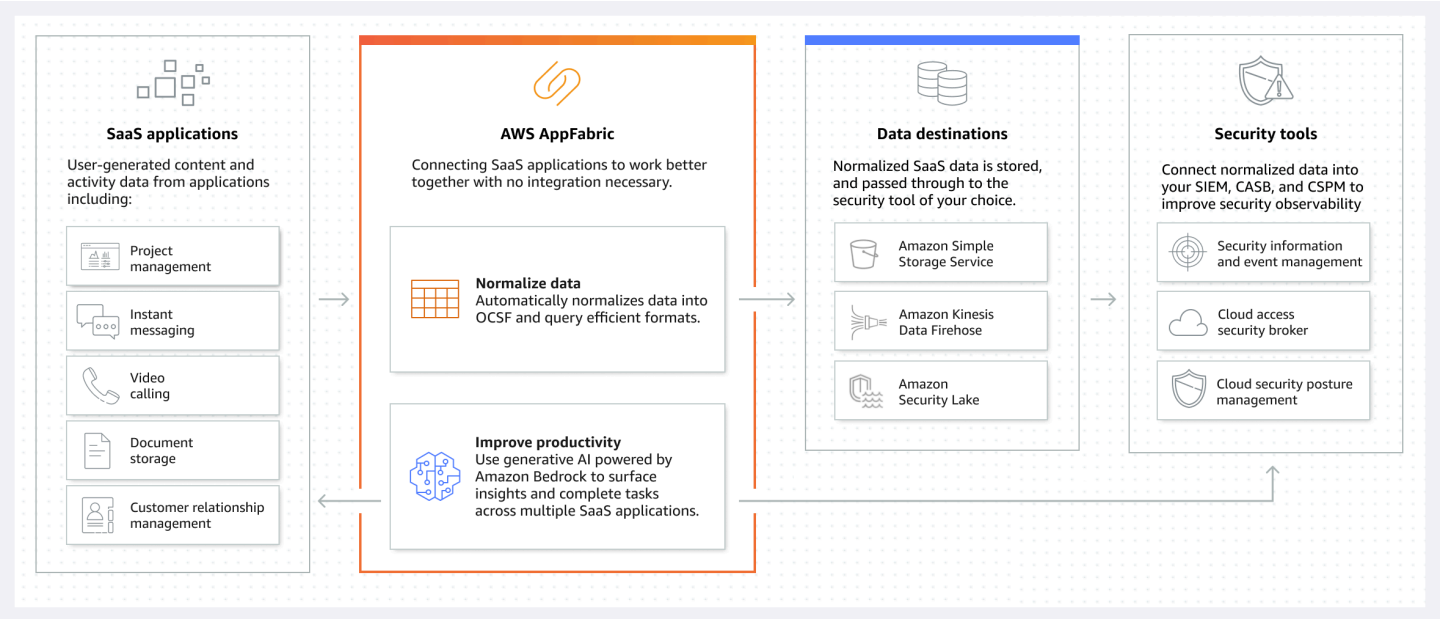
Cas d'utilisation

Vous pouvez utiliser AppFabric pour :

- Connectez rapidement vos applications SaaS
  - AppFabric for security connecte nativement les meilleures applications de productivité et de sécurité SaaS entre elles, fournissant ainsi une solution d'interopérabilité SaaS entièrement gérée.
- Améliorez votre posture de sécurité
  - Les données des applications sont automatiquement normalisées, ce qui permet aux administrateurs de définir des politiques communes, de standardiser les alertes de sécurité et de gérer facilement l'accès des utilisateurs à plusieurs applications.
- Réimaginez la productivité
  - Grâce à un assistant d'intelligence artificielle génératif commun, AppFabric for productivity permet aux employés d'obtenir des réponses rapidement, d'automatiser la gestion des tâches et de générer des informations sur leurs applications de productivité SaaS.

Comment AppFabric fonctionne

AppFabric connecte rapidement plusieurs applications SaaS sans aucun codage requis pour une productivité et une sécurité accrues. Le schéma suivant montre les avantages de AppFabric.



> **Note**
>
> AppFabric for productivity est actuellement lancé en version préliminaire et disponible dans l'est des États-Unis (Virginie du Nord) Région AWS. Pour plus d'informations sur Régions AWS, consultez la section AWS AppFabric Points de terminaison et quotas dans le Références générales AWS.

Tarification

Pour obtenir AppFabric des informations sur les prix et des exemples, consultez la section AWS AppFabric Tarification.

Disponibilité

Pour voir les AWS régions et les points de terminaison actuellement pris en charge AppFabric, consultez la section AWS AppFabric Points de terminaison et quotas dans la référence AWS générale.

Qu'est-ce que c'est AWS AppFabric pour la sécurité ?

AWS AppFabric for security connecte rapidement les applications logicielles en tant que service (SaaS) de votre organisation, afin que les équipes informatiques et de sécurité puissent facilement gérer et sécuriser les applications à l'aide d'un schéma standard.

Rubriques

- Outils et services de sécurité compatibles
- Supprimer AWS AppFabric pour les ressources de sécurité

Avantages

AppFabric Pour des raisons de sécurité, vous pouvez effectuer les opérations suivantes :

- Connectez vos applications en quelques minutes et réduisez les coûts d'exploitation.
- Améliorez la visibilité des données des applications SaaS pour améliorer votre niveau de sécurité.

Cas d'utilisation

AppFabric Pour des raisons de sécurité, vous pouvez :

- Connectez rapidement vos applications SaaS
  - AppFabric for security connecte nativement les meilleures applications de productivité et de sécurité SaaS entre elles, fournissant ainsi une solution d'interopérabilité SaaS entièrement gérée.
- Améliorez votre posture de sécurité
  - Les données des applications sont automatiquement normalisées, ce qui permet aux administrateurs de définir des politiques communes, de standardiser les alertes de sécurité et de gérer facilement l'accès des utilisateurs à plusieurs applications.

Accès AppFabric pour des raisons de sécurité

AppFabric pour la sécurité est disponible dans l'est des États-Unis (Virginie du Nord), en Europe (Irlande) et en Asie-Pacifique (Tokyo) Régions AWS. Pour plus d'informations sur Régions AWS, consultez la section AWS AppFabric Points de terminaison et quotas dans le Références générales AWS.

Dans chaque région, vous pouvez accéder AppFabric pour des raisons de sécurité de l'une des manières suivantes :

AWS Management Console

AWS Management Console Il s'agit d'une interface basée sur un navigateur que vous pouvez utiliser pour créer et gérer AWS des ressources. La AppFabric console permet d'accéder à vos AppFabric

ressources. Vous pouvez utiliser la AppFabric console pour créer et gérer toutes les AppFabric ressources.

AppFabric API

Pour y accéder AppFabric par programmation, utilisez l' AppFabric API et envoyez des requêtes HTTPS directement au service. Pour plus d'informations, consultez le Guide de référence des AWS AppFabric API.

AWS Command Line Interface (AWS CLI)

Avec le AWS CLI, vous pouvez émettre des commandes sur la ligne de commande de votre système pour interagir avec AppFabric d'autres Services AWS. Si vous souhaitez créer des scripts qui exécutent des tâches, les outils de ligne de commande sont également utiles. Pour plus d'informations sur l'installation et l'utilisation du AWS CLI, consultez le guide de AWS Command Line Interface l'utilisateur de la version 2. Pour plus d'informations sur les AWS CLI commandes pour AppFabric, consultez la AppFabric section de la AWS CLI référence.

Services connexes

AppFabric Pour des raisons de sécurité, vous pouvez utiliser ce qui suit Services AWS :

Amazon Data Firehose

Amazon Data Firehose est un service d'extraction, de transformation et de chargement (ETL) qui capture, transforme et diffuse de manière fiable des données en streaming vers des lacs de données, des magasins de données et des services d'analyse. Lorsque vous l'utilisez AppFabric, vous pouvez choisir de générer vos journaux d'audit normalisés ou bruts pour l'Open Cybersecurity Schema Framework (OCSF) au format JSON vers un flux Firehose comme destination. Pour plus d'informations, voir Création d'un emplacement de sortie dans Firehose.

Amazon Security Lake

Amazon Security Lake centralise automatiquement les données de sécurité provenant des AWS environnements, des fournisseurs de SaaS, des sources sur site et dans le cloud dans un lac de données spécialement conçu et stocké dans votre compte. Vous pouvez intégrer les données du journal AppFabric d'audit à Security Lake en sélectionnant Amazon Data Firehose comme destination et en configurant Firehose pour qu'il fournisse les données au format et au chemin corrects dans Security Lake. Pour plus d'informations, consultez la section Collecte de données à partir de sources personnalisées dans le guide de l'utilisateur d'Amazon Security Lake.

Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets offrant une évolutivité, une disponibilité des données, une sécurité et des performances de pointe. Lorsque vous l'utilisez AppFabric, vous pouvez choisir de générer vos journaux d'audit OCSF normalisés (JSON ouApache Parquet) ou bruts (JSON) vers un compartiment Amazon S3 nouveau ou existant comme destination. Pour plus d'informations, consultez Créer un emplacement de sortie dans Amazon S3.

Amazon QuickSight

Amazon fournit QuickSight aux entreprises axées sur les données une intelligence d'affaires (BI) unifiée à grande échelle. Tous les utilisateurs peuvent ainsi répondre à des besoins analytiques variés à partir de la même source de vérité grâce à des tableaux de bord interactifs modernes, à des rapports paginés, à des analyses intégrées et à des requêtes en langage naturel. QuickSight Vous pouvez analyser les données des journaux d' AppFabric audit en QuickSight choisissant le compartiment Amazon S3 dans lequel vos AppFabric journaux sont stockés comme source. Pour plus d'informations, consultez la section Création d'un ensemble de données à l'aide de fichiers Amazon S3 dans le guide de QuickSight l'utilisateur Amazon. Vous pouvez également importer AppFabric des données d'Amazon S3 vers Amazon Athena et sélectionner Amazon Athena comme source de données dans. QuickSight Pour plus d'informations, consultez la section Création d'un ensemble de données à l'aide des données Amazon Athena dans le guide de QuickSight l'utilisateur Amazon.

AWS Key Management Service

Avec AWS Key Management Service (AWS KMS), vous pouvez créer, gérer et contrôler des clés cryptographiques dans vos applications et Services AWS. Lorsque vous créez un bundle d'applications dans AppFabric, vous configurez une clé de chiffrement pour protéger en toute sécurité les données de votre application autorisée. Cette clé chiffre vos données au sein du AppFabric service. AppFabric peut utiliser une clé Clé détenue par AWS créée et gérée par AppFabric en votre nom, ou une clé gérée par le client dans laquelle vous créez et gérez AWS KMS. Pour plus d'informations, consultez la section Création d'une AWS KMS clé.

Cadre de schéma de cybersécurité ouvert

L'Open Cybersecurity Schema Framework (OCSF) est un effort collaboratif AWS et open source mené par des partenaires de premier plan dans le secteur de la cybersécurité. L'OCSF fournit un schéma standard pour les événements de sécurité courants, définit des critères de version pour

faciliter l'évolution du schéma et inclut un processus d'autogouvernance pour les producteurs et les consommateurs de journaux de sécurité. Le code source public d'OCSF est hébergé sur GitHub.

Schéma basé sur OCSF dans AppFabric

Le schéma basé sur OCSF 1.0.0-rc.3 AWS AppFabric pour la sécurité est spécialement conçu pour répondre à vos besoins en matière d'observabilité normalisée, cohérente et facile de leur portefeuille de logiciels en tant que service (SaaS). AppFabric, en collaboration avec la communauté open source de l'OCSF, a introduit de nouvelles catégories d'événements, classes d'événements, activités et objets OCSF afin que l'OCSF soit applicable aux événements d'applications SaaS. AppFabric normalise automatiquement les événements d'audit qu'il reçoit des applications SaaS et transmet ces données aux services Amazon Simple Storage Service (Amazon S3) ou Amazon Data Firehose de votre entreprise. Compte AWS Pour une destination Amazon S3, vous pouvez choisir entre deux options de normalisation (OCSF ou Raw) et deux options de format de données (JSON ouParquet). Lors de la livraison vers Firehose, vous pouvez également choisir entre deux options de normalisation (OCSF ou Raw), mais le format des données est limité au format JSON.

Catégories et classes d'événements OCSF

AppFabric utilise les deux catégories d'événements OCSF suivantes :

- Identity and Access Management : AppFabric pour des raisons de sécurité, utilise les classes d'événements suivantes dans cette catégorie :
  - Changement de compte
  - Authentification
  - Gestion des accès utilisateurs
  - Gestion des groupes
- Activité des applications : AppFabric pour des raisons de sécurité, utilise les classes d'événements suivantes dans cette catégorie :
  - Activité liée aux ressources Web
  - Activité d'accès aux ressources Web

Prérequis et recommandations

Si vous êtes un nouveau AWS client, répondez aux exigences de configuration répertoriées sur cette page avant de commencer à utiliser AWS AppFabric pour des raisons de sécurité. Pour ces

procédures de configuration, vous utilisez le service AWS Identity and Access Management (IAM). Pour des informations complètes sur IAM, consultez le Guide de l'utilisateur IAM.

Rubriques

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique en matière de sécurité consiste à attribuer un accès administratif à un utilisateur et à n'utiliser que l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l‘aide pour vous connecter en utilisant l‘utilisateur racine, consultez Connexion en tant qu‘utilisateur racine dans le Guide de l‘utilisateur Connexion à AWS .
2. Activez l‘authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, consultez la section Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d’ AWS IAM Identity Center dans le Guide de l’utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l‘URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l‘utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

(Obligatoire) Compléter les prérequis de candidature

AppFabric Pour pouvoir recevoir des informations sur les utilisateurs et des journaux d'audit de la part des applications à des fins de sécurité, de nombreuses applications nécessitent que vous disposiez de rôles et de types de plans spécifiques. Assurez-vous d'avoir examiné les conditions requises pour chaque application que vous souhaitez autoriser AppFabric pour des raisons de sécurité, et que vous disposez des plans et des rôles appropriés. Pour plus d'informations sur les prérequis spécifiques à l'application, consultez la section Applications prises en charge ou choisissez l'une des rubriques spécifiques à l'application suivantes.

- 1Password
- Asana
- Azure Monitor
- Atlassian Confluence
- Atlassian Jira suite
- Box
- Cisco Duo
- Dropbox
- Genesys Cloud
- GitHub
- Google Analytics
- Google Workspace
- HubSpot
- IBM Security® Verify
- Microsoft365

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

(Facultatif) Créez un emplacement de sortie

AppFabric pour la sécurité, prend en charge Amazon Simple Storage Service (Amazon S3) et Amazon Data Firehose en tant que destinations d'ingestion des journaux d'audit.

Amazon S3

Vous pouvez créer un nouveau compartiment Amazon S3 à l'aide de la AppFabric console lorsque vous créez une destination d'ingestion. Vous pouvez également créer un compartiment à l'aide du service Amazon S3. Si vous choisissez de créer votre compartiment à l'aide du service Amazon S3, vous devez le créer avant de créer la destination d' AppFabric ingestion, puis sélectionner le compartiment lorsque vous créez la destination d'ingestion. Vous pouvez choisir d'utiliser un compartiment Amazon S3 existant dans votre compartiment Compte AWS, à condition qu'il réponde aux exigences suivantes pour les compartiments existants :

- AppFabric pour des raisons de sécurité, votre compartiment Amazon S3 doit se trouver dans le même Région AWS emplacement que vos ressources Amazon S3.
- Vous pouvez chiffrer votre bucket à l'aide de l'une des méthodes suivantes :
  - Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)

- Chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) en utilisant la valeur par défaut (). Clé gérée par AWS `aws/s3`

Amazon Data Firehose

Vous pouvez choisir d'utiliser Amazon Data Firehose comme destination d'ingestion AppFabric pour les données de sécurité. Pour utiliser Firehose, vous pouvez créer le flux de diffusion Firehose dans votre flux Compte AWS avant de créer une ingestion ou pendant que vous créez une destination d'ingestion dans. AppFabric Vous pouvez créer un flux de diffusion Firehose à l'aide de AWS Management Console, AWS CLI, des AWS API ou des SDK. Pour les instructions de configuration des flux, consultez les rubriques suivantes :

- AWS Management Console instructions — Création d'un flux de diffusion Amazon Data Firehose dans le manuel du développeur Amazon Data Firehose
- AWS CLI instructions — create-delivery-streamdans le manuel de référence des AWS CLI commandes
- AWS Instructions relatives aux API et aux SDK, CreateDeliveryStreamdans le manuel Amazon Data Firehose API Reference

Les exigences relatives à l'utilisation d'Amazon Data Firehose comme destination de sortie AppFabric pour des raisons de sécurité sont les suivantes :

- Vous devez créer le flux de la même manière Région AWS que vos ressources AppFabric de sécurité.
- Vous devez sélectionner Direct PUT comme source.
- Associez une politique AmazonKinesisFirehoseFullAccess AWS gérée à votre utilisateur ou associez les autorisations suivantes à votre utilisateur :

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

Firehose prend en charge l'intégration avec divers outils de sécurité tiers, tels que Splunk et. Logz.io Pour savoir comment configurer correctement Amazon Kinesis afin qu'il génère des données vers ces outils, consultez les paramètres de destination dans le manuel Amazon Data Firehose Developer Guide.

(Facultatif) Créez une AWS KMS clé

Lors de la création d'un ensemble AppFabric d'applications de sécurité, vous devez sélectionner ou configurer une clé de chiffrement pour protéger vos données de manière sécurisée contre toutes les applications autorisées. Cette clé sera utilisée pour chiffrer vos données au sein du AppFabric service.

AppFabric pour des raisons de sécurité, chiffre les données par défaut. AppFabric pour des raisons de sécurité, vous pouvez utiliser une clé Clé détenue par AWS créée et gérée par en AppFabric votre nom ou une clé gérée par le client que vous créez et gérez dans AWS Key Management Service (AWS KMS). Clés détenues par AWS sont un ensemble de AWS KMS clés qu'un utilisateur Service AWS possède et gère pour une utilisation multiple Comptes AWS. Les clés gérées par le client sont des AWS KMS clés Compte AWS que vous créez, détenez et gérez. Pour plus d'informations sur Clés détenues par AWS les clés gérées par le client, consultez la section Clés et AWS clés client dans le guide du AWS Key Management Service développeur.

Si vous souhaitez utiliser une clé gérée par le client pour chiffrer vos données, telles que des jetons d'autorisation, AppFabric pour des raisons de sécurité, vous pouvez en créer une avec AWS KMS. Pour plus d'informations sur la politique d'autorisation qui accorde l'accès à votre clé d'accès gérée par le client AWS KMS, consultez la section Politique relative aux clés de ce guide.

Commencer à utiliser AWS AppFabric pour la sécurité

AWS AppFabric Pour commencer à utiliser la sécurité, vous devez d'abord créer un ensemble d'applications, puis autoriser et connecter des applications à votre ensemble d'applications. Une fois que les autorisations des applications sont connectées aux applications, vous pouvez utiliser des fonctionnalités AppFabric de sécurité telles que l'ingestion des journaux d'audit et l'accès des utilisateurs.

Cette section explique comment commencer à utiliser AppFabric dans le AWS Management Console.

Rubriques

- Étape 2 : Autoriser les applications
- Étape 3 : configurer les ingestions des journaux d'audit
- Étape 4 : utiliser l'outil d'accès utilisateur
- Étape 5 : Connectez-vous AppFabric aux données de sécurité dans les outils de sécurité et d'autres destinations

Prérequis

Avant de commencer, vous devez d'abord créer un utilisateur Compte AWS et un utilisateur administratif. Pour plus d'informations, consultez Inscrivez-vous pour un Compte AWS et Création d'un utilisateur doté d'un accès administratif.

Étape 1 : créer un bundle d'applications

Un bundle d'applications stocke toutes vos AppFabric autorisations et ingestions d'applications de sécurité. Pour créer un ensemble d'applications, configurez une clé de chiffrement afin de protéger en toute sécurité les données de vos applications autorisées.

1. Ouvrez la AppFabric console à l'adresse https://console.aws.amazon.com/appfabric/.
2. Dans le sélecteur Sélectionnez une région situé dans le coin supérieur droit de la page, sélectionnez un. Région AWS AppFabric est disponible uniquement dans les régions de l'est des États-Unis (Virginie du Nord), de l'Europe (Irlande) et de l'Asie-Pacifique (Tokyo).
3. Choisissez Mise en route.
4. Sur la page de démarrage, pour l'étape 1. Créez un ensemble d'applications, choisissez Créer un ensemble d'applications.
5. Dans la section Chiffrement, configurez une clé de chiffrement pour protéger vos données en toute sécurité contre toutes les applications autorisées. Cette clé est utilisée pour chiffrer vos données au sein du service AppFabric de sécurité.

   AppFabric pour des raisons de sécurité, chiffre les données par défaut. AppFabric peut utiliser une clé Clé détenue par AWS créée et gérée par AppFabric en votre nom ou une clé gérée par le client que vous créez et gérez dans AWS Key Management Service (AWS KMS).
6. Pour AWS KMS Clé, choisissez Utiliser Clé détenue par AWS ou Clé gérée par le client.

   Si vous choisissez d'utiliser une clé gérée par le client, entrez le nom de ressource Amazon (ARN) ou l'ID de clé de la clé existante que vous souhaitez utiliser, ou choisissez Create an AWS KMS key.

Tenez compte des points suivants lorsque vous choisissez une clé Clé détenue par AWS ou une clé gérée par le client :

- Clés détenues par AWSsont une collection de clés AWS Key Management Service (AWS KMS) qu'un utilisateur Service AWS possède et gère pour une utilisation multiple Comptes AWS. Bien qu' Clés détenues par AWS elles ne soient pas dans votre compte Compte AWS, un homme Service AWS peut les utiliser Clé détenue par AWS pour protéger les ressources de votre compte. Clés détenues par AWS ne comptez pas dans les AWS KMS quotas de votre compte. Vous n'avez pas besoin de créer ou de maintenir la clé ou sa politique de clé. La rotation des services Clés détenues par AWS varie selon les services. Pour plus d'informations sur la rotation d'un Clé détenue par AWS for AppFabric, consultez la section Chiffrement au repos.
- Les clés gérées par le client sont des clés KMS Compte AWS que vous créez, détenez et gérez. Vous avez un contrôle total sur ces AWS KMS touches. Vous pouvez établir et gérer leurs politiques clés, leurs politiques AWS Identity and Access Management (IAM) et leurs subventions. Vous pouvez les activer et les désactiver, faire pivoter leur matériel cryptographique, ajouter des balises, créer des alias faisant référence aux AWS KMS clés et planifier leur AWS KMS suppression. Les clés gérées par le client apparaissent sur la page des clés gérées par le client du AWS Management Console formulaire AWS KMS.

  Pour identifier définitivement une clé gérée par le client, utilisez l'`DescribeKey`opération. Pour les clés gérées par le client, la valeur du champ `KeyManager` de la réponse `DescribeKey` est `CUSTOMER`. Vous pouvez utiliser votre clé gérée par le client dans le cadre d'opérations cryptographiques et d'audit de l'utilisation dans les AWS CloudTrail journaux. Parmi la plupart Services AWS des solutions intégrées AWS KMS, vous pouvez spécifier une clé gérée par le client pour protéger les données stockées et gérées pour vous. Les clés gérées par le client entraînent des frais mensuels et des frais d'utilisation au-delà du niveau AWS gratuit. Les clés gérées par le client sont prises en compte dans les AWS KMS quotas de votre compte.

Pour plus d'informations sur Clés détenues par AWS les clés gérées par le client, consultez la section Clés et AWS clés client dans le guide du AWS Key Management Service développeur.

> **Note**
>
> Lorsqu'un bundle d'applications est créé, AppFabric pour des raisons de sécurité, vous créez également un rôle IAM spécial dans votre appareil, Compte AWS appelé rôle lié à un service (SLR) pour. AppFabric Cela permet au service d'envoyer des métriques à Amazon CloudWatch. Une fois que vous avez ajouté une destination AppFabric pour le journal d'audit, le SLR autorise le service de sécurité à accéder à vos ressources AWS (compartiments Amazon S3, flux de livraison Amazon Data Firehose). Pour plus d'informations, consultez Utilisation des rôles liés aux services pour AppFabric.

7. (Facultatif) Pour les balises, vous avez la possibilité d'ajouter des balises à votre ensemble d'applications. Les balises sont des paires clé-valeur qui attribuent des métadonnées aux ressources que vous créez. Pour plus d'informations, consultez la section Marquage de vos AWS ressources dans le guide de l'utilisateur de AWS Tag Editor.
8. Pour créer votre bundle d'applications, choisissez Create app bundle.

Étape 2 : Autoriser les applications

Une fois votre bundle d'applications créé avec succès, vous pouvez désormais autoriser, AppFabric pour des raisons de sécurité, la connexion et l'interaction avec chacune de vos applications. Les applications autorisées sont cryptées et stockées dans votre ensemble d'applications. Pour configurer plusieurs autorisations d'applications par bundle d'applications, répétez l'étape d'autorisation d'application selon les besoins de chaque application.

Avant de commencer les étapes d'autorisation des demandes, passez en revue et vérifiez les conditions requises pour chaque demande, telles que le type de plan requis, dansApplications prises en charge.

1. Sur la page de démarrage, pour l'étape 2. Autorisez les applications, choisissez Créer une autorisation d'application.
2. Dans la section Autorisation des applications, sélectionnez l'application à laquelle vous souhaitez autoriser la connexion à AppFabric des fins de sécurité dans la liste déroulante des applications. Les applications présentées sont celles qui sont actuellement prises en charge par AppFabric for security.
3. Lorsque vous sélectionnez une application, les champs d'information obligatoires apparaissent. Ces champs incluent l'ID du locataire et le nom du locataire et peuvent également inclure

l'identifiant du client, le secret du client ou le jeton d'accès personnel. Les valeurs d'entrée pour ces champs varient en fonction de l'application. Pour obtenir des instructions détaillées spécifiques à l'application sur la façon de trouver ces valeurs, consultez. Applications prises en charge

4. (Facultatif) Pour les balises, vous avez la possibilité d'ajouter des balises à l'autorisation de votre application. Les balises sont des paires clé-valeur qui attribuent des métadonnées aux ressources que vous créez. Pour plus d'informations, consultez la section Marquage de vos AWS ressources dans le guide de l'utilisateur de AWS Tag Editor.
5. Choisissez Créer une autorisation d'application.
6. Si une fenêtre contextuelle apparaît (en fonction de l'application connectée), sélectionnez Autoriser AppFabric pour autoriser la connexion à votre application à des fins de sécurité.

   Si l'autorisation de votre application est réussie, vous verrez un message indiquant que l'application est connectée est correctement connectée sur la page de démarrage.
7. Vous pouvez vérifier l'état de l'autorisation de votre application à tout moment sur la page des autorisations des applications répertoriée dans le volet de navigation, sous le statut de chaque application. Le statut Connecté signifie que l'autorisation de votre application a été accordée pour des AppFabric raisons de sécurité pour vous connecter à l'application et qu'elle est terminée.
8. Les statuts d'autorisation possibles des applications sont présentés dans le tableau suivant, y compris les étapes de résolution des problèmes que vous pouvez suivre pour corriger les erreurs associées.

Nom du statut	Description du statut	Étapes de résolution des problèmes
En suspens	Le statut En attente signifie qu'une autorisation d'application est créée, mais qu'elle n'est pas encore connectée à l'application AppFabric pour des raisons de sécurité.	Lorsque ce statut s'affiche, sélectionnez Connect dans le menu déroulant Actions de la page d'autorisation de l'application pour établir une connexion. Si cette erreur persiste, vérifiez si le bloqueur de fenêtres publicitaires de votre navigateur est désactivé

Nom du statut	Description du statut	Étapes de résolution des problèmes
		. Si un message d'erreur, tel que 400 Bad Request, apparaît dans la fenêtre contextuelle, vérifiez que toutes les informations, telles que l'identifiant du locataire, l'identifiant du client et le secret du client, sont correctement saisies. Il est également possible que l'autorisation de l'application ne soit pas créée correctem ent. Pour plus d'informations, consultez la section Applicati ons prises en charge.
La validation de la connexion a échoué	Le statut Échec de la validation de la connexion signifie que, AppFabric pour des raisons de sécurité, il est impossible de valider l'autoris ation de connexion de l'application à une applicati on.	Vérifiez que toutes les informations, telles que l'identifiant du locataire, l'identifiant du client et le secret du client, sont saisies correctement pour l'autoris ation de l'application.
Échec de la rotation automatique du jeton	L'état d'échec de la rotation automatique du jeton signifie que le jeton d'actualisation OAuth a échoué après la connexion réussie de l'autorisation de l'application.	Si cette erreur persiste, vérifiez l'application d'authent ification de l'application. Pour plus d'informations, consultez la section Applicati ons prises en charge.

9. Pour autoriser des applications supplémentaires, répétez les étapes 1 à 8 selon les besoins.

Étape 3 : configurer les ingestions des journaux d'audit

Après avoir créé au moins une autorisation d'application dans votre bundle d'applications, vous pouvez désormais configurer une ingestion du journal d'audit. Une ingestion de journaux d'audit consomme les journaux d'audit d'une application autorisée et les normalise dans le cadre de l'Open Cybersecurity Schema Framework (OCSF). Il les livre ensuite vers une ou plusieurs destinations à l'intérieur de l'île AWS. Vous pouvez également choisir de livrer des fichiers JSON bruts à vos destinations.

1. Sur la page de démarrage, pour l'étape 3. Configurez la section d'ingestion du journal d'audit, sélectionnez Configuration rapide des ingestions.

   > **Note**
   >
   > Pour accélérer la configuration, utilisez la page de configuration rapide des ingestions, accessible uniquement depuis la page de démarrage, afin de créer des ingestions pour plusieurs autorisations d'applications à la fois, avec la même destination d'ingestion. Par exemple, le même compartiment Amazon S3 ou le même flux de données Amazon Data Firehose.
   >
   > Vous pouvez également créer des ingestions depuis la page Ingestions, accessible depuis le volet de navigation. Sur la page Ingestions, vous pouvez configurer une ingestion à la fois pour différentes destinations. Sur la page Ingestions, vous pouvez également créer une balise pour une ingestion. Les instructions suivantes concernent la page de configuration rapide d'Ingestions.

2. Pour Sélectionner les autorisations d'applications, sélectionnez les autorisations d'applications pour lesquelles vous souhaitez créer un journal d'audit pour les ingestions. Les noms des locataires qui apparaissent dans la liste déroulante des autorisations d'applications sont les noms des clients des applications pour lesquelles vous avez déjà créé une autorisation d'application à des AppFabric fins de sécurité.
3. Pour Ajouter une destination, sélectionnez une destination pour les ingestions du journal d'audit des applications que vous avez sélectionnées. Les options de destination incluent Amazon S3 - Existing Bucket, Amazon S3 - New Bucket ou Amazon Data Firehose. Si vous sélectionnez plusieurs noms de locataires, la destination que vous choisissez est appliquée à chaque ingestion d'une autorisation d'application.
4. Lorsque vous choisissez une destination, des champs obligatoires supplémentaires apparaissent.

a. Si vous choisissez Amazon S3 — New bucket comme destination, vous devez saisir le nom du compartiment S3 que vous souhaitez créer. Pour plus d'instructions sur la création d'un compartiment Amazon S3, consultez Créer une destination de sortie.

b. Si vous choisissez Amazon S3 — Compartiment existant comme destination, sélectionnez le nom du compartiment Amazon S3 que vous souhaitez utiliser.

c. Si vous choisissez Amazon Data Firehose comme destination, sélectionnez le nom du flux de diffusion dans la liste déroulante des noms de flux de diffusion Firehose. Pour plus d'instructions sur la création d'un flux de diffusion Amazon Data Firehose, consultez Créer une destination de sortie et notez la politique d'autorisation requise AppFabric pour des raisons de sécurité.

5. Pour Schema & Format, vous pouvez choisir de stocker vos journaux d'audit au format Raw (JSON), OCSF (JSON), OCSF (Parquetpour les compartiments Amazon S3), ou Raw (JSON) ou OCSF-JSON pour Firehose.

   Le format de données brutes fournit les données de votre journal d'audit converties en JSON à partir d'une chaîne de données. Le format de données OCSF normalise les données de votre journal d'audit selon le schéma OCSF (Open Cybersecurity Schema Framework) AppFabric pour la sécurité. Pour plus d'informations sur l' AppFabric utilisation de l'OCSF, consultezCadre de schéma de cybersécurité ouvert. Vous ne pouvez sélectionner qu'un seul schéma et un seul type de données à la fois pour une ingestion. Si vous souhaitez ajouter un schéma et un type de données de format supplémentaires, vous pouvez configurer une destination d'ingestion supplémentaire en répétant le processus de création de l'ingestion.

6. (Facultatif) Si vous souhaitez ajouter une balise à une ingestion, accédez à la page Ingestions depuis le volet de navigation. Pour accéder à la page des détails de l'ingestion, sélectionnez le nom du locataire. Pour les tags, vous avez la possibilité d'ajouter des tags à votre ingestion. Les balises sont des paires clé-valeur qui attribuent des métadonnées aux ressources que vous créez. Pour plus d'informations, consultez la section Marquage de vos AWS ressources dans le guide de l'utilisateur de AWS Tag Editor.

7. Choisissez Configurer les ingestions.

   Lorsque vous avez configuré une ingestion avec succès, vous verrez un message de réussite créé sur la page Getting Started.

8. Vous pouvez également vérifier l'état de vos ingestions et le statut de vos destinations d'ingestion à tout moment sur la page Ingestions du volet de navigation. Sur cette page, vous pouvez voir le nom du locataire créé lors de la création de l'autorisation de l'application, de la

destination et de l'état de vos ingestions. L'état Activé pour votre ingestion signifie que votre ingestion est activée. Si vous choisissez le nom du locataire d'une autorisation d'application sur cette page, vous pouvez voir une page détaillée pour cette autorisation d'application, y compris les détails et le statut de la destination. Le statut Actif pour votre destination d'ingestion signifie que la destination est correctement configurée et active. Si l'autorisation de l'application a le statut Connected et que le statut de destination d'ingestion est Active, le journal d'audit doit être traité et livré. Si le statut d'autorisation de l'application ou le statut de destination d'ingestion sont l'un des états d'échec, le journal d'audit ne sera ni traité ni livré même si le statut d'ingestion est activé. Pour corriger un échec d'autorisation d'une application, reportez-vous à l'étape 2. Autorisez les applications.

9. Les états possibles d'ingestion et de destination d'ingestion sont indiqués dans le tableau suivant, avec les étapes de dépannage que vous pouvez suivre pour corriger tout état d'erreur.

État ou nom du statut	Description	Étapes de résolution des problèmes
Désactivé	Un état désactivé pour l'ingestion signifie que votre ingestion est désactivée.	Vous pouvez activer l'ingestion en sélectionnant Activer dans le menu déroulant Actions de la page Ingestions.
Échec	Un état d'échec pour la destination d'ingestion signifie que la destination d'ingestion n'accepte pas le journal d'audit. Par exemple, cet état peut être dû à un emplacement de stockage complet.	Pour résoudre ces problèmes, accédez aux consoles Amazon S3 ou Firehose.

Étape 4 : utiliser l'outil d'accès utilisateur

À l'aide de l'outil d'accès utilisateur AppFabric for security, les équipes chargées de la sécurité et des administrateurs informatiques peuvent rapidement voir qui a accès à des applications spécifiques en effectuant une simple recherche à l'aide de l'adresse e-mail professionnelle de l'employé. Cette

approche peut être utile pour réduire le temps consacré à des tâches telles que le déprovisionnement des utilisateurs, qui peuvent nécessiter de vérifier ou d'auditer manuellement l'accès des utilisateurs aux applications SaaS. Si un utilisateur est trouvé, AppFabric pour des raisons de sécurité, fournissez le nom de l'utilisateur dans l'application et son statut d'utilisateur intégré à l'application (par exemple, Actif) s'il est fourni par l'application. AppFabric pour les recherches de sécurité, toutes les applications autorisées d'un bundle d'applications renvoient une liste des applications auxquelles l'utilisateur a accès.

1. Sur la page Getting Started, pour l'étape 4. Utilisez l'outil d'accès utilisateur, choisissez Rechercher un utilisateur.
2. Dans le champ Adresse e-mail, saisissez l'adresse e-mail d'un utilisateur, puis sélectionnez Rechercher.
3. Dans la section Résultats de recherche, vous pouvez voir une liste de toutes les applications autorisées auxquelles l'utilisateur a accès. Pour afficher le nom de l'utilisateur dans l'application et son statut (si disponible), sélectionnez un résultat de recherche.
4. Un message d'utilisateur trouvé dans la colonne des résultats de recherche signifie que l'utilisateur peut accéder à l'application répertoriée. Le tableau suivant indique les résultats de recherche possibles, les erreurs et les mesures que vous pouvez prendre pour y remédier.

Résultat de la recherche	Description
L'utilisateur n'a pas été trouvé	Aucun utilisateur n'a été trouvé avec l'adresse e-mail utilisée.
Aucun jeton d'autorisation n'a été trouvé. Connectez l'autorisation de l'application pour l'application.	Vérifiez que toutes les informations, telles que l'identifiant du locataire, l'identifiant du client et le secret du client, sont saisies correctement pour l'autorisation de l'applica tion.
Le jeton d'autorisation a été révoqué. Connectez l'autorisation de l'application pour l'application.	Vérifiez que toutes les informations, telles que l'identifiant du locataire, l'identifiant du client et le secret du client, sont saisies correctement pour l'autorisation de l'applica tion.

Résultat de la recherche	Description
Nous n'avons pas pu faire pivoter le jeton d'autorisation. Connectez l'autorisation de l'application pour l'application.	Le jeton d'actualisation OAuth a échoué une fois que l'autorisation de l'application a été correctement connectée. Si cette erreur persiste, vérifiez l'application d'authentification de l'application. Pour plus d'informations, consultez la section Applications prises en charge.
Les autorisations requises n'ont pas été trouvées. Connectez l'autorisation de l'application pour l'application.	Vérifiez que toutes les informations, telles que l'identifiant du locataire, l'identifiant du client et le secret du client, sont saisies correctement pour l'autorisation de l'application.
L'autorisation de l'application n'est pas valide.	Vérifiez que toutes les informations, telles que l'identifiant du locataire, l'identifiant du client et le secret du client, sont saisies correctement pour l'autorisation de l'application.
Nous n'avons pas pu appeler l'API de l'application en raison d'autorisations insuffisantes.	Vérifiez que toutes les informations, telles que l'identifiant du locataire, l'identifiant du client et le secret du client, sont saisies correctement pour l'autorisation de l'application.
La limite de demandes de candidature a été dépassée.	Il s'agit d'un message d'erreur envoyé par l'application. Vous pouvez essayer de rechercher une adresse e-mail ultérieurement.
L'application a rencontré une erreur interne au serveur	Il s'agit d'un message d'erreur envoyé par l'application. Vous pouvez essayer de rechercher une adresse e-mail ultérieurement.

Résultat de la recherche	Description
L'application a rencontré une erreur de passerelle défectueuse	Il s'agit d'un message d'erreur envoyé par l'application. Vous pouvez essayer de rechercher une adresse e-mail ultérieur ement.
L'application n'est pas prête à traiter la demande	Il s'agit d'un message d'erreur envoyé par l'application. Vous pouvez essayer de rechercher une adresse e-mail ultérieur ement.
L'application a rencontré une erreur de demande incorrecte.	Il s'agit d'un message d'erreur que nous avons reçu de l'application. Vous pouvez réessayer de rechercher un e-mail ultérieur ement.
L'application a rencontré une erreur d'indispo nibilité du service.	Il s'agit d'un message d'erreur que nous avons reçu de l'application. Vous pouvez réessayer de rechercher un e-mail ultérieur ement.

Étape 5 : Connectez-vous AppFabric aux données de sécurité dans les outils de sécurité et d'autres destinations

Les données d'application normalisées (ou brutes) provenant de AppFabric celles-ci sont compatibles avec tous les outils prenant en charge l'ingestion de données depuis Amazon S3 et l'intégration avec Firehose, y compris les outils de sécurité Barracuda XDR tels que DynatraceLogz.io,Netskope,,NetWitness,Rapid7,, et/ou Splunk votre solution de sécurité propriétaire. Pour obtenir des données d'application normalisées (ou brutes) AppFabric, suivez les étapes 1 à 3 précédentes. Pour plus de détails sur la configuration d'outils et de services de sécurité spécifiques, consultez la section Outils et services de sécurité compatibles.

Applications prises en charge

AWS AppFabric for security prend en charge l'intégration avec les applications suivantes. Choisissez le nom d'une application pour plus d'informations sur la configuration de la sécurité AppFabric pour s'y connecter.

Rubriques

- Slack
- Smartsheet
- Terraform Cloud
- Webex by Cisco
- Zendesk
- Zoom

1Password

1Passwordest un gestionnaire de mots de passe qui vous permet de créer, de stocker et d'utiliser des mots de passe forts pour tous vos comptes en ligne. Il protège également vos données grâce au chiffrement, vous alerte en cas de violation et vous permet de partager des mots de passe.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateur1Password, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour 1Password
- Connexion AppFabric à votre 1Password compte

AppFabric support pour 1Password

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir de1Password.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis 1Password des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez disposer d'un plan d'abonnement 1Password Business ou Enterprise payant actif. Pour plus d'informations, consultez 1PasswordEnterprise sur le 1Password site Web.
- Vous devez avoir un rôle d'administrateur ou de propriétaire d'équipe dans le 1Password compte. Pour plus d'informations, consultez la section Groupes sur le site Web d'1Passwordassistance.

Considérations relatives aux limites de taux

L'API 1Password AuditLog Events limite les demandes à 600 par minute et jusqu'à 30 000 par heure. Le dépassement de ces limites renvoie une erreur. Pour plus d'informations, consultez la section Limites de débit des 1Password API dans la référence de l'API 1Password Events.

Considérations relatives au retard des données

Un délai de 30 minutes peut s'écouler avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre 1Password compte

Après avoir créé votre bundle d'applications dans le AppFabric service, vous devez autoriser AppFabric avec1Password. Pour trouver les informations requises pour 1Password l'autorisation AppFabric, procédez comme suit.

Créez un jeton 1Password d'accès personnel

1Passwordprend en charge les jetons d'accès personnels pour les clients publics. Procédez comme suit pour générer un jeton d'accès personnel.

1. Connectez-vous à votre compte 1Password.
2. Choisissez Integrations dans le volet de navigation.
3. Si des intégrations existantes sont présentes, choisissez Directory. Dans le cas contraire, passez à l'étape suivante.
4. Choisissez Autre sous Intégration des rapports d'événements.
5. Sur la page Ajouter une intégration, entrez le nom de votre système de gestion des informations de sécurité et des événements (SIEM) (par exemple, AppFabric Secure)
6. Choisissez Ajouter une intégration, puis effectuez les étapes suivantes sur la page Configurer le jeton.

    a. Indiquez le nom du jeton à utiliser dans l'environnement AppFabric sécurisé.

    b. Nous vous recommandons de sélectionner Jamais dans la liste déroulante Expire après. Si une autre valeur est sélectionnée, le jeton est 1Password révoqué une fois le délai d'expiration écoulé.

c. Dans la section Événements à signaler, choisissez Tentatives de connexion, Événements d'utilisation des articles et Événements d'audit.

7. Choisissez Émettre un jeton pour créer le jeton.
8. Choisissez Enregistrer dans 1Password et effectuez les étapes suivantes.

   a. Le titre sera automatiquement renseigné en fonction de votre système et des noms de jetons.
   b. Choisissez Privé sous Sélectionner un coffre-fort.
   c. Choisissez Enregistrer.

Pour plus d'informations, voir Commencer à utiliser les rapports d'1Passwordévénements sur le 1Password site Web.

Autorisations d'applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'identifiant du locataire AppFabric sera votre adresse de 1Password connexion. Suivez les étapes ci-dessous pour trouver votre identifiant de locataire.

1. Connectez-vous à votre compte 1Password.
2. Choisissez Settings (Paramètres) dans le volet de navigation.
3. Votre 1Password connexion est répertoriée sur la page. Par exemple, example-account.1password.com.

Nom du locataire

Entrez un nom qui identifie cette 1Password organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

Jeton de compte de service

Vous devez disposer d'un jeton de compte de service provenant d'un compte de 1Password service pour accéder à l'autorisation de AppFabric 1Password l'application. Si vous n'avez pas de jeton de compte de service, suivez les instructions suivantes :

AppFabric demandera un jeton de compte de service. Le jeton de compte de service dans AppFabric est le jeton d'accès personnel que vous avez créé. Effectuez les étapes suivantes dans le portail 1Password pour trouver le jeton d'accès personnel.

1. Choisissez Tableau de bord.
2. Choisissez des personnes.
3. Choisissez le nom du titulaire du compte.
4. Choisissez Private (Privé).
5. Choisissez View Vault.
6. Choisissez le nom du jeton.

Autorisation du client

Créez une autorisation d'application en AppFabric utilisant l'ID du locataire, le nom du locataire et le jeton du compte de service. Choisissez ensuite Connect pour activer l'autorisation.

Asana

Asanaest une plateforme de gestion du travail qui aide les individus, les équipes et les organisations à orchestrer le travail, qu'il s'agisse de tâches quotidiennes ou d'initiatives stratégiques interfonctionnelles. Il fournit un système vivant de clarté dans lequel chacun peut communiquer, collaborer et coordonner le travail. Grâce à celaAsana, les équipes intègrent les outils commerciaux essentiels en un seul endroit afin que le travail puisse avancer, où qu'il se passe.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurAsana, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Asana
- Connexion AppFabric à votre Asana compte

AppFabric support pour Asana

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deAsana.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Asana des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez disposer d'un compte Enterprise auprès deAsana. Pour plus d'informations sur la création ou la mise à niveau Asana d'un compte Enterprise, consultez AsanaEnterprise sur le Asana site Web.
- Vous devez avoir un utilisateur ayant le rôle de super administrateur dans votre Asana compte. Pour plus d'informations sur les rôles, consultez la section Rôles d'administrateur et de super administrateur Asana sur le Asana site Web.

Considérations relatives aux limites de taux

Asanaimpose des limites de débit à l'AsanaAPI. Pour plus d'informations sur les limites de débit des Asana API, consultez la section Limites de débit sur le site Web du guide du Asana développeur. Si la combinaison AppFabric de vos Asana applications existantes dépasse la limite, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Asana compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecAsana. Pour trouver les informations requises pour obtenir Asana une autorisation AppFabric, procédez comme suit.

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'ID du locataire dans AppFabric est appelé l'ID de domaine dansAsana. Pour trouver l'ID de domaine, suivez les instructions suivantes depuis l'écran d'Asanaaccueil :

1. Choisissez la photo de profil de votre compte et sélectionnez Admin Console.
2. Sélectionnez ensuite Réglages.
3. Faites défiler l'écran jusqu'à Paramètres du domaine.
4. Entrez l'ID de domaine indiqué dans cette section dans la configuration de l'ID du AppFabric locataire.

Nom du locataire

Entrez un nom qui identifie cette Asana organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

Jeton de compte de service

Vous devez disposer d'un jeton de compte de service provenant d'un compte de Asana service pour accéder à l'autorisation de AppFabric Asana l'application. Si vous n'avez pas de jeton de compte de service, suivez les instructions suivantes :

1. Pour créer un compte de service, suivez les instructions de la section Comptes de service sur le site Web du AsanaGuide.
2. Copiez et enregistrez le jeton en bas de la page Ajouter un compte de service la première fois que vous consultez la page Ajouter un compte de service.
3. Si vous fermez la page Ajouter un compte de service avant d'enregistrer le jeton, vous devez modifier votre compte de service, générer un nouveau jeton et l'enregistrer.

Azure Monitor

Azure Monitorest une solution de surveillance complète permettant de collecter, d'analyser et de répondre aux données de surveillance provenant de vos environnements cloud et sur site. Vous pouvez l'utiliser Azure Monitor pour optimiser la disponibilité et les performances de vos applications et services. Il vous aide à comprendre les performances de vos applications et vous permet de réagir manuellement et par programmation aux événements du système.

Azure Monitorcollecte et agrège les données de chaque couche et composant de votre système sur plusieurs abonnements et locataires Azure et non-Azure. Il les stocke sur une plate-forme de données commune pour être utilisée par un ensemble commun d'outils capables de corréler, d'analyser, de visualiser et/ou de répondre aux données. Vous pouvez également intégrer d'autres

outils Microsoft et non-Microsoft. Le journal Azure Monitor d'activité est un journal de plateforme qui fournit un aperçu des événements liés à l'abonnement. Le journal d'activité contient des informations telles que la modification d'une ressource ou le démarrage d'une machine virtuelle.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurAzure Monitor, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Azure Monitor
- Connexion AppFabric à votre Azure Monitor compte

AppFabric support pour Azure Monitor

AppFabric est capable de recevoir des informations sur les utilisateurs et des journaux d'audit à partir des Azure Monitor services suivants :

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

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Azure Monitor des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez avoir un Microsoft Azure compte avec un essai gratuit ou un pay-as-you-go abonnement.
- Au moins un abonnement est requis pour récupérer les événements inclus dans cet abonnement.

Considérations relatives aux limites de taux

Azure Monitorimpose des limites de débit au responsable de la sécurité (utilisateur ou application) à l'origine des demandes et à l'identifiant d'abonnement ou à l'identifiant du locataire. Pour plus

d'informations sur les limites de débit des Azure Monitor API, consultez Comprendre comment Azure Resource Manager les demandes sont limitées sur le site Web du Azure Monitordéveloppeur.

Considérations relatives au retard des données

Un délai de 30 minutes peut s'écouler avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Azure Monitor compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecAzure Monitor. Pour trouver les informations requises pour Azure Monitor l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Azure Monitorutilisation d'OAuth2. Procédez comme suit pour créer une application OAuth2 dans : Azure Monitor

1. Accédez au Microsoft Azureportail et connectez-vous.
2. Accédez à Microsoft EntraID.
3. Choisissez Inscriptions d'applications.
4. Choisissez Nouvel enregistrement.
5. Entrez un nom pour le client, tel que Azure Monitor OAuth Client. Ce sera le nom de l'application enregistrée.
6. Vérifiez que les types de comptes pris en charge sont définis sur Single Tenant.
7. Pour l'URI de redirection, sélectionnez Web comme plate-forme et ajoutez un URI de redirection. Utilisez le format suivant pour l'URI de redirection :

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

   Cette adresse contient *<region>* le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

La réponse d'authentification sera envoyée à l'URI fourni après l'authentification réussie de l'utilisateur. L'indiquer maintenant est facultatif et peut être modifié ultérieurement, mais une valeur est requise pour la plupart des scénarios d'authentification.

8. Choisissez Register (S'inscrire).
9. Dans l'application enregistrée, choisissez Certificats et secrets, puis Nouveau secret client.
10. Ajoutez une description du secret.
11. Sélectionnez la durée d'expiration du secret. Vous pouvez sélectionner n'importe quelle durée prédéfinie dans le menu déroulant ou définir une durée personnalisée.
12. Choisissez Ajouter. Les valeurs secrètes du client ne peuvent être consultées qu'immédiatement après leur création. Assurez-vous de sauvegarder le secret dans un endroit sûr avant de quitter la page.

Autorisations nécessaires

Vous devez ajouter les autorisations suivantes à votre application OAuth. Pour ajouter des autorisations, suivez les instructions de la section Ajouter des autorisations pour accéder à votre API Web du Guide du Microsoft Entra développeur.

- Microsoft GraphAPI d'accès utilisateur > User.Read.All (sélectionnez le type délégué)
- Microsoft GraphAPI d'accès utilisateur > offline_access (sélectionnez le type délégué)
- AzureAPI du journal d'audit de gestion des services > user_impersonation (sélectionnez le type délégué)

Après avoir ajouté les autorisations, pour accorder le consentement de l'administrateur à ces autorisations, suivez les instructions figurant dans la section du guide du Microsoft Entra développeur consacrée au bouton de consentement de l'administrateur.

Autorisations relatives aux applications

AppFabric prend en charge la réception d'informations utilisateur et de journaux d'audit à partir de votre Azure Monitor compte. Pour recevoir à la fois les journaux d'audit et les données utilisateurAzure Monitor, vous devez créer deux autorisations d'application, l'une nommée Azure Monitordans la liste déroulante des autorisations d'applications et l'autre nommée journaux Azure Monitor d'audit dans la liste déroulante des autorisations d'applications. Vous pouvez utiliser le même identifiant de locataire, le même identifiant client et le même secret client pour les deux

autorisations d'application. Pour recevoir des journaux d'audit de Azure Monitor votre part, vous avez besoin des autorisations de l'application Audit Logs Azure Monitoret de celles de l'application Azure MonitorAudit Logs. Pour utiliser uniquement l'outil d'accès utilisateur, seule l'autorisation de Azure Monitorl'application est requise.

ID de locataire

AppFabric vous demandera votre numéro de locataire. Procédez comme suit pour trouver votre ID client dans Azure Monitor :

1. Accédez au Microsoft Azureportail.
2. Accédez à Azure Active Directory.
3. Dans la section Inscriptions d'applications, choisissez l'application créée précédemment.
4. Dans la section Vue d'ensemble, copiez l'ID du locataire depuis le champ ID du répertoire (tenant).

Nom du locataire

Entrez un nom identifiant cet Azure Monitor abonnement unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

> **Note**
>
> Le nom du locataire doit comporter au maximum 2 048 caractères composés de chiffres, de lettres minuscules ou majuscules et des caractères spéciaux suivants : point (.), trait de soulignement (_), tiret (-) et espace vide.

ID de client

AppFabric demandera un identifiant client. Procédez comme suit pour trouver votre numéro de client dans Azure Monitor :

1. Accédez au Microsoft Azureportail.
2. Accédez à Azure Active Directory.
3. Dans la section Inscriptions d'applications, choisissez l'application créée précédemment.

4. Dans la section Vue d'ensemble, copiez l'ID du client depuis le champ ID de l'application (client).

Secret client

AppFabric demandera un secret client. Le secret client de l'application OAuth enregistrée est celui que vous avez généré à l'étape 11 de la section de création de l'application OAuth. Si vous égarez le secret client généré lors de la création de l'application OAuth, répétez les étapes 8 à 11 de la section Création de l'application OAuth pour en régénérer un nouveau.

Autorisation de l'application

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous Microsoft Azure demandant d'approuver l'autorisation. Connectez-vous à votre compte depuis la fenêtre et approuvez l' AppFabric autorisation en choisissant Autoriser.

Atlassian Confluence

Créez, collaborez et organisez tout votre travail au même endroit. Confluenceest un espace de travail d'équipe où les connaissances et la collaboration se rencontrent. Les pages dynamiques permettent à votre équipe de créer, de capturer et de collaborer sur n'importe quel projet ou idée. Les espaces aident votre équipe à structurer, à organiser et à partager le travail, afin que chaque membre de l'équipe ait une visibilité sur les connaissances institutionnelles et ait accès aux informations dont il a besoin pour donner le meilleur d'lui-même. AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurConfluence, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Atlassian Confluence
- Connexion AppFabric à votre Atlassian Confluence compte

AppFabric support pour Atlassian Confluence

AppFabric prend en charge la réception des journaux d'audit deAtlassian Confluence.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Atlassian Confluence des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Pour accéder aux journaux d'audit, vous devez disposer d'un compte standard, premium ou d'entreprise. Pour plus d'informations sur la création ou la mise à niveau vers le type de Confluence plan applicable, consultez la section ConfluenceTarification sur le Atlassian site Web.
- Pour accéder aux journaux d'audit, vous devez disposer des autorisations d'administrateur pour votre compte. Pour plus d'informations sur les rôles, consultez la section Donner aux utilisateurs des autorisations d'administrateur sur le site Web du Atlassian Support.

Considérations relatives aux limites de taux

Confluenceimpose des limites de débit à l'Atlassian ConfluenceAPI. Si la combinaison de AppFabric vos applications Atlassian Confluence API existantes dépasse les limites fixées, Atlassian Confluence l'affichage des journaux d'audit AppFabric risque d'être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Atlassian Confluence compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecAtlassian Confluence. Pour trouver les informations requises pour Atlassian Confluence l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Atlassian Confluenceutilisation d'OAuth. Pour créer une application OAuth dansAtlassian Confluence, procédez comme suit.

1. Accédez à la AtlassianDeveloper Console.
2. Choisissez l'icône de votre profil en haut à droite, puis choisissez Developer Console.
3. À côté de Mes applications, choisissez Créer, intégration OAuth 2.0.
4. Choisissez Autorisations dans le volet de navigation de gauche, puis choisissez Ajouter à côté de Confluence l'API.
5. Sous Éscopes classiques, sélectionnez Read user (`read:confluence-user`).
6. Sous Étendue granulaire, sélectionnez Afficher les enregistrements d'audit ()`read:audit-log:confluence`.

7. Choisissez Autorisation dans le volet de navigation de gauche, puis choisissez Ajouter à côté de OAuth 2.0 (3LO).
8. Utilisez une URL de redirection au format suivant dans la zone de texte URL de rappel et choisissez Enregistrer les modifications.

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

   Dans cette URL se <region>trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) estus-east-1. Pour cette région, l'URL de redirection esthttps://*us-east-1*.console.aws.amazon.com/appfabric/oauth2.

Champs d'application requis

Vous devez ajouter l'une des étendues suivantes à votre application Atlassian Confluence OAuth. Pour plus d'informations sur les étendues, consultez la section Étendue pour les applications OAuth 2.0 (3LO) et Forge sur le site Web du développeur. Atlassian Utilisez la lunette classique lorsqu'elle est disponible.

- Oscopes classiques :
  - `read:confluence-user`
- Éscopes granulaires :
  - `read:audit-log:confluence`

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'ID du locataire AppFabric est le sous-domaine de votre Atlassian Confluence instance. Vous pouvez trouver le sous-domaine de votre Atlassian Confluence instance dans la barre d'adresse de votre navigateur entre https ://et. atlassian.net.

Nom du locataire

Entrez un nom qui identifie cette Atlassian Confluence organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. Pour trouver votre identifiant client dansAtlassian Confluence, procédez comme suit :

1. Accédez à la AtlassianDeveloper Console.
2. Choisissez l'icône de votre profil en haut à droite, puis sélectionnez Console pour développeurs, Mes applications.
3. Sélectionnez l'application OAuth que vous utilisez pour vous connecter. AppFabric
4. Entrez l'ID client depuis la page Paramètres dans le champ ID client de AppFabric.

Secret client

AppFabric demandera un secret client. Pour trouver le secret de votre client dansAtlassian Confluence, procédez comme suit :

1. Accédez à la AtlassianDeveloper Console.
2. Choisissez l'icône de votre profil en haut à droite, puis sélectionnez Console pour développeurs, Mes applications.
3. Sélectionnez l'application OAuth que vous utilisez pour vous connecter. AppFabric
4. Entrez le secret depuis la page Paramètres dans le champ Secret du client dans AppFabric.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous Atlassian Confluence demandant d'approuver l'autorisation. Pour approuver l' AppFabric autorisation, choisissez Autoriser.

Atlassian Jira suite

Atlassianlibère le potentiel de chaque équipe. Leurs logiciels agiles de gestion des services informatiques et de gestion du travail aident les équipes à organiser, à discuter et à effectuer le travail partagé. DevOps La majorité des entreprises du Fortune 500 et plus de 240 000 entreprises de toutes tailles dans le monde, y compris la NASA,, et Kiva Deutsche BankSalesforce, s'appuient sur Atlassian des solutions pour aider leurs équipes à mieux travailler ensemble et à obtenir des résultats de qualité dans les délais impartis. En savoir plus sur Atlassian les produitsJira Software, notammentConfluence,Jira Service Management,Trello,Bitbucket, et Jira Align sur Atlassian.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateur depuis Jira suite (autre queJira Align), normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

AppFabric soutien à la Jira suite

AppFabric prend en charge la réception d'informations utilisateur et de journaux d'audit depuis leJira suite, à l'exception deJira Align.

Prérequis

Pour pouvoir AppFabric transférer les journaux d'audit des Jira suite destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez avoir un plan Jira standard ou supérieur. Pour plus d'informations sur les fonctionnalités des Jira plans, consultez les pages de tarification relatives aux Jiralogiciels, à la gestion des Jira services, à la gestion du Jira travail et à la découverte de Jira produits.
- Vous devez avoir un utilisateur ayant le rôle d'administrateur de l'organisation dans votre Jira compte. Pour plus d'informations sur les rôles, consultez la section Donner aux utilisateurs des autorisations d'administrateur sur le site Web du Atlassian Support.

Considérations relatives aux limites de taux

La Jira suite impose des limites de débit à l'JiraAPI. Pour plus d'informations sur les limites de débit des Jira suite API, consultez la section Limitation de débit sur le site Web du guide du Atlassian développeur. Si la combinaison AppFabric de vos applications Jira API existantes dépasse la limite, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Un délai de 30 minutes peut s'écouler avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Jira compte

Après avoir créé votre bundle d'applications dans le AppFabric service, vous devez autoriser AppFabric avecJira. Pour trouver les informations requises pour Jira l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Jira suiteOAuth utilisateur. Pour créer une application OAuth dansJira, procédez comme suit :

1. Accédez à la AtlassianDeveloper Console.
2. À côté de Mes applications, choisissez Créer, intégration OAuth 2.0.
3. Donnez un nom à votre application et choisissez Create.
4. Accédez à la section Autorisation et choisissez Ajouter à côté de OAuth 2.0.
5. Utilisez une URL au format suivant dans le champ URL de rappel et choisissez Enregistrer les modifications.

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

   Dans cette URL se <region>trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
6. Accédez à la section Paramètres, copiez votre identifiant client et votre secret client, puis enregistrez-les pour les utiliser pour l'autorisation de AppFabric l'application.

Étendue requise

Vous devez ajouter les étendues suivantes à la page des autorisations de votre application Jira OAuth :

- Dans le cadre des scopes classiques :
  - JiraAPI > `read:jira-user`
- Sous Granular Scopes :
  - JiraAPI > `read:audit-log:jira`

- JiraAPI > `read:user:jira`

Autorisations d'applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'ID du locataire AppFabric est le sous-domaine de votre Jira instance. Vous trouverez le sous-domaine de votre Jira instance dans la barre d'adresse de votre navigateur entre https ://et. atlassian.net.

Nom du locataire

Entrez un nom identifiant ce Jira serveur unique. AppFabricutilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric vous demandera votre numéro de client. Pour trouver votre identifiant client dans Jira, procédez comme suit :

1. Accédez à la AtlassianDeveloper Console.
2. Sélectionnez l'application OAuth que vous utilisez pour vous connecter. AppFabric
3. Entrez l'ID client depuis la page Paramètres dans le champ ID client de AppFabric.

Secret client

AppFabric vous demandera le secret de votre client. Le secret du client AppFabric est le secret dansJira. Pour trouver votre secretJira, procédez comme suit :

1. Accédez à la AtlassianDeveloper Console.
2. Sélectionnez l'application OAuth que vous utilisez pour vous connecter. AppFabric
3. Entrez le secret depuis la page Paramètres dans le champ Secret du client dans AppFabric.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application, AppFabric vous recevrez une fenêtre contextuelle vous Jira permettant d'approuver l'autorisation. Pour approuver l' AppFabricautorisation, choisissez Autoriser.

Box

Boxest le principal Content Cloud, une plateforme unique qui permet aux entreprises de gérer l'ensemble du cycle de vie du contenu, de travailler en toute sécurité où qu'elles se trouvent et de s'intégrer à toutes les best-of-breed applications.

Vous pouvez l'utiliser AWS AppFabric pour recevoir des journaux d'audit et des données utilisateurBox, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les envoyer vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric soutien à Box
- Connexion AppFabric à votre Box compte

AppFabric soutien à Box

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deBox.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Box des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Pour accéder aux journaux d'audit, vous devez disposer d'un abonnement payant actif aux forfaits Business, Business Plus, Enterprise ou Enterprise Plus.
- Vous devez avoir un utilisateur doté des privilèges d'administrateur.
- L'authentification à deux facteurs doit être activée sur votre Box compte pour consulter et copier le secret client de l'application depuis l'onglet de configuration.

Considérations relatives aux limites de taux

Boximpose des limites de débit à l'BoxAPI. Pour plus d'informations sur les limites de débit des Box API, consultez la section Limites de débit sur le site Web du guide du Box développeur. Si la combinaison AppFabric de vos Box applications existantes dépasse la limite, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Il se peut qu'un événement d'audit attende jusqu'à 30 minutes avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Box compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez obtenir une autorisation AppFabric auprès deBox. Pour trouver les informations requises pour Box l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'BoxOAuth utilisateur. Suivez les étapes ci-dessous pour créer une application OAuth dans. Pour plus d'informationsBox, voir Création d'une application OAuth sur le site Web. Box

1. Connectez-vous Box et accédez à la Developer Console.
2. Choisissez Créer une nouvelle application.
3. Choisissez Custom App dans la liste des types d'applications. Un modal apparaîtra pour demander une sélection pour l'étape suivante.
4. Entrez le nom et la description de l'application.
5. Choisissez Intégration dans la liste déroulante Objectif.
    a. Choisissez Sécurité et conformité dans la liste déroulante des catégories.
    b. Entrez AWS AppFabric Securedans le champ Quel système externe vous intégrez-vous ? zone de texte.
6. Choisissez l'authentification du serveur (octroi d'informations d'identification client) si vous souhaitez vérifier l'identité de l'application à l'aide d'un ID client et d'un secret client.
7. Sélectionnez Create App (Créer une application).
8. Cliquez sur l'onglet Configuration.
9. Dans la section Niveau d'accès aux applications de la page, choisissez App + Enterprise Access.
10. Dans la section Champs d'application de la page, choisissez les propriétés Gérer les utilisateurs et Gérer l'entreprise.
11. Choisissez Save Changes (Enregistrer les modifications).

Un Box administrateur doit autoriser l'application dans la console Box d'administration avant de pouvoir l'utiliser. Procédez comme suit pour demander une autorisation.

a. Choisissez l'onglet Autorisation pour votre application dans la Developer Console.

b. Choisissez Réviser et envoyer pour envoyer un e-mail à l'administrateur de votre Box entreprise pour approbation. Pour plus d'informations, consultez la section Autorisation dans le Boxguide.

> **Note**
>
> Vous devez soumettre à nouveau votre application si des modifications sont apportées après la soumission.

Champs d'application requis

Les champs d'application suivants sont requis. Pour plus d'informations sur les portées, consultez la section Scopes sur le site Web de documentation de Box.

- Gérer les propriétés de l'entreprise (`manage_enterprise_properties`)
- Gérer les utilisateurs (`manage_managed_users`)

Autorisations relatives aux applications

ID de locataire

AppFabric demandera un identifiant de locataire. L'ID de locataire indiqué AppFabric est l'identifiant Box d'entreprise. L'BoxEnterprise ID se trouve dans la console d'administration sous Compte et facturation > Informations sur le compte > Enterprise ID. Pour plus d'informations, consultez Enterprise ID sur le site Web de documentation de Box.

Nom du locataire

Entrez un nom qui identifie cette Box organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toute ingestion créée à partir de l'autorisation de l'application.

ID client et code secret du client

1. Connectez-vous Box et accédez à la Developer Console.
2. Choisissez Mes applications dans le menu de navigation.
3. Choisissez l'application OAuth que vous utilisez pour vous connecter. AppFabric
4. Cliquez sur l’onglet Configuration.
5. Accédez à la section Informations d'identification Oauth 2.0 de la page.
6. Entrez l'ID client de votre identifiant client OAuth dans le champ ID client de. AppFabric
7. Choisissez Fetch Client Secret.
8. Entrez le secret client de votre secret client OAuth dans le champ Secret client de. AppFabric

Cisco Duo

Cisco Duoprotège contre les violations grâce à une suite de gestion des accès de pointe qui fournit de solides défenses à plusieurs niveaux et des fonctionnalités innovantes qui permettent aux utilisateurs légitimes d'entrer et d'empêcher les acteurs malveillants d'entrer. Pour toute organisation préoccupée par les failles de sécurité et ayant besoin d'une solution Cisco Duo rapide, permet une sécurité renforcée tout en améliorant la productivité des utilisateurs. AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurCisco Duo, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Cisco Duo
- Connectez-vous AppFabric à votre Cisco Duo compte

AppFabric support pour Cisco Duo

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deCisco Duo.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Cisco Duo des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Pour accéder aux journaux d'audit, vous devez disposer d'un abonnement actif à une édition Duo Essentials, Duo Advantage ou Duo Premier. Les nouveaux clients bénéficiant d'un essai Advantage ou Premier peuvent également y accéder. Pour plus d'informations sur les Cisco Duo éditions, consultez la section Éditions et prix.
- Vous devez être un administrateur avec le rôle de propriétaire pour créer ou modifier l'API d'administration.
- Vous devez ajouter les autorisations « Grant read log resource » pour accéder aux journaux d'audit dans l'API d'administration.

Considérations relatives aux limites de taux

Cisco Duoimpose des limites de débit à l'Cisco DuoAPI. Pour plus d'informations sur les limites de débit des Cisco Duo API, consultez les limites de débit sous Journaux d'authentification. Si la combinaison de AppFabric vos applications Cisco Duo API existantes dépasse les limites fixées, Cisco Duo l'affichage des journaux d'audit AppFabric risque d'être retardé. Contactez Cisco Duo si vous avez besoin d'une augmentation de la limite de débit.

Considérations relatives au retard des données

Un délai de 30 minutes peut s'écouler avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connectez-vous AppFabric à votre Cisco Duo compte

Après avoir créé votre bundle d'applications dans le AppFabric service, vous devez autoriser AppFabric avecCisco Duo. Pour trouver les informations requises pour Cisco Duo l'autorisation AppFabric, procédez comme suit.

Création d'une application API d'Cisco Duoadministration

AppFabric s'intègre à Cisco Duo l'utilisation d'un jeton de service API. Pour créer une application dansCisco Duo, procédez comme suit.

- Pour créer une application d'API Cisco Duo d'administration, suivez les instructions de la section Premiers pas dans l'API Cisco Duo d'administration.

Autorisations nécessaires

Vous devez ajouter les étendues suivantes à votre Cisco Duo application :

- Journal de lecture de Grant
- Subvention : lire une ressource

Autorisations d'applications

ID de locataire

AppFabric demandera un identifiant de locataire. Vous pouvez trouver l'ID du locataire dans le Cisco Duo nom d'hôte. Pour trouver le nom d'hôteCisco Duo, procédez comme suit.

1. Accédez à la page de connexion de l'Cisco Duoadministrateur et connectez-vous.
2. Accédez à Applications, puis choisissez Protéger une application.
3. Recherchez l'entrée relative à l'API d'administration dans la liste des applications, puis choisissez Protéger à l'extrême droite pour configurer votre application et obtenir le nom d'hôte de votre API.
4. Le nom d'hôte de l'API est `api-<tenant-id>.duosecurity.com` formaté comme suit : `<tenant-id>` ID du locataire.

Nom du locataire

Entrez un nom qui identifie cette Cisco Duo organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

Jeton de service

AppFabric demandera un jeton de service. Le jeton de service est une clé d'intégration et une clé secrète séparées par des deux-points au format suivant.

```
integrationkey:secretkey
```

Pour trouver votre clé d'intégration et votre clé secrèteCisco Duo, procédez comme suit.

1. Accédez à la page de connexion de l'Cisco Duoadministrateur et connectez-vous.

2. Accédez à Applications, puis choisissez Protéger une application.
3. « Cliquez sur Protéger une application et recherchez l'entrée relative à l'API d'administration dans la liste des applications. Cliquez sur Protéger à l'extrême droite pour configurer l'application. Faites défiler la page jusqu'à la section des portées et ajoutez **`Grant read log`** et**`Grant read resource`**.

Dropbox

Dropboxaide votre organisation à mieux travailler plus rapidement en rassemblant vos employés, quels que soient le sujet sur lequel ils travaillent, l'endroit où ils travaillent ou le type d'outils qu'ils utilisent. Il permet aux utilisateurs d'accélérer l'innovation et l'efficacité en fournissant un moyen simple et sécurisé de partager du contenu. Dropboxest un endroit où il est possible d'organiser la vie et de faire avancer le travail. Avec plus de 700 millions d'utilisateurs enregistrés dans 180 pays, Dropbox elle a pour mission de concevoir une méthode de travail plus éclairée.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurDropbox, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Dropbox
- Connexion AppFabric à votre Dropbox compte

AppFabric support pour Dropbox

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deDropbox.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Dropbox des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez disposer d'un compte Dropbox professionnel. Pour plus d'informations sur la création ou la mise à niveau Dropbox d'un compte Business, consultez DropboxBusiness sur le Dropbox site Web.

- Vous devez avoir un utilisateur ayant le rôle d'administrateur d'équipe sur votre Dropbox compte. Pour plus d'informations sur les rôles, consultez Comment modifier les droits d'administrateur de votre Dropbox équipe sur le site Web du centre d'Dropboxaide.

Considérations relatives aux limites de taux

Dropboximpose des limites de débit à l'DropboxAPI. Pour plus d'informations sur les limites de débit des Dropbox API, consultez la section Limites de débit sur le site Web du Guide des Dropbox performances. Si la combinaison AppFabric de vos applications Dropbox API existantes dépasse la limite, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Dropbox compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecDropbox. Pour trouver les informations requises pour obtenir Dropbox une autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Dropboxutilisation d'OAuth. Pour créer une application OAuth dansDropbox, procédez comme suit :

1. Choisissez Créer une application dans l'DropboxApp Console à l'adresse https://www.dropbox.com/developers/apps.
2. Sur la nouvelle page de configuration de l'application, choisissez Accès étendu pour l'API.
3. Ensuite, sélectionnez Complet Dropbox pour le type d'accès.
4. Nommez votre application OAuth, puis choisissez Create app pour terminer la configuration initiale de l'application OAuth.
5. Sur la page d'informations de l'application, ajoutez une URL de redirection au format suivant dans le champ URI de redirection OAuth2.

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

Dans cette URL se *<region>* trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2`.

6. Choisissez Ajouter.
7. Copiez et enregistrez la clé et le secret de votre application pour les utiliser dans le cadre de l'autorisation de AppFabric l'application.
8. Vous pouvez conserver les valeurs par défaut de tous les autres champs de l'onglet Paramètres.

Champs d'application requis

Vous devez ajouter les étendues suivantes à votre Dropbox application à l'aide de l'onglet Autorisations de l'écran d'informations de l'application :

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

Choisissez Soumettre une fois que vous avez terminé.

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. Entrez toute valeur identifiant de manière unique votre Dropbox compte, telle que le nom de l'équipe.

Nom du locataire

Entrez un nom qui identifie ce Dropbox compte unique. AppFabricutilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. L'ID client indiqué AppFabric est la clé de votre Dropbox application. Pour trouver la clé de votre application Dropbox, procédez comme suit :

1. Accédez à l'DropboxApp Console à l'adresse https://www.dropbox.com/developers/apps.
2. Trouvez l'application que vous utilisez pour vous connecter AppFabric.
3. Trouvez la clé de l'application dans la section État de la page d'informations de l'application.
4. Entrez la clé d'application de votre Dropbox application dans le champ ID client de AppFabric.

Secret client

AppFabric demandera un secret client. Le code secret du client AppFabric est le secret de votre Dropbox application. Pour trouver le secret de votre Dropbox application, procédez comme suit :

1. Accédez à l'DropboxApp Console à l'adresse https://www.dropbox.com/developers/apps.
2. Trouvez l'application que vous utilisez pour vous connecter AppFabric.
3. Trouvez le secret de l'application dans la section État de la page d'informations de l'application.
4. Entrez le secret de l'application pour votre Dropbox application dans le champ Secret du client dans AppFabric.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous Dropbox demandant d'approuver l'autorisation. Pour approuver l' AppFabric autorisation, choisissez Autoriser.

Genesys Cloud

Genesys Cloudcrée des conversations fluides sur les canaux numériques et vocaux dans une all-in-one interface simple. Cela permet aux entreprises d'offrir des expériences exceptionnelles à leurs employés et à leurs clients et de tirer parti des avantages de déploiements rapides, d'une complexité réduite et d'une administration simplifiée. AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurGenesys Cloud, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

AppFabric support pour Genesys Cloud

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deGenesys Cloud.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Genesys Cloud des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez avoir un Genesys Cloud compte.
- Vous devez avoir un utilisateur ayant le rôle d'administrateur dans votre Genesys Cloud compte.

Considérations relatives aux limites de taux

Genesys Cloudimpose des limites de débit à l'Genesys CloudAPI. Pour plus d'informations sur les limites de débit des Genesys Cloud API, consultez la section Limites de débit sur le Genesys Cloud Developer site Web.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Genesys Cloud compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecGenesys Cloud. Pour trouver les informations requises pour obtenir Genesys Cloud une autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Genesys Cloudutilisation d'OAuth. Pour créer une application OAuth dansGenesys Cloud, procédez comme suit :

1. Suivez les instructions de la section Créer un client OAuth sur le site Web du centre de Genesys Cloud ressources.

   Pour les types de subventions, choisissez Code Authorization.

2. Utilisez une URL de redirection au format suivant comme URI de redirection autorisée.

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

   Dans cette URL se <region>trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

3. Sélectionnez la case Étendue pour afficher la liste des étendues disponibles pour votre application. Sélectionnez l'étendue `audits:readonly` et`users:readonly`. Pour plus d'informations sur les étendues, consultez la section OAuth Scopes dans le Developer Center. Genesys Cloud

4. Choisissez Enregistrer. Genesys Cloudcrée un ID client et un secret client (jeton).

Champs d'application requis

Vous devez ajouter les étendues suivantes à votre application Genesys Cloud OAuth :

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

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'ID du locataire AppFabric est le nom de votre Genesys Cloud instance. Vous trouverez votre identifiant de locataire dans la barre d'adresse de votre navigateur. Par exemple, l'ID du locataire `usw2.pure.cloud` se trouve-t-il dans l'URL suivante`https://login.usw2.pure.cloud`.

Nom du locataire

Entrez un nom qui identifie cette Genesys Cloud organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. Pour trouver votre identifiant client dansGenesys Cloud, procédez comme suit :

1. Choisissez Admin.
2. Sous Intégrations, choisissez OAuth.
3. Choisissez le client OAuth pour obtenir l'ID du client.

Secret client

AppFabric demandera un secret client. Pour trouver le secret de votre client dansGenesys Cloud, procédez comme suit :

1. Choisissez Admin.
2. Sous Intégrations, choisissez OAuth.
3. Choisissez le client OAuth pour obtenir le secret du client.

GitHub

GitHubest une plateforme et un service basé sur le cloud pour le développement de logiciels et le contrôle de version à l'aide de Git, permettant aux développeurs de stocker et de gérer leur code. Il fournit le contrôle de version distribué de Git ainsi que le contrôle d'accès, le suivi des bogues, les demandes de fonctionnalités logicielles, la gestion des tâches, l'intégration continue et les wikis pour chaque projet. AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurGitHub, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour GitHub
- Connexion AppFabric à votre GitHub compte

AppFabric support pour GitHub

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deGitHub.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis GitHub des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Pour accéder aux journaux d'audit, vous devez disposer d'un compte d'entreprise.
- Pour accéder aux journaux d'audit d'entreprise, vous devez avoir le rôle d'administrateur pour votre compte d'entreprise.
- Pour obtenir les journaux d'audit de l'organisation, vous devez être propriétaire de l'organisation.

Considérations relatives aux limites de taux

GitHubimpose des limites de débit à l'GitHubAPI. Pour plus d'informations sur les limites de débit des GitHub API, consultez la section Limites et allocations des demandes d'API sur le GitHubsite Web. Si la combinaison de vos applications GitHub API existantes AppFabric et de vos applications d'API existantes dépasse GitHub's les limites, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre GitHub compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecGitHub. Pour trouver les informations requises pour obtenir GitHub une autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'GitHubOAuth utilisateur. Procédez comme suit pour créer une application OAuth dans. GitHub Pour plus d'informations, consultez la section Création d' GitHubs applications sur le GitHubsite Web.

1. Choisissez votre photo de profil située dans le coin supérieur droit de la page, puis sélectionnez Paramètres.
2. Choisissez Paramètres du développeur dans le volet de navigation de gauche.
3. Choisissez les applications OAuth dans le volet de navigation de gauche.
4. Choisissez Nouvelle application OAuth.

   > **Note**
   >
   > Ce bouton sera intitulé Enregistrer une nouvelle application si vous n'avez pas encore créé d'application OAuth.

5. Entrez le nom de votre application dans la zone de texte Nom de l'application.
6. Entrez l'URL complète de l'instance de l'application dans la zone de texte URL de la page d'accueil.
7. (Facultatif) Entrez une description pour votre application dans la zone de texte Description de l'application. Les utilisateurs verront cette description.
8. Entrez une URL au format suivant dans la zone de texte URL de rappel d'autorisation.

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

   Dans cette URL se <region>trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
9. Choisissez Activer le flux d'appareils si votre application OAuth utilisera le flux d'appareils pour identifier et autoriser les utilisateurs. Pour plus d'informations sur le flux d'appareils, consultez la section Autorisation des applications OAuth sur le site Web. GitHub
10. Choisissez Enregistrer l'application.

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'ID du locataire doit être fourni dans l'un des formats suivants :

Journal d'audit de l'entreprise :

Utilisez le journal d'audit de l'entreprise si vous souhaitez connaître les actions agrégées de toutes les organisations détenues par votre compte d'entreprise.

Pour utiliser le journal d'audit d'entreprise, l'identifiant du locataire est l'identifiant d'entreprise de votre compte. Vous trouverez votre identifiant d'entreprise dans la barre d'adresse de votre navigateur. Par exemple, l'ID d'entreprise *exampleenterprise* se trouve-t-il dans l'URL suivantehttps://github.com/settings/enterprises/*examplenterprise*.

Lorsque vous spécifiez l'ID du locataire pour le journal d'audit de l'entreprise, vous devez le préfixer parenterprise:. Par conséquent, spécifiez l'exemple précédent sous la formeenterprise:examplenterprise.

Journal d'audit de l'organisation :

Utilisez le journal d'audit de l'organisation en tant qu'administrateur de l'organisation si vous souhaitez connaître les actions effectuées par les membres de votre organisation. Il inclut des détails tels que qui a effectué l'action, quelle était l'action et quand elle a été effectuée.

Pour utiliser le journal d'audit de l'organisation, l'identifiant du locataire est l'identifiant de votre organisation. L'identifiant de votre organisation se trouve dans la barre d'adresse de votre navigateur. Par exemple, l'ID de l'organisation *exampleorganization* se trouve-t-il dans l'URL suivantehttps://github.com/settings/organizations/*exampleorganization*.

Lorsque vous spécifiez l'ID du locataire pour le journal d'audit de l'organisation, vous devez le préfixer parorganization:. Par conséquent, spécifiez l'exemple précédent sous la formeorganization:exampleorganization.

Nom du locataire

Entrez un nom qui identifie cette GitHub entreprise ou organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. Suivez les étapes ci-dessous pour trouver votre identifiant client dansGitHub,

1. Choisissez votre photo de profil située dans le coin supérieur droit de la page, puis sélectionnez Paramètres.

2. Choisissez Paramètres du développeur dans le volet de navigation de gauche.
3. Choisissez les applications OAuth dans le volet de navigation de gauche.
4. Choisissez l'application OAuth spécifique, puis recherchez la valeur de l'ID client.

Secret client

AppFabric demandera un secret client. Suivez les étapes ci-dessous pour trouver le secret de votre client dansGitHub.

1. Choisissez votre photo de profil située dans le coin supérieur droit de la page, puis sélectionnez Paramètres.
2. Choisissez Paramètres du développeur dans le volet de navigation de gauche.
3. Choisissez les applications OAuth dans le volet de navigation de gauche.
4. Choisissez l'application OAuth spécifique, puis recherchez la valeur du secret client. Si vous ne parvenez pas à trouver un secret client existant, vous devrez peut-être en générer un nouveau.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous GitHub demandant d'approuver l'autorisation. Pour approuver l' AppFabric autorisation, choisissez Autoriser.

Assurez-vous que vos organisations ont accordé l'accès à l'application OAuth, si les restrictions d'accès à l'application OAuth sont activées.

Google Analytics

Google Analyticsest un service d'analyse Web qui fournit des statistiques et des outils analytiques de base à des fins d'optimisation des moteurs de recherche (SEO) et de marketing. Google Analyticsest utilisé pour suivre les performances du site Web et recueillir des informations sur les visiteurs. Il peut aider les organisations à déterminer les principales sources de trafic utilisateur, à évaluer le succès de leurs activités et campagnes marketing, à suivre la réalisation des objectifs (tels que les achats, l'ajout de produits aux paniers), à découvrir des modèles et des tendances en matière d'engagement des utilisateurs et à obtenir d'autres informations sur les visiteurs, telles que des données démographiques. Les sites Web de vente au détail de petite et moyenne taille utilisent souvent Google Analytics pour obtenir et analyser diverses analyses du comportement des clients,

qui peuvent être utilisées pour améliorer les campagnes marketing, générer du trafic sur le site Web et mieux fidéliser les visiteurs.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurAzure Monitor, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

AppFabric support pour Google Analytics

AppFabric prend en charge la réception des journaux d'audit deGoogle Analytics.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Google Analytics des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez être administrateur du Google Analytics compte.
- AppFabric Pour fournir des journaux, vous devez activer l'API Google Analytics Admin sur votre Google Cloud projet. Assurez-vous d'utiliser un nouveau projet lors de la configuration de l'application Google Analytics OAuth.

Considérations relatives aux limites de taux

Google Analyticsimpose des limites de débit à l'Google AnalyticsAPI. Pour plus d'informations sur les limites de débit des Google Analytics API, consultez la section Limites et quotas sur le site Web de Google Analytics. Si la combinaison AppFabric de vos applications API Google Analytics existantes dépasse la limite, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Google Analytics compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecGoogle Analytics. Suivez les étapes ci-dessous pour trouver les informations nécessaires à l'autorisation Google Analytics auprès de AppFabric.

Création d'une application OAuth

AppFabric s'intègre à l'Google AnalyticsOAuth utilisateur. Procédez comme suit pour créer une application OAuth dans : Google Analytics

1. Pour configurer votre écran de consentement OAuth, suivez les instructions de la section Configurer l'écran de consentement OAuth dans le guide du développeur de Google sur le site Web de Google.
2. Choisissez Externe pour le type d'utilisateur
3. Pour configurer les informations d'identification OAuth pour AppFabric, suivez les instructions de la section Informations d'identification du client OAuth de la page Créer des informations d'identification d'accès du guide du développeur de Google.
4. Utilisez une URL de redirection au format suivant.

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

   Cette adresse contient *<region>* le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Champs d'application requis

Vous devez ajouter l'étendue suivante à votre application Google Analytics OAuth :

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

Autorisations relatives aux applications

ID de locataire

AppFabric demandera un identifiant de locataire. L'identifiant du locataire indiqué AppFabric est l'identifiant de votre Google Analytics compte.

1. Accédez à la page Google Analytics d'accueil.
2. Choisissez Admin dans le volet de navigation.
3. Vous trouverez votre numéro de compte sous Compte > Paramètres du compte > Détails du compte > Numéro de compte.

Nom du locataire

Entrez un nom qui identifie cette Google Analytics organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. Suivez les étapes ci-dessous pour trouver votre identifiant client dans Google Analytics :

1. Accédez à la page des informations d'identification.
2. Dans la section ID client OAuth 2.0, choisissez l'ID client que vous avez créé.
3. L'ID client est répertorié dans la section Informations supplémentaires de la page.

Secret client

AppFabric demandera un secret client. Suivez les étapes ci-dessous pour trouver le secret de votre client dans Google Analytics :

1. Accédez à la page des informations d'identification.
2. Dans la section ID client OAuth 2.0, choisissez le nom du client.
3. Le secret du client est répertorié dans la section Secrets du client de la page.

Autorisation de l'application

Après avoir créé l'autorisation de l'application, AppFabric vous recevrez une fenêtre contextuelle vous Google Analytics permettant d'approuver l'autorisation. Pour approuver l' AppFabric autorisation en choisissant Autoriser.

Google Workspace

Google Workspaceest un ensemble d'outils de cloud computing, de productivité et de collaboration, de logiciels et de produits développés et commercialisés par Google.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurGoogle Workspace, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Google Workspace
- Connexion AppFabric à votre Google Workspace compte

AppFabric support pour Google Workspace

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deGoogle Workspace.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Google Workspace des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez souscrire au plan Google Workspace Enterprise Standard. Pour plus d'informations sur la création ou la mise à niveau vers le plan Google Workspace Enterprise Standard, consultez le site Web Google Workspacedes plans.
- Vous devez avoir un utilisateur ayant le rôle d'administrateur dans votreGoogle Workspace.
- AppFabric Pour fournir des journaux, vous devez activer l'API du SDK Google Admin sur votre projet Google Cloud. Pour plus d'informations, consultez la section Activer les API Google Workspace dans le guide du Google Workspace développeur.

Considérations relatives aux limites de taux

Google Workspaceimpose des limites de débit à l'Google WorkspaceAPI. Pour plus d'informations sur les limites de débit des Google Workspace API, consultez la section Limites et quotas du guide Google Workspace d'administration disponible sur le Google Workspace site Web. Si la combinaison

AppFabric de vos applications Google Workspace API existantes dépasse la limite, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Il est possible que la plupart des événements d'audit soient retardés de 30 minutes et que certains événements d'audit soient livrés à destination jusqu'à 4 heures. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Pour plus d'informations, consultez la section Conservation des données et temps de latence sur le site Web WorkSpace d'aide aux administrateurs de Google. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Google Workspace compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecGoogle Workspace. Pour trouver les informations requises pour obtenir Google Workspace une autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Google Workspaceutilisation d'OAuth. Pour créer une application OAuth dansGoogle Workspace, procédez comme suit :

1. Pour configurer votre écran de consentement OAuth, suivez les instructions de la section Configurer l'écran de consentement OAuth dans le guide du Google Workspace développeur sur le site Web. Google Workspace

   Choisissez Internal pour le type d'utilisateur.
2. Pour configurer les informations d'identification OAuth pour AppFabric, suivez les instructions de la section Informations d'identification du client OAuth de la page Créer des informations d'identification d'accès du guide du développeur. Google Workspace
3. Utilisez une URL de redirection au format suivant.

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

   Dans cette URL se *<region>* trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2`.

Champs d'application requis

Vous devez ajouter les étendues suivantes à votre application Google Workspace OAuth :

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

Si ces étendues ne s'affichent pas, ajoutez l'API du SDK d'administration à votre bibliothèque d'API Google Cloud.

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'identifiant du locataire indiqué AppFabric est l'identifiant de votre Google Workspace projet. Pour trouver l'ID de votre projet, voir Localiser l'ID du projet sur le site Web d'aide de l'GoogleAPI Console.

Nom du locataire

Entrez un nom qui identifie cet objet uniqueGoogle Workspace. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric vous demandera votre numéro de client. Pour trouver votre identifiant client, procédez comme suit :

1. Trouvez votre identifiant client à l'aide des informations de la section Afficher les informations d'identification de la page Gérer les informations d'identification du guide du Google Workspace développeur.
2. Entrez l'ID client de votre client OAuth dans le champ ID client de. AppFabric

Secret client

AppFabric vous demandera le secret de votre client. Pour trouver le secret de votre client, procédez comme suit :

1. Trouvez le secret de votre client à l'aide des informations contenues dans la section Afficher les informations d'identification de la page Gérer les informations d'identification du guide du Google Workspace développeur.
2. Si vous devez réinitialiser votre secret client, suivez les instructions de la section Réinitialiser le secret client de la page Gérer les informations d'identification du guide du Google Workspace développeur.
3. Entrez le secret de votre client dans le champ Secret client de AppFabric.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application, AppFabric vous recevrez une fenêtre contextuelle vous Google Workspace permettant d'approuver l'autorisation. Pour approuver l' AppFabric autorisation, choisissez Autoriser.

HubSpot

HubSpotest une plateforme client dotée de tous les logiciels, intégrations et ressources dont vous avez besoin pour connecter votre marketing, vos ventes, votre gestion de contenu et votre service client. HubSpotLa plateforme connectée vous permet de développer votre activité plus rapidement en vous concentrant sur ce qui compte le plus : vos clients. AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurHubSpot, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour HubSpot
- Connexion AppFabric à votre HubSpot compte

AppFabric support pour HubSpot

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deHubSpot.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis HubSpot des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez disposer d'un compte avec l'abonnement Enterprise HubSpot pour accéder aux journaux d'audit. Pour plus d'informations sur HubSpot les abonnements, voir Gérer votre HubSpot abonnement dans la base de HubSpot connaissances.
- Vous devez disposer d'un compte développeur et d'une application associée à ce compte.
- Vous devez être un super administrateur pour installer des applications sur votre HubSpot compte ou disposer de l'autorisation App Marketplace Access et des autorisations utilisateur pour accepter les étendues demandées par l'application.

Considérations relatives aux limites de taux

HubSpotimpose des limites de débit à l'HubSpotAPI. Pour plus d'informations sur les limites de débit des HubSpot API, y compris les limites pour les applications utilisant OAuth, consultez la section Limites de débit sur le HubSpot site Web. Si la combinaison de AppFabric vos applications HubSpot API existantes dépasse les limites fixées, HubSpot l'affichage des journaux d'audit AppFabric risque d'être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre HubSpot compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecHubSpot. Pour trouver les informations requises pour obtenir HubSpot une autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'HubSpotutilisation d'OAuth. Pour créer une application OAuth dansHubSpot, procédez comme suit :

1. Suivez les instructions de la section Créer une application publique du HubSpot guide sur le HubSpot site Web.
2. Dans l'onglet Auth, ajoutez les trois étendues répertoriées dans. Champs d'application requis
3. Utilisez une URL de redirection au format suivant dans URL de redirection.

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

Dans cette URL se <region>trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) estus-east-1. Pour cette région, l'URL de redirection esthttps://*us-east-1*.console.aws.amazon.com/appfabric/oauth2.

4. Choisissez Créer une application.

Champs d'application requis

Vous devez ajouter les étendues suivantes à votre application HubSpot OAuth :

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

Autorisations relatives aux applications

ID de locataire

Entrez un identifiant identifiant cette HubSpot organisation unique. Par exemple, entrez votre identifiant de HubSpot compte.

Nom du locataire

Entrez un nom qui identifie cette HubSpot organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. Pour trouver votre identifiant client dansHubSpot, procédez comme suit :

1. Accédez à la page de HubSpot connexion et connectez-vous à l'aide des informations d'identification de votre compte développeur.
2. Dans le menu Applications, choisissez votre application.
3. Dans l'onglet Auth, recherchez la valeur de l'ID client.

Secret client

AppFabric demandera un secret client. Pour trouver le secret de votre client dansHubSpot, procédez comme suit :

1. Accédez à la page de HubSpot connexion et connectez-vous à l'aide des informations d'identification de votre compte développeur.
2. Dans le menu Applications, choisissez votre application.
3. Dans l'onglet Auth, recherchez la valeur secrète du client.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous HubSpot demandant d'approuver l'autorisation. Connectez-vous à votre compte à l'aide des informations d'identification de votre compte d'entreprise (et non de votre compte développeur) pour approuver l' AppFabric autorisation. Choisissez Autoriser.

IBM Security® Verify

La IBM Security® Verify gamme fournit des fonctionnalités automatisées, basées sur le cloud et sur site pour administrer la gouvernance des identités, gérer l'identité et l'accès du personnel et des consommateurs, et contrôler les comptes privilégiés. Que vous deviez déployer une solution dans le cloud ou sur site, IBM Security® Verify cela vous aide à établir la confiance et à vous protéger contre les menaces internes, tant pour votre personnel que pour les consommateurs.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurIBM Security® Verify, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric soutien à IBM Security® Verify
- Connexion AppFabric à votre IBM Security® Verify compte

AppFabric soutien à IBM Security® Verify

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deIBM Security® Verify.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis IBM Security® Verify des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Pour accéder aux journaux d'audit, vous devez disposer d'un compte IBM Security® Verify SaaS.
- Pour accéder aux journaux d'audit, vous devez avoir un rôle d'administrateur dans votre compte IBM Security® Verify SaaS.

Considérations relatives aux limites de taux

IBM Security® Verifyimpose des limites de débit à l'IBM Security® VerifyAPI. Pour plus d'informations sur les limites de débit des IBM Security® Verify API, consultez les conditions IBM. Si la combinaison de vos applications IBM Security® Verify API existantes AppFabric et de vos applications d'API existantes dépasse IBM Security® Verify les limites, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Il se peut qu'un événement d'audit attende jusqu'à 30 minutes avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre IBM Security® Verify compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecIBM Security® Verify. Pour trouver les informations requises pour obtenir IBM Security® Verify une autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'IBM Security® VerifyOAuth utilisateur. Pour créer une application OAuth dansIBM Security® Verify, consultez la section Créer un client API sur le site Web de documentation IBM.

1. Pour vous connecter pour la première fois, utilisez l'URL de connexion et les informations d'identification qui ont été envoyées à l'adresse e-mail que vous avez enregistrée.
2. Accédez à la console d'administration à l'adresse`https://<hostname>.verify.ibm.com/ui/admin/`. Pour plus d'informations, consultez Accès à IBM Security® Verify.

3. Dans la console d'administration, sous Sécurité < Accès aux API < Client API, choisissez Ajouter.
4. Sélectionnez les options suivantes. Ils sont nécessaires pour lire le journal d'audit et les détails de l'utilisateur.
   - Lire les rapports
   - Utilisateurs et groupes en lecture
5. Conservez l'option Par défaut dans la méthode d'authentification du client.

   Ne modifiez pas le champ Étendue personnalisée.
6. Choisissez Suivant.
7. Ne modifiez pas le champ du filtre IP.
8. Choisissez Suivant.
9. Ne modifiez pas le champ Propriétés supplémentaires.
10. Choisissez Suivant.
11. Spécifiez un nom et une description. La description est facultative.
12. Choisissez Create API client.

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. Vous pouvez trouver l'ID du locataire dans l'URL IBM Security® Verify standard. Par exemple, dans l'`https://`*`hostname`*`.verify.ibm.com/`URL, l'ID du locataire est le *`nom d'hôte`* qui se trouve auparavant `.verify.ibm.com` (ou avant `ice.ibmcloud.com` si vous utilisez un ancien nom d'hôte). Si vous utilisez une URL personnalisée, contactez votre équipe d'IBM Security® Verifyassistance pour obtenir votre URL standard.

Nom du locataire

Entrez un nom qui identifie ce IBM Security® Verify locataire unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toute ingestion créée à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. Pour trouver votre identifiant client dansIBM Security® Verify, procédez comme suit :

1. Pour vous connecter pour la première fois, utilisez l'URL de connexion et les informations d'identification qui ont été envoyées à l'adresse e-mail que vous avez enregistrée.
2. Accédez à la console d'administration à l'adresse`https://<hostname>.verify.ibm.com/ui/admin/`. Pour plus d'informations, consultez Accès à IBM Security® Verify.
3. Dans la console d'administration, sous Sécurité **<** Accès aux API **<** Client API, choisissez les points de suspension () à côté de l'application OAuth spécifique.
4. Choisissez Détails de connexion.
5. Localisez l'ID client sous les informations d'identification de l'API.

Secret client

AppFabric demandera un secret client. Pour trouver le secret de votre client dansIBM Security® Verify, procédez comme suit :

1. Pour vous connecter pour la première fois, utilisez l'URL de connexion et les informations d'identification qui ont été envoyées à l'adresse e-mail que vous avez enregistrée.
2. Accédez à la console d'administration à l'adresse`https://<hostname>.verify.ibm.com/ui/admin/`. Pour plus d'informations, consultez Accès à IBM Security® Verify.
3. Dans la console d'administration, sous Sécurité **<** Accès aux API **<** Client API, choisissez les points de suspension () à côté de l'application OAuth spécifique.
4. Choisissez Détails de connexion.
5. Localisez le secret du client sous les informations d'identification de l'API.

Microsoft365

Microsoft365 est une famille de produits de logiciels de productivité, de collaboration et de services cloud appartenant àMicrosoft.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir les journaux d'audit et les données utilisateur de Microsoft 365, normaliser les données au format Open Cybersecurity Schema

Framework (OCSF) et les envoyer dans un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Microsoft 365
- Connexion AppFabric à votre compte Microsoft 365

AppFabric support pour Microsoft 365

AppFabric prend en charge la réception d'informations utilisateur et de journaux d'audit à partir de Microsoft 365.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit de Microsoft 365 vers des destinations prises en charge, vous devez répondre aux exigences suivantes :

- Vous devez souscrire à un plan Microsoft 365 Enterprise. Pour plus d'informations sur la création ou la mise à niveau d'un plan Microsoft 365 Enterprise, consultez la section Plans Microsoft 365 Enterprise sur le Microsoft site Web.
- Vous devez disposer d'un utilisateur avec des autorisations d'administrateur dans votre compte Microsoft 365.
- Vous devez activer la journalisation des audits pour votre organisation. Pour plus d'informations, voir Activer ou désactiver l'audit sur le Microsoft site Web.

Considérations relatives aux limites de taux

Microsoft365 impose des limites de débit à l'API Microsoft 365. Pour plus d'informations sur les limites de débit des API Microsoft 365, consultez la section Limites de limitation spécifiques au service Microsoft Graph dans la documentation Microsoft Graph sur le site Web. Microsoft Si la combinaison de vos applications AppFabric d'API Microsoft 365 existantes dépasse la limite, l'affichage des journaux d'audit AppFabric risque d'être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application

ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre compte Microsoft 365

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez l'autoriser AppFabric auprès de Microsoft 365. Pour trouver les informations requises pour autoriser Microsoft 365 avec AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à Microsoft 365 en utilisant OAuth. Pour créer une application OAuth dans Microsoft 365, procédez comme suit :

1. Suivez les instructions de la section Enregistrer une application du Guide du développeur Azure Active Directory sur le Microsoft site Web.

   Choisissez Comptes dans ce répertoire organisationnel uniquement dans la configuration des types de comptes pris en charge.
2. Suivez les instructions de la section Ajouter un URI de redirection du Guide du développeur Azure Active Directory.

   Choisissez la plateforme Web.

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

   Dans cette URL se *<region>* trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

   Vous pouvez ignorer les autres champs de saisie de la plateforme Web.
3. Suivez les instructions de la section Ajouter un secret client du Guide du développeur Azure Active Directory.

Autorisations nécessaires

Vous devez ajouter les autorisations suivantes à votre application OAuth. Pour ajouter des autorisations, suivez les instructions de la section Ajouter des autorisations pour accéder à votre API Web du Guide du développeur Azure Active Directory.

- `Microsoft Graph API>` `User.Read` (ajouté automatiquement)
- `Office 365 Management APIs>` `ActivityFeed.Read` (Sélectionnez le type délégué)
- `Office 365 Management APIs>` `ActivityFeed.ReadDlp` (Sélectionnez le type délégué)
- `Office 365 Management APIs>` `ServiceHealth.Read` (Sélectionnez le type délégué)

Après avoir ajouté les autorisations, pour accorder le consentement de l'administrateur à ces autorisations, suivez les instructions de la section relative au bouton de consentement de l'administrateur du guide du développeur Azure Active Directory.

Autorisations relatives aux applications

AppFabric prend en charge la réception d'informations utilisateur et de journaux d'audit à partir de votre compte Microsoft 365. Pour recevoir à la fois les journaux d'audit et les données utilisateur de Microsoft 365, vous devez créer deux autorisations d'application, l'une nommée Microsoft365 dans la liste déroulante des autorisations d'applications et l'autre nommée Microsoft365 Audit Log dans la liste déroulante des autorisations d'applications. Vous pouvez utiliser le même identifiant de locataire, le même identifiant client et le même secret client pour les deux autorisations d'application. Pour recevoir les journaux d'audit de Microsoft 365, vous avez besoin des autorisations des applications MicrosoftMicrosoft365 et 365 Audit Log. Pour utiliser uniquement l'outil d'accès utilisateur, seule l'autorisation de l'application Microsoft365 est requise.

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'ID de locataire dans AppFabric est votre identifiant de locataire Azure Active Directory. Pour trouver votre identifiant de client Azure Active Directory, consultez Comment trouver votre identifiant de client Azure Active Directory dans la documentation du produit Azure sur le Microsoft site Web.

Nom du locataire

Entrez un nom qui identifie ce compte Microsoft 365 unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric vous demandera votre numéro de client. L'ID client entré AppFabric est l'ID de l'application Microsoft 365 (client). Pour trouver votre identifiant d'application (client) Microsoft 365, procédez comme suit :

1. Ouvrez la page de présentation de l'application OAuth que vous utilisez. AppFabric
2. L'ID de l'application (client) apparaît sous Essentials.
3. Entrez l'identifiant de l'application (client) de votre client OAuth dans le champ ID client de. AppFabric

Secret client

AppFabric vous demandera le secret de votre client. Microsoft365 fournit cette valeur uniquement lorsque vous créez initialement le secret client pour votre application OAuth. Pour générer un nouveau secret client si vous n'en avez pas, procédez comme suit :

1. Pour créer un secret client, suivez les instructions de la section Ajouter un secret client du Guide du développeur Azure Active Directory.
2. Entrez le contenu du champ Valeur dans le champ Secret du client dans AppFabric.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle de Microsoft 365 pour approuver l'autorisation. Pour approuver l' AppFabric autorisation, choisissez Autoriser.

Miro

Miroest un espace de travail en ligne dédié à l'innovation qui permet aux équipes distribuées de toutes tailles de créer la prochaine grande innovation. Le canevas infini de la plateforme permet aux équipes d'animer des ateliers et des réunions captivants, de concevoir des produits, de réfléchir à des idées, etc. Miro, dont le siège social est situé à San Francisco et à Amsterdam, dessert plus de 50 millions d'utilisateurs dans le monde, dont 99 % des entreprises du Fortune 100. Miroa été fondée en 2011 et compte actuellement plus de 1 500 employés répartis dans 12 hubs à travers le monde. Pour en savoir plus, rendez-vous sur Miro.

Miroinclut une suite complète de fonctionnalités collaboratives conçues pour l'innovation, notamment la création de diagrammes, le wireframing, la visualisation des données en temps réel, l'animation

d'ateliers et le support intégré pour les pratiques agiles, les ateliers et les présentations interactives. Miroa récemment annoncé une Miro intelligence artificielle qui étend ses capacités, avec Miro la cartographie et la création de diagrammes pilotés par l'IA, le clustering et la synthèse, ainsi que la génération de contenu. Miropermet aux entreprises de réduire le nombre d'outils autonomes, réduisant ainsi la fragmentation des informations et les coûts.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurMiro, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

AppFabric support pour Miro

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deMiro.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Miro des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez disposer d'un plan Miro d'entreprise. Pour plus d'informations sur les types de forfaits Miro, consultez la page de Mirotarification du site Miro Web.
- Vous devez avoir un utilisateur ayant le rôle d'administrateur de l'entreprise sur votre Miro compte. Pour plus d'informations sur les rôles, consultez la section Rôles au niveau de l'entreprise sur le site Web du centre d'aide Miro.
- Vous devez disposer d'une équipe de développeurs d'entreprise dans votre Miro compte. Pour plus d'informations sur la création d'équipes de développeurs, consultez la section Équipes de développeurs d'entreprise sur le site Web du centre d'aide Miro.

Considérations relatives aux limites de taux

Miroimpose des limites de débit à l'MiroAPI. Pour plus d'informations sur les limites de débit des Miro API, consultez la section Limitation de débit dans le guide du Miro développeur sur le Miro site Web.

Si la combinaison AppFabric de vos applications Miro API existantes dépasse la limite, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Un délai de 30 minutes peut s'écouler avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Miro compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecMiro. Pour trouver les informations requises pour Miro l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Miroutilisation d'OAuth. Pour créer une application OAuth dansMiro, procédez comme suit :

1. Pour créer une application OAuth, suivez les instructions de la section Création et installation d'applications de l'article relatif aux équipes de développeurs d'entreprise sur le site Web du centre d'aide Miro.
2. Dans la boîte de dialogue de création de l'application, cochez la case Expirer le jeton d'autorisation utilisateur après avoir sélectionné une équipe de développeurs au sein de l'organisation de l'entreprise.

   > **Note**
   >
   > Vous devez le faire avant de créer l'application, car vous ne pouvez pas modifier cette option une fois l'application créée.

3. Sur la page de l'application, entrez une URL au format suivant dans la section URI de redirection pour OAuth 2.0.

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

   Dans cette URL se <region>trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie

du Nord) estus-east-1. Pour cette région, l'URL de redirection esthttps://*us-east-1*.console.aws.amazon.com/appfabric/oauth2.

4. Copiez et enregistrez votre identifiant client et votre secret client pour les utiliser dans l'autorisation de AppFabric l'application.

Étendue requise

Vous devez ajouter les étendues suivantes dans la Permissions section de la page de votre application Miro OAuth :

- auditlogs:read
- organizations:read

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'identifiant du locataire indiqué AppFabric est votre identifiant d'Miroéquipe. Pour savoir comment trouver votre identifiant Miro Team, consultez la section Questions fréquemment posées de Je suis un nouvel Miro administrateur. Par où commencer ? sur le site Web du centre d'Miroaide.

Nom du locataire

Entrez un nom qui identifie cette Miro organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric vous demandera votre numéro de client. Pour trouver votre identifiant client, procédez comme suit :

1. Accédez aux paramètres Miro de votre profil.
2. Sélectionnez l'onglet Vos applications.
3. Sélectionnez l'application que vous utilisez pour vous connecter AppFabric.
4. Entrez l'ID client dans la section Informations d'identification de l'application dans le champ ID client de AppFabric.

Secret client

AppFabric vous demandera le secret de votre client. Pour trouver le secret de votre client, procédez comme suit :

1. Accédez aux paramètres Miro de votre profil.
2. Sélectionnez l'onglet Vos applications.
3. Sélectionnez l'application que vous utilisez pour vous connecter AppFabric.
4. Entrez le secret du client dans la section Informations d'identification de l'application dans le champ Secret du client dans AppFabric.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous Miro demandant d'approuver l'autorisation. Pour approuver l' AppFabric autorisation, choisissez Autoriser.

Okta

Oktaest la World's Identity Company. En tant que principal partenaire indépendant en matière d'identité, chacun Okta peut utiliser n'importe quelle technologie en toute sécurité, n'importe où, sur n'importe quel appareil ou application. Les marques les plus fiables font confiance Okta pour garantir un accès, une authentification et une automatisation sécurisés. La flexibilité et la neutralité étant au cœur des clouds Okta Workforce Identity et Customer Identity, les chefs d'entreprise et les développeurs peuvent se concentrer sur l'innovation et accélérer la transformation numérique, grâce à des solutions personnalisables et à plus de 7 000 intégrations prédéfinies. Oktac'est construire un monde où l'identité vous appartient. Pour en savoir plus, rendez-vous sur okta .com.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurOkta, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Okta
- Connexion AppFabric à votre Okta compte

AppFabric support pour Okta

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deOkta.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Okta des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous pouvez l'utiliser AppFabric avec n'importe quel type de Okta plan.
- Vous devez avoir un utilisateur ayant le rôle de super administrateur dans votre Okta compte.
- L'utilisateur qui approuve l'autorisation de l'application AppFabric doit également avoir le rôle de super administrateur dans votre Okta compte.

Considérations relatives aux limites de taux

Oktaimpose des limites de débit à l'OktaAPI. Pour plus d'informations sur les limites de débit des Okta API, consultez la section Limites de débit dans le guide du Okta développeur sur le Okta site Web. Si la combinaison de AppFabric vos applications Okta API existantes dépasse les limites fixées, Okta l'affichage des journaux d'audit AppFabric risque d'être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Okta compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecOkta. Pour trouver les informations requises pour Okta l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Oktautilisation d'OAuth. Pour créer une application OAuth à laquelle vous connecter AppFabric, suivez les instructions de la section Créer des intégrations d'applications OIDC sur le site Web du Okta centre d'aide. Voici les considérations relatives à la configuration pour AppFabric :

1. Pour Type d'application, sélectionnez Application Web.
2. Pour le type de subvention, choisissez le code d'autorisation et le jeton d'actualisation.
3. Utilisez une URL de redirection au format suivant comme URI de redirection de connexion et URI de redirection de déconnexion.

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

   Dans cette URL se <region>trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
4. Vous pouvez ignorer la configuration de Trusted Origins.
5. Accordez l'accès à tous les membres de votre Okta organisation dans la configuration Accès contrôlé.

   > **Note**
   >
   > Si vous ignorez cette étape lors de la création initiale de l'application OAuth, vous pouvez affecter tous les membres de votre organisation en tant que groupe à l'aide de l'onglet Attributions de la page de configuration de l'application.

6. Vous pouvez conserver les valeurs par défaut de toutes les autres options.

Champs d'application requis

Vous devez ajouter les étendues suivantes à votre application Okta OAuth :

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

Autorisations relatives aux applications

ID de locataire

AppFabric demandera un identifiant de locataire. L'ID du locataire AppFabric est celui de votre Okta domaine. Pour plus d'informations sur la recherche de votre Okta domaine, consultez la section Trouver votre Okta domaine dans le guide du Okta développeur disponible sur le Okta site Web.

Nom du locataire

Entrez un nom qui identifie cette Okta organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. Pour trouver votre identifiant client dansOkta, procédez comme suit :

1. Accédez à la console du Okta développeur.
2. Choisissez l'onglet Applications.
3. Choisissez votre application, puis cliquez sur l'onglet Général.
4. Accédez à la section Informations d'identification du client.
5. Entrez l'ID client de votre client OAuth dans le champ ID client de. AppFabric

Secret client

AppFabric demandera un secret client. Pour trouver le secret de votre client dansOkta, procédez comme suit :

1. Accédez à la console du Okta développeur.
2. Choisissez l'onglet Applications.
3. Choisissez votre application, puis cliquez sur l'onglet Général.
4. Accédez à la section Informations d'identification du client.
5. Entrez le secret client de votre application OAuth dans le champ Client Secret de. AppFabric

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous Okta demandant d'approuver l'autorisation. Pour approuver l' AppFabric autorisation, choisissez Autoriser. L'utilisateur qui approuve l'Oktaautorisation doit disposer de l'autorisation de super administrateur. Okta

OneLogin by One Identity

OneLogin by One Identityest une solution moderne de gestion des accès basée sur le cloud qui gère de manière fluide toutes les identités numériques de votre personnel, de vos clients et de vos partenaires. OneLoginfournit une authentification unique (SSO) sécurisée, une authentification multifactorielle (MFA), une authentification adaptative, une authentification MFA au niveau du bureau, l'intégration d'annuaires avec AD, LDAP, G Suite et d'autres annuaires externes, la gestion du cycle de vie des identités et bien plus encore. Vous pouvez ainsi protéger votre entreprise contre les attaques les plus courantes, ce qui se traduit par une sécurité accrue, une expérience utilisateur fluide et le respect des exigences réglementaires. AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurOneLogin, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les envoyer dans un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose. OneLogin

Rubriques

AppFabric support pour OneLogin by One Identity

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deOneLogin by One Identity.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis OneLogin by One Identity des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez disposer d'un compte OneLogin Advanced ou Professional.
- Vous devez avoir un utilisateur doté des privilèges d'administrateur/administrateur délégué.

Considérations relatives aux limites de taux

OneLogin by One Identityimpose des limites de débit à l'OneLoginAPI. Pour plus d'informations sur les limites de débit des OneLogin API, consultez la section Obtenir une limite de débit dans la référence des OneLogin API. Si la combinaison de AppFabric vos applications OneLogin API existantes dépasse les limites fixées, OneLogin l'affichage des journaux d'audit AppFabric risque

d'être retardé. Toutefois, le OneLogin taux limite peut être augmenté. Pour obtenir de l'aide, contactez votre responsable de OneLogin by One Identity compte ou contactez One Identity.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre OneLogin by One Identity compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecOneLogin by One Identity. Pour trouver les informations requises pour OneLogin l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'OneLogin by One Identityutilisation d'OAuth. Pour créer une application OAuth dansOneLogin, procédez comme suit :

1. Accédez à la page de OneLogin connexion et connectez-vous.
2. Dans le menu Développeurs, choisissez API Credentials.
3. Choisissez Nouvelles informations d'identification, entrez un nom pour vos nouvelles informations d'identification, puis choisissez Lire tout.
4. Choisissez Enregistrer. OneLogincrée un identifiant client et un secret client.

Étendue requise

Vous devez ajouter les étendues suivantes à votre application OneLogin by One Identity OAuth :

- Lisez tout. Pour plus d'informations sur les étendues et les informations d'identification du client, consultez la section Utilisation des informations d'identification d'API dans la référence des OneLogin API.

Autorisations relatives aux applications

ID de locataire

AppFabric demandera un identifiant de locataire. L'ID du locataire AppFabric est le sous-domaine de votre instance. Vous trouverez votre identifiant de locataire dans la barre d'adresse de votre navigateur. Par exemple, l'ID du locataire `subdomain` se trouve-t-il dans l'URL suivante`https://subdomain.onelogin.com`.

Nom du locataire

Entrez un nom qui identifie cette OneLogin by One Identity organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. Pour trouver votre identifiant client dansOneLogin by One Identity, procédez comme suit :

1. Accédez à la page de OneLogin connexion et connectez-vous.
2. Dans le menu Développeurs, choisissez API Credentials.
3. Choisissez les informations d'identification de l'API pour obtenir l'ID client.

Secret client

AppFabric demandera un secret client. Pour trouver le secret de votre client dansOneLogin by One Identity, procédez comme suit :

1. Accédez à la page de OneLogin connexion et connectez-vous.
2. Dans le menu Développeurs, choisissez API Credentials.
3. Choisissez les informations d'identification de l'API pour obtenir le secret du client.

Autorisation de l'application cliente

Dans AppFabric, créez une autorisation d'application à l'aide de votre identifiant et de votre nom de locataire, ainsi que de votre identifiant et de votre nom de client. Choisissez Connect pour activer l'autorisation.

PagerDuty

PagerDutyest une plateforme de gestion des opérations numériques qui aide les équipes à atténuer les problèmes ayant un impact sur les clients en transformant chaque signal en action afin que vous puissiez résoudre les problèmes plus rapidement et fonctionner plus efficacement. S'intègre CloudWatch àGuardDuty,CloudTrail, etPersonal Health Dashboard. AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurPagerDuty, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour PagerDuty
- Connexion AppFabric à votre PagerDuty compte

AppFabric support pour PagerDuty

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir dePagerDuty.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis PagerDuty des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Pour accéder aux journaux d'audit, vous devez disposer d'un plan d'opérations PagerDuty commerciales ou numériques.
- Vous devez être un administrateur global ou le propriétaire du PagerDuty compte.

Considérations relatives aux limites de taux

PagerDutyimpose des limites de débit à l'PagerDutyAPI. Pour plus d'informations sur les limites de débit des PagerDuty API, consultez la section Limites de débit des API REST sur la plateforme pour PagerDuty développeurs. Si la combinaison de AppFabric vos applications PagerDuty API existantes dépasse les limites fixées, PagerDuty l'affichage des journaux d'audit AppFabric risque d'être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application

ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre PagerDuty compte

La PagerDuty plateforme prend en charge les clés d'accès aux API. Pour générer une clé d'accès à l'API, procédez comme suit.

Création d'une clé d'accès à l'API

AppFabric s'intègre à PagerDuty l'utilisation d'une clé d'accès API pour les clients publics. Pour créer une clé d'accès à l'API dansPagerDuty, procédez comme suit :

1. Accédez à la page de PagerDuty connexion et connectez-vous.
2. Choisissez Intégrations, clés d'accès aux API.
3. Choisissez Créer une nouvelle clé d'API.
4. Entrez une description, puis sélectionnez Clé d'API en lecture seule.
5. Choisissez Create key (Créer une clé).
6. Copiez et enregistrez la clé d'API. Vous en aurez besoin plus tard AppFabric. Si vous fermez la page avant d'enregistrer la clé d'API, vous devez générer une nouvelle clé d'API et l'enregistrer. Cette clé doit être dédiée afin d' AppFabric éviter de partager la limite de débit de l'PagerDutyAPI avec vos autres intégrations.

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'ID de locataire de votre PagerDuty compte est l'URL de base de votre compte. Vous pouvez le trouver en vous connectant PagerDuty et en copiant depuis la barre d'adresse de votre navigateur Web. L'ID du locataire doit suivre l'un des formats suivants :

- Pour les comptes américains, `subdomain.pagerduty.com`
- Pour les comptes de l'UE, `subdomain.eu.pagerduty.com`

Nom du locataire

Entrez un nom qui identifie cette PagerDuty organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

Jeton de compte de service

AppFabric demandera votre jeton de compte de service. Le jeton de compte de service intégré AppFabric est la clé d'accès à l'API que vous avez créée dansCréation d'une clé d'accès à l'API.

Ping Identity

ChezPing Identity, nous croyons qu'il est important de rendre les expériences numériques à la fois sécurisées et fluides pour tous les utilisateurs, sans compromis. C'est pourquoi plus de la moitié des entreprises du Fortune 100 choisissent Ping Identity de protéger les interactions numériques de leurs utilisateurs tout en simplifiant les expériences. Le 23 août 2023, Ping Identity et nous nous sommes ForgeRock associés pour offrir un plus grand choix, une expertise plus approfondie et une solution d'identité plus complète aux clients et aux partenaires. AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurPing Identity, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Ping Identity
- Connexion AppFabric à votre Ping Identity compte

AppFabric support pour Ping Identity

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir dePing Identity.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Ping Identity des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez disposer d'un Ping Identity compte Essential, Plus ou Premium. Pour plus d'informations sur la création ou la mise à niveau vers le type de Ping Identity plan applicable, consultez la Ping Identitytarification de toutes les fonctionnalités du Ping Identity site Web.

- Vous devez avoir le rôle de lecture seule des données d'identité dans votre Ping Identity compte. Vous pouvez ajouter des rôles à votre compte en attribuant des rôles à votre application. Pour plus d'informations sur les rôles, consultez la section Rôles sur le site Web de Ping Identity Support.

Considérations relatives aux limites de taux

Ping Identityne publie pas de limites de taux. Vous devez créer un dossier d'assistance ou contacter votre équipe Ping Identity Customer Success. Si la combinaison de AppFabric vos applications Ping Identity API existantes dépasse les limites fixées, Ping Identity l'affichage des journaux d'audit AppFabric risque d'être retardé.

Considérations relatives au retard des données

Un délai de 30 minutes peut s'écouler avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Ping Identity compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecPing Identity. Pour trouver les informations requises pour Ping Identity l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Ping Identityutilisation d'OAuth. Pour créer une application OAuth dansPing Identity, procédez comme suit :

1. Suivez les instructions de la section Créer une connexion à une application du guide PingOnedestiné aux développeurs sur le Ping Identity site Web.
2. Après avoir créé l'application, personnalisez les types de subventions.
    a. Lorsque vous êtes connecté à l'application, choisissez l'onglet Configuration et cliquez sur l'icône en forme de crayon pour apporter des modifications à la configuration existante.
    b. Sous Type de subvention, sélectionnez Code d'autorisation. Conservez l'application de la PKCE comme FACULTATIVE.
    c. Sélectionnez Refresh Token et choisissez vos durées d'actualisation.
3. Utilisez une URL de redirection au format suivant dans URL de redirection/URL de rappel.

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

Dans cette URL se <region>trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) estus-east-1. Pour cette région, l'URL de redirection esthttps://*us-east-1*.console.aws.amazon.com/appfabric/oauth2.

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'ID du locataire AppFabric est le nom de votre Ping Identity instance. Vous trouverez votre identifiant de locataire dans la barre d'adresse de votre navigateur. Par exemple, *API_PATH*/v1/environments/*environmentID*. Where *API_PATH* représente le domaine régional du PingOne serveur, par exempleapi.pingone.com, et *environmentID* représente votre ID d'environnement indiqué dans les propriétés de l'environnement de votre application. Pour plus d'informations sur les propriétés de l'environnement, consultez la section Propriétés de l'environnement sur le Ping Identity site Web.

Nom du locataire

Entrez un nom qui identifie cette Ping Identity organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. Pour trouver votre identifiant clientPing Identity, procédez comme suit :

1. Connectez-vous à la PingOne console d'administration et choisissez Applications.
2. Choisissez l'application dans la liste.
3. Choisissez l'onglet Vue d'ensemble, puis recherchez la valeur de l'ID client.

Secret client

AppFabric demandera un secret client. Pour trouver le secret de votre client dansPing Identity, procédez comme suit :

1. Connectez-vous à la PingOne console d'administration et choisissez Applications.
2. Choisissez l'application dans la liste.
3. Choisissez l'onglet Vue d'ensemble, puis recherchez la valeur du secret client.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous Ping Identity demandant d'approuver l'autorisation. Pour approuver l' AppFabric autorisation, choisissez Autoriser.

Salesforce

Salesforcefabrique des logiciels basés sur le cloud conçus pour aider les entreprises à trouver plus de prospects, à conclure plus de ventes et à impressionner les clients avec un service exceptionnel. Salesforce's Customer 360 propose une suite complète de produits, réunit les équipes des ventes, du service, du marketing, du commerce et de l'informatique autour d'une vision unique et partagée des informations clients, aidant ainsi les entreprises à développer leurs relations avec les clients comme avec les employés. Vous pouvez l'utiliser AWS AppFabric pour recevoir des journaux d'audit et des données utilisateurSalesforce, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les envoyer vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Salesforce
- Connexion AppFabric à votre Salesforce compte

AppFabric support pour Salesforce

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deSalesforce.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Salesforce des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez disposer d'une édition Performance, Enterprise ou Unlimited deSalesforce. Contactez-nous Salesforce pour passer à l'une de ces éditions.

- Si vous souhaitez AppFabric transférer des fichiers journaux d'événements horaires contenant l'ensemble complet des événements depuisSalesforce, vous devez vous abonner à Event Monitoring dans le cadre des fonctionnalités Shield deSalesforce. Sinon, AppFabric les événements limités (connexion, déconnexion, utilisation totale de l'API InsecureExternalAssets, violation CORS et événements HostnameRedirects ELF) seront transférés du fichier journal quotidien Salesforce's standard. Vous pouvez vérifier si votre Salesforce compte est déjà abonné à Shield Features en accédant à Configuration > Gestionnaire d'événements. Si 19 événements ou plus sont répertoriés, votre compte est abonné à la surveillance des événements. Si vous ne disposez pas de Event Monitoring, vous pouvez acheter un abonnement à ce module complémentaire en contactantSalesforce.
- Vous devez activer la génération du journal des événements dans les Salesforce paramètres.
- Vous devez utiliser le profil d'administrateur système pour créer une application OAuth et vous connecter avec les mêmes informations d'identification pour. AppFabric

> **Note**
>
> L'utilisation totale de l'API, l'enregistrement des violations CORS, les redirections de noms d'hôte, les actifs externes non sécurisés, les événements de connexion et de déconnexion sont disponibles sans frais supplémentaires dans les éditions prises en charge de. Salesforce Contactez-nous Salesforce pour acheter les autres types d'événements. Pour plus d'informations sur les types Salesforce d'événements, consultez la section Types d'événements EventLogFile pris en charge sur le Salesforce site Web.
> AppFabric peut prendre en charge jusqu'à 100 000 événements par type d'événement et par instance de fichier journal (tous les jours ou toutes les heures, selon l'abonnement au module complémentaire de surveillance des événements). Un fichier journal dépassant le seuil peut entraîner l'exclusion de l'intégralité du fichier journal de l'ingestion.

Considérations relatives aux limites de taux

Salesforceimpose des limites de débit à l'SalesforceAPI. Pour plus d'informations sur les limites de débit des Salesforce API, consultez la section Limites et allocations des demandes d'API sur le Salesforce site Web. Si la combinaison de AppFabric vos applications Salesforce API existantes dépasse les Salesforce's limites, l'affichage des journaux d'audit AppFabric risque d'être retardé.

Considérations relatives au retard des données

Vous pouvez constater un retard allant jusqu'à 6 heures sur le fichier journal quotidien ou jusqu'à 29 heures sur le fichier journal horaire pour qu'un événement d'audit soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Salesforce compte

Après avoir créé votre bundle d'applications dans le AppFabric service, vous devez autoriser AppFabric avecSalesforce. Pour trouver les informations requises pour Salesforce l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'SalesforceOAuth utilisateur. Pour créer une application OAuth dansSalesforce, procédez comme suit :

1. Connectez-vous à votre Salesforce compte.
2. Accédez à la page de configuration comme décrit dans la Salesforcedocumentation.
3. Recherchez App Manager dans la recherche rapide.
4. Choisissez Nouvelle application connectée.
5. Entrez les informations requises dans les champs du formulaire.
6. Choisissez Activer les paramètres OAuth.
7. Assurez-vous de désactiver les options suivantes :
   - Exiger une clé de preuve pour l'extension d'échange de code (PKCE) pour les flux d'autorisation pris en charge
   - Exiger un secret pour le flux du serveur Web
   - Exiger un secret pour Refresh Token Flow
8. Entrez une URL au format suivant dans la zone de texte URL de rappel, puis choisissez Enregistrer les modifications.

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

   Dans cette URL se <region>trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie

du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

9. Renseignez les champs selon vos besoins (décrits dans la Champs d'application requis section suivante). Tous les autres champs peuvent conserver leurs valeurs par défaut.
10. Choisissez Enregistrer.
11. Procédez comme suit pour vérifier la politique de jeton d'actualisation pour la nouvelle application OAuth :

    a. Sur la page Configuration, saisissez Applications connectées dans la zone de texte Recherche rapide, puis choisissez Gérer les applications connectées.

    b. Choisissez Modifier à côté de l'application que vous venez de créer.

    c. Assurez-vous que le jeton d'actualisation est valide jusqu'à ce que l'option de révocation soit sélectionnée.

    d. Enregistrez vos modifications.
12. Procédez comme suit pour vérifier que les journaux d'audit sont générés :

    a. Sur la page Configuration, entrez le fichier journal des événements dans la zone de texte Recherche rapide, puis choisissez Navigateur de fichiers journaux d'événements.

    b. Vérifiez que les journaux d'événements sont répertoriés dans le navigateur de fichiers journaux d'événements.
13. Accédez à l'application créée, puis choisissez Afficher dans le menu déroulant.
14. Choisissez Gérer les informations du consommateur.

    Vous serez redirigé vers un nouvel onglet où vous devrez vérifier votre identité. Dans cet onglet, notez les valeurs Consumer Key et Consumer Secret. Vous en aurez besoin ultérieurement pour vous connecter.

Champs d'application requis

Vous devez ajouter les étendues suivantes à votre application Salesforce OAuth :

- Gérez les données utilisateur via des API (`API`).
- Exécutez la demande à tout moment (`refresh_tokenetoffline_access`).

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'ID du locataire AppFabric est le sous-domaine de votre Salesforce My Domain. Vous trouverez votre sous-domaine Mon domaine dans la barre d'adresse de votre navigateur entre `https://` et `.my.salesforce.com`.

Pour trouver votre Salesforce My Domain, suivez les instructions ci-dessous depuis l'écran d'Salesforceaccueil.

1. Accédez à la page de configuration comme décrit dans la Salesforcedocumentation.
2. Recherchez les paramètres de l'entreprise dans la recherche rapide, puis choisissez Mon domaine dans les résultats.

Nom du locataire

Entrez un nom qui identifie cette Salesforce organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. Pour trouver votre identifiant client dansSalesforce, procédez comme suit :

1. Accédez à la page de configuration.
2. Choisissez Configuration, puis App Manager.
3. Choisissez l'application créée, puis sélectionnez Afficher dans le menu déroulant.
4. Choisissez Gérer les informations du consommateur. Vous allez être redirigé vers un nouvel onglet.
5. Vérifiez votre identité, puis recherchez la valeur de la clé du consommateur.
6. Entrez la clé du consommateur dans le champ d'identification du client AppFabric.

Secret client

AppFabric vous demandera le secret de votre client. Le secret du client dans AppFabric est le secret du consommateur dansSalesforce. Pour trouver votre secretSalesforce, procédez comme suit :

1. Accédez à la page de configuration.
2. Choisissez Configuration, puis App Manager.
3. Choisissez l'application créée, puis sélectionnez Afficher dans le menu déroulant.
4. Choisissez Gérer les informations du consommateur. Vous allez être redirigé vers un nouvel onglet.
5. Vérifiez votre identité, puis recherchez la valeur du secret du consommateur.
6. Entrez le secret du consommateur dans le champ secret du client AppFabric.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous Salesforce demandant d'approuver l'autorisation. Sur la page d'approbation, assurez-vous d'utiliser le rôle d'administrateur Salesforce système ou un Salesforce utilisateur disposant des autorisations utilisateur View Event Log Files et API Enabled lors de l'autorisation. Choisissez Autoriser pour approuver l' AppFabricautorisation.

ServiceNow

ServiceNowest l'un des principaux fournisseurs de services basés sur le cloud qui automatisent les opérations informatiques des entreprises. ServiceNow, l'ITOM offre aux entreprises une visibilité et un contrôle complets de l'ensemble de leur environnement informatique, y compris l'infrastructure virtualisée et cloud. Il simplifie la cartographie, la fourniture et l'assurance des services, en consolidant les données relatives aux services informatiques et à l'infrastructure dans un seul système d'enregistrement. Il automatise et rationalise également les processus clés, notamment la gestion des événements, des incidents, des problèmes, de la configuration et des modifications. AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurServiceNow, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour ServiceNow
- Considérations relatives au retard des données
- Connexion AppFabric à votre ServiceNow compte

AppFabric support pour ServiceNow

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deServiceNow.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis ServiceNow des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous pouvez l'utiliser AppFabric avec n'importe quel type de ServiceNow plan.
- Vous devez avoir un utilisateur ayant le rôle d'administrateur dans votre ServiceNow compte.
- Vous devez avoir une ServiceNow instance.

Considérations relatives aux limites de taux

ServiceNowimpose des limites de débit à l'ServiceNowAPI. Pour plus d'informations sur les limites de débit des ServiceNow API, consultez la section Limitation du débit des API REST entrantes sur le ServiceNow site Web. Si la combinaison AppFabric de vos applications ServiceNow API existantes dépasse les limites, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Un délai de 30 minutes peut s'écouler avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre ServiceNow compte

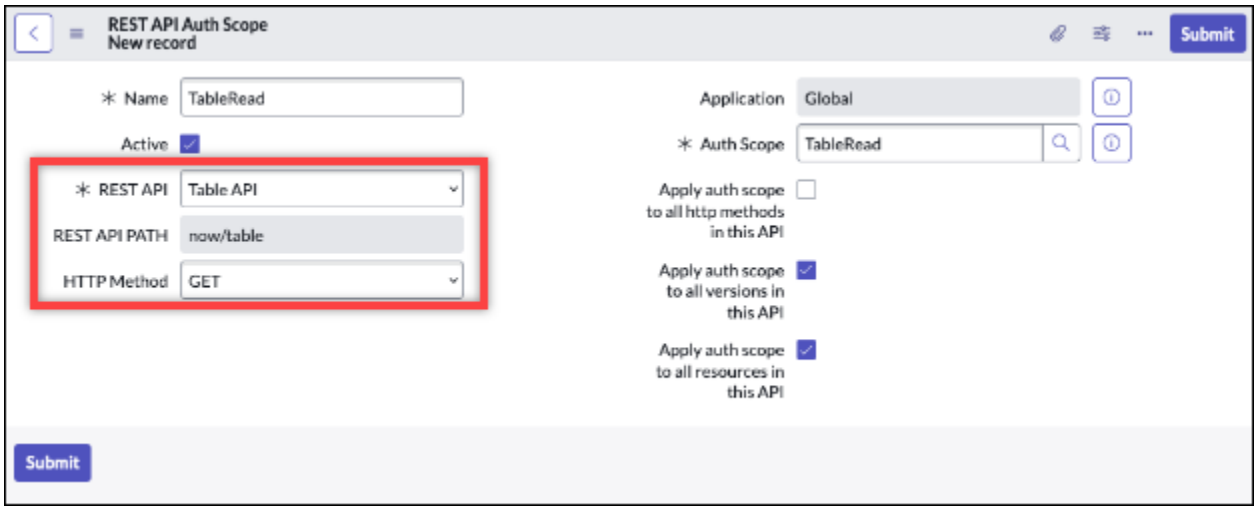
Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecServiceNow. Suivez les étapes ci-dessous pour trouver les informations requises pour autoriser ServiceNow auprès de AppFabric.

Création d'une application OAuth

Il Now Platform prend en charge le type OAuth 2.0 - Autorisation Grant permettant aux clients publics de générer un jeton d'accès.

1. Enregistrez votre application OAuth. Cela nécessite les trois étapes suivantes. Pour plus d'informations sur la réalisation de ces étapes, consultez la section Enregistrez votre candidature ServiceNow sur le ServiceNowsite Web.

   a. Enregistrez l'application et assurez-vous que l'Auth Scope a accès à l'API Table, avec un PATH d'API REST de now/table et une méthode HTTP de GET, comme indiqué dans l'exemple suivant.



   b. Générez un code d'autorisation.

   c. Générez un jeton porteur à l'aide du code d'autorisation.

2. Utilisez une URL de redirection au format suivant.

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

   Dans cette URL se <region>trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) estus-east-1. Pour cette région, l'URL de redirection esthttps://*us-east-1*.console.aws.amazon.com/appfabric/oauth2.

Autorisations relatives aux applications

ID de locataire

AppFabric demandera un identifiant de locataire. L'ID du locataire AppFabric est le nom de votre instance. Vous trouverez votre identifiant de locataire dans la barre d'adresse de votre navigateur. Par exemple, l'ID du locataire *example* se trouve-t-il dans l'URL suivantehttps://*example*.service-now.com.

Nom du locataire

Entrez un nom qui identifie cette ServiceNow organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. Suivez les étapes ci-dessous pour trouver votre identifiant client dansServiceNow.

1. Accédez à la console ServiceNow.
2. Choisissez System OAuth, puis sélectionnez l'onglet Registre des applications.
3. Choisissez votre application.
4. Entrez l'ID client de votre client OAuth dans le champ ID client de. AppFabric

Secret client

AppFabric demandera un secret client. Suivez les étapes ci-dessous pour trouver le secret de votre client dansServiceNow.

1. Accédez à la console ServiceNow.
2. Choisissez System OAuth, puis sélectionnez l'onglet Registre des applications.
3. Choisissez votre application.
4. Entrez le secret client de votre application OAuth dans le champ Client Secret de. AppFabric

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous ServiceNow demandant d'approuver l'autorisation. Choisissez Autoriser pour approuver l' AppFabric autorisation.

Singularity Cloud

La Singularity Cloud plateforme protège votre entreprise contre les menaces de toutes catégories, à tous les stades. Son intelligence artificielle brevetée étend la sécurité des signatures et modèles connus aux attaques les plus sophistiquées, telles que le zero-day et les ransomwares.

Vous pouvez l'utiliser AWS AppFabric pour recevoir des journaux d'audit et des données utilisateurSingularity Cloud, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les envoyer vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

> **Note**
>
> Singularity Cloudla documentation n'est accessible qu'une fois que vous vous êtes connecté à votre Singularity Cloud compte. Par conséquent, nous ne pouvons pas créer de lien direct vers la Singularity Cloud documentation à partir de ce document.

Rubriques

AppFabric support pour Singularity Cloud

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deSingularity Cloud.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Singularity Cloud des destinations prises en charge, vous devez avoir un rôle d'administrateur dans votre Singularity Cloud compte. Pour plus d'informations sur les limites de débit des Singularity Cloud API, connectez-vous à votre compte Singularity Cloud, parcourez la section de documentation et recherchez des rôles.

Considérations relatives aux limites de taux

Singularity Cloudimpose des limites de débit à l'Singularity CloudAPI. Pour plus d'informations sur les limites de débit des Singularity Cloud API, connectez-vous à votre compte Singularity Cloud, parcourez la section de documentation et recherchez les limites de débit des API.

Considérations relatives au retard des données

La livraison d'un événement d'audit à destination peut prendre jusqu'à 30 minutes de retard. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions

prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Singularity Cloud compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecSingularity Cloud. Pour trouver les informations requises pour Singularity Cloud l'autorisation AppFabric, procédez comme suit.

Créez un jeton d'API pour Singularity Cloud

Procédez comme suit pour créer un jeton d'API associé à un utilisateur du service. Le jeton d'API ne sera pas lié à un utilisateur de console ou à une adresse e-mail spécifique.

> **Note**
>
> Créez un nouvel utilisateur ou copiez l'utilisateur du service pour obtenir un nouveau jeton d'API avant ou après l'expiration d'un jeton d'API d'utilisateur du service.

1. Connectez-vous à votre compte Singularity Cloud.
2. Dans la barre d'outils des paramètres, choisissez Utilisateurs, puis sélectionnez Utilisateurs du service.
3. Choisissez Actions, puis sélectionnez Créer un nouvel utilisateur du service.
4. Dans la page Créer un nouvel utilisateur du service, entrez le nom, la description et la date d'expiration de l'utilisateur du service.
5. Choisissez Suivant.
6. Dans la section Sélectionner l'étendue de l'accès, sélectionnez l'étendue.
   - Sélectionnez Compte pour le niveau d'accès.
   - Sélectionnez le compte pour lequel vous souhaitez obtenir les journaux d'audit.
7. Choisissez Créer un utilisateur.

   Le jeton d'API est généré. Une fenêtre s'ouvre et affiche la chaîne du jeton avec un message indiquant que c'est la dernière fois que vous pouvez voir le jeton.
8. (Facultatif) Choisissez Copier le jeton d'API et stockez-le dans un endroit sûr.

9. Choisissez Fermer.

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'identifiant du locataire AppFabric sera le sous-domaine de l'adresse du Sentinel One site Web sur lequel vous vous connectez au service. Par exemple, si vous vous connectez à votre Singularity Cloud compte à cette `example-company-1.sentinelone.net` adresse, votre identifiant de locataire est`example-company-1`.

Nom du locataire

Entrez un nom qui identifie cette Singularity Cloud organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

Jeton de compte de service

Utilisez le jeton que vous avez généré en suivant les étapes décrites dans la Créez un jeton d'API pour Singularity Cloud section de ce guide. Si vous égarez ou ne trouvez pas le jeton, vous pouvez en générer un nouveau en suivant à nouveau les mêmes étapes.

> **Note**
>
> Si un nouveau jeton d'API est généré dans la console Singularity Cloud lors AppFabric de l'ingestion des journaux d'audit, les ingestions s'arrêteront. Dans ce cas, vous devrez mettre à jour l'autorisation de l'application avec un nouveau jeton d'API pour reprendre l'ingestion du journal d'audit.

Slack

Slacka pour mission de rendre la vie professionnelle des gens plus simple, plus agréable et plus productive. Il s'agit de la plateforme de productivité destinée aux entreprises clientes qui améliore les performances en permettant à chacun de bénéficier d'une automatisation sans code, en simplifiant la recherche et le partage des connaissances, et en maintenant les équipes connectées et engagées alors qu'elles progressent ensemble. Dans le cadre deSalesforce, Slack est profondément intégré à Salesforce Customer 360, augmentant ainsi la productivité des équipes de vente, de service et de marketing. Pour en savoir plus et commencer Slack gratuitement, rendez-vous sur slack.com.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurSlack, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Slack
- Connexion AppFabric à votre Slack compte

AppFabric support pour Slack

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deSlack.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Slack des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez avoir un plan Enterprise Grid avecSlack. Pour plus d'informations, consultez la section Présentation d'SlackEnterprise Grid sur le Slack site Web.
- Vous devez avoir un utilisateur ayant le rôle de propriétaire de l'organisation dans votre Slack compte. Pour plus d'informations sur les rôles, consultez la section Types de rôles Slack dans le centre d'Slackaide du site Slack Web.

Considérations relatives aux limites de taux

Slackimpose des limites de débit à l'SlackAPI. Pour plus d'informations sur les limites de débit des Slack API, consultez la section Limites de débit dans le guide d'utilisation des Slack API sur le Slack site Web. Si la combinaison AppFabric de vos applications Slack API existantes dépasse la limite, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Un délai de 30 minutes peut s'écouler avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Slack compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecSlack. Pour trouver les informations requises pour Slack l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Slackutilisation d'OAuth. Il existe deux manières de créer une application OAuth : en utilisant un manifeste d'application ou en partant de zéro. Pour créer une application OAuth dansSlack, procédez comme suit.

Using an app manifest

1. Accédez à l'interface utilisateur de gestion des Slack applications dans votre navigateur.
2. Choisissez Créer une nouvelle application.
3. Choisissez À partir d'un manifeste d'application.
4. Choisissez l'espace de travail pour lequel vous souhaitez autoriser AppFabric.
5. Dans la zone Entrez le manifeste de l'application ci-dessous, choisissez JSON et remplacez le JSON existant par le suivant. Remplacez <region>par le produit approprié Région AWS (par exemple, *us-east-1*).

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

```
        "token_rotation_enabled": true
    }
}
```

6. Copiez et enregistrez l'ID client et le secret du client depuis la page Informations de base.
7. Pour ce `auditLogs:read` faire, vous devez activer la distribution publique de votre application. Pour plus d'informations, consultez Activer la distribution publique sur le site Web de Slack.

From scratch

1. Choisissez À partir de zéro sur l'écran Créer une application.
2. Donnez un nom à votre application et choisissez un espace de travail.
3. Copiez et enregistrez l'ID client et le secret du client depuis la page Informations de base.
4. Sur la page OAuth et autorisations, optez pour l'option Sécurité avancée des jetons via la rotation des jetons.
5. Ajoutez une URL au format suivant dans la section URL de redirection de la page OAuth & Permissions.

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

   Dans cette URL se *<region>* trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
6. Pour ce `auditLogs:read` faire, vous devez activer la distribution publique de votre application. Pour plus d'informations, consultez Activer la distribution publique sur le site Web de Slack.

Étendue requise

> **Note**
>
> Cette section ne s'applique que si vous avez choisi de créer l'application OAuth à partir de zéro. Ignorez cette section si vous avez choisi d'utiliser le manifeste de l'application pour créer une autorisation d'application.

Vous devez ajouter les étendues de jetons utilisateur suivantes sur la page OAuth et autorisations de votre Slack application OAuth :

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

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'identifiant du locataire indiqué AppFabric est l'identifiant de votre Slack espace de travail. Pour obtenir votre identifiant de locataire, suivez les instructions de la section Localiser votre Slack URL dans le centre d'Slackaide du Slack site Web. L'URL Slack de votre espace de travail a un format similaire à `examplecorp.slack.com` ou`examplecorp.enterprise.slack.com`. L'identifiant de locataire dont vous avez besoin est `examplecorp` sans `.slack.com` ou `.enterprise.slack.com`.

Nom du locataire

Entrez un nom identifiant l'identifiant de votre Slack espace de travail. AppFabricutilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application

ID de client

AppFabric demandera l'ID client à votre application Slack OAuth. Pour trouver l'ID client, procédez comme suit :

1. Accédez à l'interface utilisateur de gestion des Slack applications dans votre navigateur.
2. Choisissez l'application OAuth que vous utilisez. AppFabric
3. Entrez l'ID client de la page Informations de base dans le champ ID client de AppFabric.

Secret client

AppFabric demandera le secret du client à votre application Slack OAuth. Pour trouver le secret du client, procédez comme suit :

1. Accédez à l'interface utilisateur de gestion des Slack applications dans votre navigateur.
2. Choisissez l'application OAuth que vous utilisez. AppFabric
3. Entrez le secret du client depuis la page Informations de base dans le champ Secret du client dans AppFabric.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous Slack demandant d'approuver l'autorisation. Pour approuver l' AppFabric autorisation, choisissez Autoriser.

Smartsheet

Smartsheetest une plateforme de gestion du travail qui vous aide à harmoniser le travail, le personnel et la technologie au sein de votre entreprise. Smartsheetpropose un ensemble robuste de fonctionnalités professionnelles permettant à chacun de gérer des projets, d'automatiser les flux de travail et de créer rapidement des solutions à grande échelle, créant ainsi un environnement propice à l'innovation tout en préservant la sécurité et la conformité.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurSmartsheet, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Smartsheet
- Connexion AppFabric à votre Smartsheet compte

AppFabric support pour Smartsheet

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deSmartsheet.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Smartsheet des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez disposer d'un compte Smartsheet Business, Enterprise ou Advance. Pour plus d'informations sur la création ou la mise à niveau de votre Smartsheet compte, consultez la section SmartsheetTarification ou SmartsheetAdvance sur le Smartsheet site Web.
- Vous devez terminer le processus d'enregistrement des Smartsheet développeurs.

Considérations relatives aux limites de taux

Smartsheetimpose des limites de débit à l'SmartsheetAPI. Pour plus d'informations sur les limites de débit des Smartsheet API, consultez la section Limitation de débit dans la référence des API Smartsheet sur le site Web de Smartsheet.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Smartsheet compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecSmartsheet. Pour trouver les informations requises pour Smartsheet l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Smartsheetutilisation d'OAuth. Pour créer une application OAuth dansSmartsheet, procédez comme suit :

1. Accédez aux outils de développement de votre Smartsheet compte.
2. Choisissez Create New App dans l'écran des outils de développement.
3. Complétez tous les champs de saisie sur l'écran Créer une nouvelle application.
4. Utilisez n'importe quelle valeur unique pour l'URL de l'application et le contact/support de l'application.
5. Utilisez une URL de redirection au format suivant comme URL de redirection de l'application.

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

Dans cette URL se *<region>* trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) estus-east-1. Pour cette région, l'URL de redirection esthttps://*us-east-1*.console.aws.amazon.com/appfabric/oauth2.

6. Choisissez Enregistrer.
7. Copiez et enregistrez l'ID client de l'application et le secret de l'application.

Étendue requise

Smartsheetne vous oblige pas à ajouter explicitement des étendues à votre configuration OAuth. AppFabric demandera les champs d'application suivants dans la demande d'autorisation envoyée à votre Smartsheet compte :

- READ_EVENTS
- READ_USERS

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'identifiant du locataire indiqué AppFabric est l'identifiant de votre Smartsheet compte.

Nom du locataire

AppFabric vous demandera votre numéro de locataire. Entrez toute valeur identifiant de manière unique votre Smartsheet compte.

ID de client

AppFabric vous demandera votre numéro de client. L'ID client indiqué AppFabric est l'ID client de votre Smartsheet application. Pour trouver l'ID client de votre application dansSmartsheet, procédez comme suit :

1. Accédez aux outils de développement de votre Smartsheet compte.
2. Sélectionnez l'application OAuth à laquelle vous vous connectez. AppFabric
3. Entrez l'ID client de l'application depuis l'écran Profil de l'application dans le champ ID client de AppFabric.

Secret client

AppFabric vous demandera le secret de votre client. Le secret du client AppFabric est le secret de votre Smartsheet application. Pour trouver le secret de votre application dansSmartsheet, procédez comme suit :

1. Accédez aux outils de développement de votre Smartsheet compte.
2. Sélectionnez l'application OAuth à laquelle vous vous connectez. AppFabric
3. Entrez le secret de l'application depuis l'écran du profil de l'application dans le champ Secret du client dans AppFabric.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous Smartsheet demandant d'approuver l'autorisation. Pour approuver l' AppFabric autorisation, choisissez Autoriser.

Terraform Cloud

HashiCorp Terraform Cloudest le produit de provisionnement multicloud le plus utilisé au monde. L'Terraformécosystème compte plus de 3 000 fournisseurs, 14 000 modules et 250 millions de téléchargements. Terraform Cloudest le moyen le plus rapide à adopterTerraform, fournissant tout ce dont les professionnels, les équipes et les entreprises internationales ont besoin pour créer et collaborer sur une infrastructure et gérer les risques liés à la sécurité, à la conformité et aux contraintes opérationnelles. AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurTerraform Cloud, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Terraform Cloud
- Connexion AppFabric à votre Terraform Cloud compte

AppFabric support pour Terraform Cloud

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deTerraform Cloud.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Terraform Cloud des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Pour accéder aux journaux d'audit, vous devez disposer d'un plan Terraform Cloud Plus Edition et être le propriétaire de l'organisation. Pour plus d'informations sur Terraform Cloud les forfaits, consultez Terraformles tarifs sur le HashiCorp Terraform site Web.
- Les journaux d'audit TBD sont disponibles pour les organisations qui peuvent être créés à partir du Terraform Cloud compte.

Considérations relatives aux limites de taux

Terraform Cloudimpose des limites de débit à l'Terraform CloudAPI. Pour plus d'informations sur les limites de débit d'Terraform CloudAPI, voir Limitation de débit d'API dans les paramètres généraux d'administration des Terraform Cloud développeurs sur le Terraform Cloud site Web. Si la combinaison de AppFabric vos applications Terraform Cloud API existantes dépasse les limites fixées, Terraform Cloud l'affichage des journaux d'audit AppFabric risque d'être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Terraform Cloud compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecTerraform Cloud. Pour trouver les informations requises pour obtenir Terraform Cloud une autorisation AppFabric, procédez comme suit.

Création d'un jeton d'API d'organisation

AppFabric s'intègre à Terraform Cloud l'utilisation d'un jeton d'API d'organisation. Pour plus d'informations sur les jetons d'API d'Terraform Cloudorganisation, consultez la section Jetons d'API d'organisation. Pour créer une organisation, suivez les instructions de la section Creating Organizations. Pour créer un jeton d'API d'organisation dansTerraform Cloud, procédez comme suit.

1. Accédez à la Terraform Cloud page de connexion et connectez-vous.

2. Choisissez Organisation, Paramètres dans le panneau de gauche, puis choisissez les jetons d'API.
3. Sous Jetons d'organisation, choisissez Créer un jeton d'organisation, puis sélectionnez Générer un jeton.
4. (Facultatif) Entrez la date ou l'heure d'expiration du jeton, ou créez un jeton qui n'expire jamais.
5. Copiez et enregistrez le jeton. Vous en aurez besoin plus tard AppFabric. Si vous fermez la page avant d'enregistrer le jeton, vous devez révoquer l'ancien jeton et en créer un nouveau.

Autorisations relatives aux applications

ID de locataire

AppFabric demandera un identifiant de locataire. L'ID de locataire de votre Terraform Cloud compte est l'URL actuelle de l'organisation de votre compte. Vous pouvez le trouver en vous connectant à votre Terraform Cloud organisation et en copiant l'URL actuelle de l'organisation. L'ID du locataire doit suivre l'un des formats suivants :

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

Nom du locataire

Entrez un nom qui identifie cette Terraform Cloud organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

Jeton de compte de service

AppFabric demandera votre jeton de compte de service. Le jeton de compte de service dans AppFabric est le jeton d'API de l'organisation que vous avez créé dansCréation d'un jeton d'API d'organisation.

Webex by Cisco

Ciscoest un leader mondial de la technologie qui alimente Internet. Ciscoouvre de nouvelles perspectives en réinventant vos applications, en sécurisant vos données, en transformant votre infrastructure et en donnant à vos équipes les moyens d'un futur mondial et inclusif.

À propos de Webex by Cisco

Webexest l'un des principaux fournisseurs de solutions de collaboration basées sur le cloud, notamment les visioconférences, les appels, la messagerie, les événements, les solutions d'expérience client telles que les centres d'appels et les appareils de collaboration spécialement conçus. Webex, qui met l'accent sur la fourniture d'expériences de collaboration inclusives, alimente l'innovation, qui tire parti de l'IA et du Machine Learning pour éliminer les obstacles liés à la géographie, à la langue, à la personnalité et à la familiarité avec la technologie. Ses solutions reposent sur la sécurité et la confidentialité dès la conception. Webexfonctionne avec les principales applications professionnelles et de productivité au monde, fournies via une application et une interface uniques. Découvrez-en plus sur webex.com.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurWebex, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

AppFabric support pour Webex

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deWebex.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Webex des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez disposer d'un forfait Collaboration Flex, d'un plan Meet, d'un plan d'appel ou d'une version supérieure. Pour plus d'informations sur la création ou la mise à niveau vers le type de Webex plan applicable, consultez la Webextarification de toutes les fonctionnalités du Webex site Web.
- Votre compte doit disposer de la licence Pro Pack pour accéder aux événements d'audit de sécurité fournis par l'une des AuditLog API Cisco.
- Vous devez avoir un utilisateur doté du rôle Administrateur organisationnel > Administrateur complet.

- L'option Compliance Officer doit être activée dans la configuration des rôles d'administrateur pour votre administrateur complet.

Considérations relatives aux limites de taux

Webeximpose des limites de débit à l'WebexAPI. Pour plus d'informations sur les limites de débit des Webex API, consultez la section Limites de débit dans le guide du Webex développeur sur le Webex site Web. Si la combinaison AppFabric de vos applications Webex API existantes dépasse la limite, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai de 30 minutes s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Webex compte

Après avoir créé votre bundle d'applications au sein du AppFabric service, vous devez autoriser AppFabric avecWebex. Pour trouver les informations requises pour obtenir Webex une autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Webexutilisation d'OAuth. Pour créer une application OAuth dansWebex, procédez comme suit :

1. Suivez les instructions de la section Enregistrement de votre intégration de la page Intégrations et autorisations du Guide du Webex développeur.
2. Utilisez une URL de redirection au format suivant.

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

   Dans cette URL se *<region>* trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2`.

Champs d'application requis

Vous devez ajouter les étendues suivantes à votre application Webex OAuth :

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

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'identifiant du locataire indiqué AppFabric est Webex l'identifiant de votre organisation. Pour plus d'informations sur la façon de trouver Webex l'identifiant de votre organisation, voir Rechercher l'identifiant de votre organisation dans CiscoWebex Control Hub sur le site Web du centre d'Webexaide.

Nom du locataire

Entrez un nom qui identifie cette Webex instance unique. AppFabricutilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric vous demandera votre numéro de Webex client. Pour trouver votre identifiant Webex client, procédez comme suit :

1. Connectez-vous à votre Webex compte à l'adresse https://developer.webex.com.
2. Choisissez votre avatar en haut à droite.
3. Choisissez My Webex Apps.
4. Choisissez l'application OAuth2 que vous utilisez pour. AppFabric
5. Entrez l'ID client sur cette page dans le champ ID client de AppFabric.

Secret client

AppFabric vous demandera le secret de votre Webex client. Webexne présente le secret de votre client qu'une seule fois lors de la création initiale de votre application OAuth. Pour générer un nouveau secret client si vous n'avez pas enregistré le secret client initial, procédez comme suit :

1. Connectez-vous à votre Webex compte à l'adresse https://developer.webex.com.
2. Choisissez votre avatar en haut à droite.
3. Choisissez My Webex Apps.
4. Choisissez l'application OAuth2 que vous utilisez pour. AppFabric
5. Sur cette page, générez un nouveau secret client.
6. Entrez le nouveau secret client dans le champ Secret client de AppFabric.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application, AppFabric vous recevrez une fenêtre contextuelle vous Webex permettant d'approuver l'autorisation. Pour approuver l' AppFabricautorisation, choisissez Accepter.

Zendesk

Zendeskа lancé la révolution de l'expérience client en 2007 en permettant à toutes les entreprises du monde entier de mettre leur service client en ligne. Aujourd'hui, Zendesk elle est la championne d'un service de qualité pour tous, accessible à tous, et alimente des milliards de conversations, reliant plus de 100 000 marques à des centaines de millions de clients par téléphone, chat, e-mail, messagerie, réseaux sociaux, communautés, sites d'avis et centres d'assistance. Zendeskles produits sont conçus avec amour pour être aimés. L'entreprise a été conçue à Copenhague, au Danemark, construite et développée en Californie, et emploie aujourd'hui plus de 6 000 personnes dans le monde entier.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurZendesk, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Zendesk
- Connexion AppFabric à votre Zendesk compte

AppFabric support pour Zendesk

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deZendesk.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Zendesk des destinations prises en charge, vous devez répondre aux exigences suivantes :

- Vous devez disposer d'un compte Zendesk Suite Enterprise ou Enterprise Plus ou d'un compte Zendesk Support Enterprise. Pour plus d'informations sur la création ou la mise à niveau d'un compte Zendesk Enterprise, consultez la section Vérification du type de forfait Zendesk sur le Zendesk site Web.
- Vous devez avoir un utilisateur ayant le rôle d'administrateur dans votre Zendesk compte. Pour plus d'informations sur les rôles, consultez la section Comprendre les rôles des utilisateurs du Zendesk support sur le Zendesk site Web.

Considérations relatives aux limites de taux

Zendeskimpose des limites de débit à l'ZendeskAPI. Pour plus d'informations sur les limites de débit des Zendesk API, consultez la section Limites de débit dans le guide du Zendesk développeur sur le Zendesk site Web. Si la combinaison AppFabric de vos applications Zendesk API existantes dépasse la limite, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Un délai de 30 minutes peut s'écouler avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données. Toutefois, cela peut être personnalisable au niveau du compte. Pour obtenir de l'aide, contactez AWS Support.

Connexion AppFabric à votre Zendesk compte

Après avoir créé votre bundle d'applications dans le AppFabric service, vous devez autoriser AppFabric avecZendesk. Pour trouver les informations requises pour Zendesk l'autorisation AppFabric, procédez comme suit.

Création d'une application OAuth

AppFabric s'intègre à l'Zendeskutilisation d'OAuth. DansZendesk, vous devez créer une application OAuth avec les paramètres suivants :

1. Suivez les instructions de la section Enregistrer votre application auprès de Zendesk de l'article Utiliser l'authentification OAuth avec votre application sur le site Web de SupportZendesk.

2. Utilisez une URL de redirection au format suivant.

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

   Dans cette URL se *<region>* trouve le code Région AWS dans lequel vous avez configuré votre bundle d' AppFabric applications. Par exemple, le code de la région USA Est (Virginie du Nord) est`us-east-1`. Pour cette région, l'URL de redirection est`https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Autorisations d'applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'ID du locataire AppFabric est votre Zendesk sous-domaine. Pour plus d'informations sur la recherche de votre Zendesk sous-domaine, consultez Où puis-je trouver mon Zendesk sous-domaine sur le site Web du Zendesk Support.

Nom du locataire

Entrez un nom qui identifie cette Zendesk organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric demandera un identifiant client. L'ID client dans AppFabric est l'identifiant unique de votre Zendesk API. Pour trouver votre identifiant unique Zendesk, procédez comme suit :

1. Accédez au centre d'administration de votre Zendesk compte.
2. Choisissez Applications et intégrations.
3. Choisissez des API, Zendeskdes API.
4. Choisissez l'onglet Clients OAuth.
5. Choisissez l'application OAuth pour laquelle vous avez créé. AppFabric
6. Entrez l'identifiant unique de votre client OAuth dans le champ ID client de. AppFabric

Secret client

AppFabric demandera un secret client. Le secret du client AppFabric est votre jeton Zendesk secret. Zendeskne présente votre jeton secret qu'une seule fois lorsque vous créez votre application Zendesk OAuth pour la première fois. Pour générer un nouveau jeton secret si vous n'avez pas enregistré le jeton secret initial, procédez comme suit :

1. Accédez au centre d'administration de votre Zendesk compte.
2. Choisissez Applications et intégrations.
3. Choisissez des API, Zendeskdes API.
4. Choisissez l'onglet Clients OAuth.
5. Choisissez l'application OAuth pour laquelle vous avez créé. AppFabric
6. Cliquez sur le bouton Régénérer à côté du champ Jeton secret.
7. Entrez le nouveau jeton secret dans le champ Secret du client dans AppFabric.

Approuver l'autorisation

Après avoir créé l'autorisation de l'application dans AppFabric, vous recevrez une fenêtre contextuelle vous Zendesk demandant d'approuver l'autorisation. Pour approuver l' AppFabric autorisation, choisissez Autoriser.

Zoom

Zoomest une plateforme de collaboration all-in-one intelligente qui rend la connexion plus facile, plus immersive et plus dynamique pour les entreprises et les particuliers. Zoomla technologie place les personnes au centre, en permettant des connexions significatives, en facilitant la collaboration moderne et en stimulant l'innovation humaine grâce à des solutions telles que le chat d'équipe, le téléphone, les réunions, le centre d'appels omnicanal dans le cloud, les enregistrements intelligents, le tableau blanc, etc., le tout dans une seule offre.

AWS AppFabric Pour des raisons de sécurité, vous pouvez recevoir des journaux d'audit et des données utilisateurZoom, normaliser les données au format Open Cybersecurity Schema Framework (OCSF) et les exporter vers un bucket Amazon Simple Storage Service (Amazon S3) ou un flux Amazon Data Firehose.

Rubriques

- AppFabric support pour Zoom

- Connexion AppFabric à votre Zoom compte

AppFabric support pour Zoom

AppFabric prend en charge la réception d'informations sur les utilisateurs et de journaux d'audit à partir deZoom.

Prérequis

Pour pouvoir AppFabric transférer des journaux d'audit depuis Zoom des destinations prises en charge, vous devez satisfaire aux exigences suivantes :

- Vous devez disposer d'un forfait Zoom Pro, Business, Education ou Enterprise.
- Votre rôle Zoom d'administrateur doit être autorisé à créer des applications server-to-server OAuth. Pour plus d'informations sur l'activation des applications server-to-server OAuth, consultez la section Activer les autorisations de la page OAuth de serveur à serveur du guide du développeur sur le Zoom site Web. Zoom
- Votre rôle Zoom d'administrateur doit être autorisé à consulter les journaux d'activité des administrateurs et à vous connecter/déconnecter des activités d'audit. Pour plus d'informations sur l'activation de l'autorisation de consulter les activités d'audit, consultez les sections Utilisation de la gestion des rôles et Utilisation des journaux d'activité des administrateurs sur le site Web de Zoom support.

Considérations relatives aux limites de taux

Zoomimpose des limites de débit à l'ZoomAPI. Pour plus d'informations sur les limites de débit des Zoom API, consultez la section Limites de débit dans le guide du Zoom développeur. Si la combinaison AppFabric de vos Zoom applications existantes dépasse la limite, l'affichage des journaux d'audit AppFabric peut être retardé.

Considérations relatives au retard des données

Il se peut qu'un délai d'environ 24 heures s'écoule avant qu'un événement d'audit ne soit livré à votre destination. Cela est dû au retard dans les événements d'audit mis à disposition par l'application ainsi qu'aux précautions prises pour réduire les pertes de données.

Connexion AppFabric à votre Zoom compte

Après avoir créé votre bundle d'applications dans le AppFabric service, vous devez autoriser AppFabric avecZoom. Pour trouver les informations requises pour Zoom l'autorisation AppFabric, procédez comme suit.

Création d'une application server-to-server OAuth

AppFabric utilise server-to-server OAuth avec les informations d'identification de l'application à intégrer. Zoom Pour créer une application server-to-server OAuth dansZoom, suivez les instructions de la section Créer une application OAuth de serveur à serveur dans le Guide du développeur. Zoom AppFabric ne prend pas en charge les Zoom webhooks, et vous pouvez ignorer la section relative à l'ajout d'abonnements aux webhooks.

Étendue requise

Vous devez ajouter les étendues suivantes à votre application Zoom server-to-server OAuth :

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

Autorisations relatives aux applications

ID de locataire

AppFabric vous demandera votre numéro de locataire. L'identifiant du locataire AppFabric est l'identifiant du Zoom compte. Pour trouver l'identifiant de votre Zoom compte, procédez comme suit :

1. Accédez au Zoom marché.
2. Choisissez Gérer.
3. Choisissez l'application server-to-server OAuth que vous utilisez pour. AppFabric
4. Entrez l'identifiant du compte sur la page Informations d'identification de l'application dans le champ ID du locataire de AppFabric.

Nom du locataire

Entrez un nom qui identifie cette Zoom organisation unique. AppFabric utilise le nom du locataire pour étiqueter les autorisations de l'application et toutes les ingestions créées à partir de l'autorisation de l'application.

ID de client

AppFabric vous demandera votre numéro de client. Pour trouver votre identifiant Zoom client, procédez comme suit :

1. Accédez au Zoom marché.
2. Choisissez Gérer.
3. Choisissez l'application server-to-server OAuth que vous utilisez pour. AppFabric
4. Entrez l'ID client depuis la page Informations d'identification de l'application dans le champ ID client de AppFabric.

Secret client

AppFabric vous demandera le secret de votre client. Pour trouver Zoom le secret de votre client, procédez comme suit :

1. Accédez au Zoom marché.
2. Choisissez Gérer.
3. Choisissez l'application server-to-server OAuth que vous utilisez pour. AppFabric
4. Entrez le secret du client depuis la page Informations d'identification de l'application dans le champ Secret du client dans AppFabric.

Livraison du journal d'audit

Zoommet à disposition les journaux d'audit en accédant à l'API toutes les 24 heures. Lorsque vous consultez les journaux d'audit avec AppFabric, les données que vous voyez concernent les activités de la veille. Zoom

Outils et services de sécurité compatibles

AWS AppFabric for security prend en charge l'intégration avec les outils et services de sécurité suivants. Choisissez le nom d'un service pour plus d'informations sur la configuration de la sécurité AppFabric pour s'y connecter.

Rubriques

- Barracuda XDR
- Dynatrace

- Logz.io
- Netskope
- NetWitness
- Amazon QuickSight
- Rapid7
- Amazon Security Lake
- Singularity Cloud
- Splunk

Barracuda XDR

Barracuda Networksest un partenaire de confiance et un fournisseur de premier plan de solutions de sécurité axées sur le cloud, protégeant le courrier électronique, les réseaux, les données et les applications grâce à des solutions innovantes qui évoluent et s'adaptent au parcours des entreprises. Barracuda XDRest une solution ouverte de détection et de réponse étendue qui associe des technologies sophistiquées à une équipe d'analystes de sécurité au sein de notre centre des opérations de sécurité (SOC). La Barracuda XDR plateforme analyse des milliards d'événements bruts par jour à partir de plus de 40 sources de données intégrées. Associée à de nombreuses règles de détection des menaces correspondant au framework MITRE ATT&CK®, elle peut détecter les menaces plus rapidement et réduire le temps de réponse.

AWS AppFabric considérations relatives à l'ingestion des journaux d'audit

Les sections suivantes décrivent le schéma AppFabric de sortie, les formats de sortie et les destinations de sortie à utiliserBarracuda XDR.

Schéma et format

Barracuda XDRprend en charge le schéma et les formats de AppFabric sortie suivants :

- OCSF - JSON : AppFabric normalise les données à l'aide de l'Open Cybersecurity Schema Framework (OCSF) et les produit au format JSON.

Emplacements de sortie

Barracuda XDRprend en charge la réception des journaux d'audit d'Amazon Security Lake. Pour envoyer des données de AppFabric àBarracuda XDR, suivez les instructions ci-dessous :

1. Envoyer des données vers Amazon Security Lake : configurez AppFabric pour envoyer des données vers Amazon Security Lake via un Amazon Data Firehose. Pour plus d'informations, consultez Amazon Security Lake.
2. Envoyer les données à Barracuda XDR : configurez Barracuda XDR pour recevoir les journaux d'audit d'Amazon Security Lake. Pour plus d'informations, consultez Configuration et utilisation d'Amazon Security Lake.

Dynatrace

Il Dynatrace® Platform combine une observabilité étendue et approfondie et une sécurité continue des applications en temps d'exécution avec des AIOps avancés pour fournir des réponses et une automatisation intelligente à partir des données. Cela permet aux innovateurs de moderniser et d'automatiser les opérations dans le cloud, de fournir des logiciels plus rapidement et de manière plus sécurisée, et de garantir des expériences numériques sans faille.

AWS AppFabric considérations relatives à l'ingestion des journaux d'audit

Les sections suivantes décrivent le schéma AppFabric de sortie, les formats de sortie et les destinations de sortie à utiliser avec leDynatrace Platform.

Schéma et format

Dynatrace PlatformSupporte le schéma et les formats de AppFabric sortie suivants :

- OCSF - JSON : AppFabric normalise les données à l'aide de l'Open Cybersecurity Schema Framework (OCSF) et les produit au format JSON.

Emplacements de sortie

Les Dynatrace Platform supports reçoivent des journaux d'audit à partir des emplacements AppFabric de sortie suivants.

- Amazon Simple Storage Service (Amazon S3)
  - Pour configurer le Dynatrace Platform afin de recevoir des données depuis le compartiment Amazon S3 qui contient vos journaux d'audit, suivez les instructions du projet S3 Log Forwarder de Dynatrace sur. GitHub

Logz.io

Logz.ioaide les entreprises natives du cloud à surveiller et à sécuriser leurs environnements via la plateforme Logz.ioOpen 360, transformant ainsi l'observabilité et la sécurité d'une charge coûteuse à faible valeur ajoutée en un outil rentable et à forte valeur ajoutée pour de meilleurs résultats commerciaux.

Logz.ioLe cloud SIEM répond directement aux principaux défis de sécurité actuels, qu'il s'agisse de la surcharge de données ou du manque omniprésent de compétences informatiques, grâce à des requêtes rapides, à une détection multidimensionnelle et à un contenu de sécurité personnalisable approfondi pour vous aider à surveiller et à étudier l'ensemble de votre environnement cloud, sans dégradation des performances, quels que soient les volumes de données.

La Logz.io solution a été spécialement conçue pour fournir une analyse et une investigation avancées des menaces avec une complexité et un coût réduits. Les clients bénéficient du soutien d'analystes de sécurité dédiés, de contenus liés aux menaces sous forme de service et de fonctionnalités basées sur l'IA, spécialement conçues pour aider à réduire le volume des données et à se concentrer sur les informations qui permettent à votre équipe de hiérarchiser rapidement les menaces du monde réel.

AWS AppFabric considérations relatives à l'ingestion des journaux d'audit

Les sections suivantes décrivent le schéma AppFabric de sortie, les formats de sortie et les destinations de sortie à utiliserLogz.io.

Schéma et format

Logz.ioprend en charge le schéma et les formats de AppFabric sortie suivants :

- Brut - JSON
  - AppFabric affiche les données dans le schéma d'origine utilisé par l'application source au format JSON.
- OCSF - JSON
  - AppFabric normalise les données à l'aide de l'Open Cybersecurity Schema Framework (OCSF) et les produit au format JSON.

Emplacements de sortie

Logz.ioprend en charge les emplacements AppFabric de sortie suivants :

- Amazon Data Firehose
  - Pour configurer votre flux de diffusion Firehose de manière à ce qu'il envoie des donnéesLogz.io, suivez les instructions de la section Choisissez votre Logz.io destination dans le manuel Amazon Data Firehose Developer Guide.
- Amazon Simple Storage Service (Amazon S3)
  - Logz.ioPour configurer la réception de données depuis le compartiment Amazon S3 qui contient vos journaux d'audit, suivez les instructions de la section Configurer un compartiment Amazon S3 sur le Logz.io site Web.

Netskope

Netskope, un leader mondial de la cybersécurité, redéfinit la sécurité du cloud, des données et des réseaux afin d'aider les entreprises à appliquer les principes du zéro confiance pour protéger les données. Rapide et facile à utiliser, la Netskope plateforme fournit un accès optimisé et une sécurité zéro confiance pour les personnes, les appareils et les données, où qu'ils aillent. Netskopeaide les clients à réduire les risques, à accélérer les performances et à obtenir une visibilité inégalée sur toutes les activités liées au cloud, au Web et aux applications privées. Des milliers de clients, dont plus de 25 entreprises du Fortune 100, font confiance Netskope à son puissant NewEdge réseau pour faire face à l'évolution des menaces, aux nouveaux risques, aux évolutions technologiques, aux changements organisationnels et au réseau, ainsi qu'aux nouvelles exigences réglementaires. Découvrez comment Netskope aider les clients à être prêts à tout au long de leur parcours SASE, rendez-vous sur netskope.com.

AWS AppFabric considérations relatives à l'ingestion des journaux d'audit

Les sections suivantes décrivent le schéma AppFabric de sortie, les formats de sortie et les destinations de sortie à utiliserNetskope.

Schéma et format

Netskopeprend en charge le schéma et les formats de AppFabric sortie suivants :

- Brut - JSON
  - AppFabric affiche les données dans le schéma d'origine utilisé par l'application source au format JSON.
- OCSF - JSON

- AppFabric normalise les données à l'aide de l'Open Cybersecurity Schema Framework (OCSF) et les produit au format JSON.

Emplacements de sortie

Netskopeprend en charge l'emplacement AppFabric de sortie suivant :

- Amazon Simple Storage Service (Amazon S3)
  - NetskopePour configurer la réception de données depuis le compartiment Amazon S3 qui contient vos journaux d'audit, suivez les instructions de la section Protection des données pour Amazon Web Services S3 sur le Netskope site Web.

NetWitness

NetWitnessest l'un des principaux développeurs de logiciels de détection et de réponse étendues (XDR). Sa base mondiale de clients très soucieux de la sécurité s'appuie sur NetWitness XDR pour se défendre contre des adversaires sophistiqués et agressifs. Doté de la plateforme la plus complète, intégrée et mature du secteur pour détecter, étudier et répondre aux attaques numériques, le NetWitness XDR constitue la base unificatrice d'un SOC moderne et efficace.

Grâce à son architecture hautement modulaire, NetWitness XDR détecte les menaces où qu'elles se produisent : dans le cloud, sur site, avec des travailleurs mobiles et distants, ou n'importe où entre les deux. La NetWitness plate-forme XDR offre une visibilité complète associée à des informations sur les menaces appliquées et à des analyses du comportement des utilisateurs pour détecter les menaces, hiérarchiser les activités, enquêter et automatiser les réponses. Tout cela permet aux analystes de sécurité d'être plus efficaces et plus rapides pour que les opérations de sécurité aient une longueur d'avance sur les menaces ayant un impact sur l'entreprise.

AWS AppFabric considérations relatives à l'ingestion des journaux d'audit

Les sections suivantes décrivent le schéma AppFabric de sortie, les formats de sortie et les destinations de sortie à utiliserNetWitness.

Schéma et format

NetWitness prend en charge le schéma et les formats de AppFabric sortie suivants :

- Brut - JSON

  - AppFabric affiche les données dans le schéma d'origine utilisé par l'application source au format JSON.
- OCSF - JSON
  - AppFabric normalise les données à l'aide de l'Open Cybersecurity Schema Framework (OCSF) et les produit au format JSON.

Emplacements de sortie

NetWitnessprend en charge l'emplacement AppFabric de sortie suivant :

- Amazon Simple Storage Service (Amazon S3)
  - NetWitnessPour configurer la réception de données depuis le compartiment Amazon S3 qui contient vos journaux d'audit, suivez les instructions du Guide de configuration du journal des sources d'événements du connecteur universel S3 sur la page Intégrations de NetWitness plateforme du NetWitness site Web.

Amazon QuickSight

Amazon fournit QuickSight aux entreprises axées sur les données une intelligence d'affaires (BI) unifiée à grande échelle. Tous les utilisateurs peuvent ainsi répondre à des besoins analytiques variés à partir de la même source de vérité grâce à des tableaux de bord interactifs modernes, à des rapports paginés, à des analyses intégrées et à des requêtes en langage naturel. QuickSight Vous pouvez analyser les données des journaux AWS AppFabric d'audit en QuickSight choisissant comme source votre bucket Amazon Simple Storage Service (Amazon S3) dans lequel AppFabric vos journaux de sécurité sont stockés.

AppFabric considérations relatives à l'ingestion des journaux d'audit

Les sections suivantes décrivent le schéma AppFabric de sortie, les formats de sortie et les destinations de sortie à utiliser avec Amazon QuickSight.

Schéma et formats

QuickSight prend en charge le schéma et les formats de AppFabric sortie suivants :

- Brut - JSON
  - AppFabric affiche les données dans le schéma d'origine utilisé par l'application source au format JSON.

- OCSF - JSON
  - AppFabric normalise les données à l'aide de l'Open Cybersecurity Schema Framework (OCSF) et les produit au format JSON.

Emplacements de sortie

QuickSight prend en charge les emplacements AppFabric de sortie suivants :

- Amazon S3
  - Vous pouvez ingérer des données d'Amazon S3 directement dans Amazon S3 en QuickSight créant un ensemble de données à l'aide de fichiers Amazon S3. Pour vérifier que votre ensemble de fichiers cible ne dépasse pas les quotas QuickSight des sources de données, consultez la section Quotas des sources de données dans le guide de QuickSight l'utilisateur Amazon.
  - Si votre ensemble de fichiers dépasse les QuickSight quotas pour une source de données Amazon S3, vous pouvez ingérer vos données dans Amazon S3 à l'aide d'Amazon Athena AWS Glue et de tables. L'utilisation d'Athena dans votre QuickSight jeu de données entraînera des coûts supplémentaires. Pour plus d'informations sur les tarifs d'Athena, consultez la page de tarification d'Athena.

    Pour utiliser Athena, procédez comme suit :

    1. Suivez les instructions de la section Utilisation AWS Glue pour vous connecter à des sources de données dans Amazon S3 dans le guide de l'utilisateur d'Athena.
    2. Suivez les instructions de la section Création d'un ensemble de données à l'aide des données Athena dans le guide de QuickSight l'utilisateur Amazon.

Rapid7

Rapid7, Inc. a pour mission de créer un monde numérique plus sûr en simplifiant et en rendant la cybersécurité plus accessible. Rapid7permet aux professionnels de la sécurité de gérer une surface d'attaque moderne grâce à la best-in-class technologie, à des recherches de pointe et à une vaste expertise stratégique. Rapid7Les solutions de sécurité complètes aident plus de 10 000 clients du monde entier à unir la gestion des risques liés au cloud et la détection des menaces afin de réduire les surfaces d'attaque et d'éliminer les menaces avec rapidité et précision.

AWS AppFabric considérations relatives à l'ingestion des journaux d'audit

Les sections suivantes décrivent le schéma AppFabric de sortie, le format de sortie et les destinations de sortie à utiliserRapid7.

Schéma et format

Rapid7prend en charge le schéma et les formats de AppFabric sortie suivants :

- Brut - JSON
  - AppFabric affiche les données dans le schéma d'origine utilisé par l'application source au format JSON.
- OCSF - JSON
  - AppFabric normalise les données à l'aide de l'Open Cybersecurity Schema Framework (OCSF) et les produit au format JSON.

Emplacements de sortie

Rapid7prend en charge l'emplacement AppFabric de sortie suivant :

- Amazon Simple Storage Service (Amazon S3)
  - Pour configurer Rapid7 afin de recevoir les données du compartiment Amazon S3 qui contient vos journaux d'audit, suivez les instructions du billet de blog Comment surveiller votre activité Amazon S3 avec InsightIDR sur le site Web du blog. Rapid7

Amazon Security Lake

Amazon Security Lake centralise automatiquement les données de sécurité provenant des AWS environnements, des fournisseurs de logiciels en tant que service (SaaS), des sources sur site et dans le cloud dans un lac de données spécialement conçu et stocké dans votre. Compte AWS Avec Security Lake, vous pouvez obtenir une compréhension plus complète de vos données de sécurité dans l'ensemble de votre organisation. Security Lake a adopté l'Open Cybersecurity Schema Framework (OCSF), un schéma d'événements de sécurité open source. Grâce au support OCSF, le service normalise et combine les données de sécurité issues d' AWS un large éventail de sources de données de sécurité d'entreprise.

AppFabric considérations relatives à l'ingestion des journaux d'audit

Vous pouvez transférer vos journaux d'audit SaaS dans Amazon Security Lake en Compte AWS ajoutant une source personnalisée à Security Lake. Les sections suivantes décrivent le schéma AppFabric de sortie, le format de sortie et les destinations de sortie à utiliser avec Security Lake.

Schéma et format

Security Lake prend en charge le schéma et le format de AppFabric sortie suivants :

- OCSF - JSON
  - AppFabric normalise les données à l'aide de l'Open Cybersecurity Schema Framework (OCSF) et les produit au format JSON.

Emplacements de sortie

Security Lake prend en charge AppFabric le support en tant que source personnalisée en utilisant un flux de livraison Amazon Data Firehose comme emplacement de sortie AppFabric d'ingestion. Pour configurer la AWS Glue table et le flux de diffusion Firehose, et pour configurer une source personnalisée dans Security Lake, utilisez les procédures suivantes.

Création d'une AWS Glue table

1. Accédez à Amazon Simple Storage Service (Amazon S3) et créez un bucket portant le nom de votre choix.
2. Accédez à la AWS Glue console.
3. Pour le catalogue de données, accédez à la section Tables, puis choisissez Ajouter une table.
4. Entrez le nom de votre choix pour ce tableau.
5. Sélectionnez le compartiment Amazon S3 que vous avez créé à l'étape 1.
6. Pour le format des données, sélectionnez JSON, puis Next.
7. Sur la page Choisir ou définir un schéma, choisissez Modifier le schéma au format JSON.
8. Entrez le schéma suivant et terminez le processus de création de la AWS Glue table.

```
[
    {
        "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>"
    }
]
```

Création d'une source personnalisée dans Security Lake

1. Accédez à la console Amazon Security Lake.
2. Sélectionnez Sources personnalisées dans le volet de navigation.
3. Choisissez Créer une source personnalisée.
4. Entrez un nom pour votre source personnalisée et sélectionnez une classe d'événements OCSF applicable.

> **Note**
>
> AppFabric utilise les classes d'événements de changement de compte, d'authentification, de gestion de l'accès utilisateur, de gestion des groupes, d'activité des ressources Web et d'activité d'accès aux ressources Web.

5. Entrez votre Compte AWS identifiant à la fois pour l'ID et pour l' Compte AWS ID externe. Ensuite, choisissez Créer.
6. Enregistrez l'emplacement Amazon S3 de la source personnalisée. Vous l'utiliserez pour configurer un flux de diffusion Amazon Data Firehose.

Créer un flux de diffusion dans Firehose

1. Accédez à la console Amazon Data Firehose.
2. Choisissez Créer un flux de diffusion.
3. Pour Source, sélectionnez Direct PUT.
4. Pour Destination, choisissez S3.
5. Dans la section Transformer et convertir les enregistrements, choisissez Activer la conversion du format d'enregistrement et choisissez Apache Parquetcomme format de sortie.
6. Pour le AWS Glue tableau, choisissez le AWS Glue tableau que vous avez créé lors de la procédure précédente, puis choisissez la dernière version.

7. Pour les paramètres de destination, choisissez le compartiment Amazon S3 que vous avez créé avec la source personnalisée Security Lake.
8. Pour le partitionnement dynamique, choisissez Activé.
9. Pour l'analyse en ligne pour JSON, choisissez Enabled.
   - Pour Keyname, entrez`eventDayValue`.
   - Pour JQ Expression, entrez`(.time/1000)|strftime("%Y%m%d")`.
10. Pour le préfixe du compartiment S3, entrez la valeur suivante.

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

    Remplacez <region>et <account_id>par votre Compte AWS identifiant Région AWS et.
11. Pour le préfixe de sortie d'erreur du compartiment S3, entrez la valeur suivante.

    ```
    ext/AppFabric/error/
    ```
12. Pour la durée de la nouvelle tentative, sélectionnez 300.
13. Pour la taille de la mémoire tampon, sélectionnez 128 MiB.
14. Pour l'intervalle de mémoire tampon, sélectionnez 60s.
15. Terminez le processus de création du flux de diffusion Firehose.

Créez des AppFabric ingestions

Pour envoyer des données à Amazon Security Lake, vous devez créer une ingestion dans la AppFabric console qui utilise le flux de diffusion Firehose que vous avez créé précédemment comme emplacement de sortie. Pour plus d'informations sur la configuration des AppFabric ingestions afin d'utiliser Firehose comme emplacement de sortie, consultez la section Créer un emplacement de sortie.

Singularity Cloud

La Singularity Cloud plateforme protège votre entreprise contre les menaces de toutes catégories, à tous les stades. Son IA (intelligence artificielle) brevetée étend la sécurité des signatures et modèles connus aux attaques les plus sophistiquées, telles que le zero-day et les ransomwares.

AWS AppFabric considérations relatives à l'ingestion des journaux d'audit

Les sections suivantes décrivent le schéma AppFabric de sortie, les formats de sortie et les destinations de sortie à utiliserSingularity Cloud.

Schéma et format

Singularity Cloudprend en charge le schéma et les formats de AppFabric sortie suivants :

OCSF - JSON : AppFabric normalise les données à l'aide de l'Open Cybersecurity Schema Framework (OCSF) et les produit au format JSON.

Emplacements de sortie

Singularity Cloudprend en charge la réception des journaux d'audit à partir des emplacements AppFabric de sortie suivants.

- Amazon Simple Storage Service (Amazon S3)
  - Singularity CloudPour configurer la réception de données depuis le compartiment Amazon S3 qui contient vos journaux d'audit, suivez les instructions de la Singularity Cloud’s documentation.

Splunk

Splunkcontribue à rendre les organisations plus résilientes. Les grandes entreprises utilisent Splunk la plateforme unifiée de sécurité et d'observabilité pour garantir la sécurité et la fiabilité de leurs systèmes numériques. Organisations font confiance Splunk pour éviter que les problèmes liés à la sécurité, à l'infrastructure et aux applications ne se transforment en incidents majeurs, pour absorber les chocs liés aux perturbations numériques et pour accélérer la transformation numérique.

AWS AppFabric considérations relatives à l'ingestion des journaux d'audit

Les sections suivantes décrivent le schéma AppFabric de sortie, les formats de sortie et les destinations de sortie à utiliserSplunk.

Schéma et format

Splunk prend en charge le schéma et les formats AppFabric de sortie suivants :

- Brut - JSON
  - AppFabric affiche les données dans le schéma d'origine utilisé par l'application source au format JSON.

- OCSF - JSON
  - AppFabric normalise les données à l'aide de l'Open Cybersecurity Schema Framework (OCSF) et les produit au format JSON.
- OCSF - Parquet
  - AppFabric normalise les données à l'aide de l'Open Cybersecurity Schema Framework (OCSF) et affiche les données dans le Apache Parquet format.

Emplacements de sortie

Splunkprend en charge les emplacements AppFabric de sortie suivants :

- Amazon Data Firehose
  - SplunkPour configurer la réception des journaux d'audit à partir du flux Firehose qui contient vos journaux d'audit, suivez les instructions de la section SplunkModule complémentaire pour Amazon Data Firehose sur le site Web. Splunk
- Amazon Simple Storage Service (Amazon S3)
  - SplunkPour configurer la réception de données depuis le compartiment Amazon S3 qui contient vos journaux d'audit, suivez les instructions de la section Configurer les entrées S3 basées sur SQL pour le Splunk module complémentaire pour AWS le Splunk site Web.

Supprimer AWS AppFabric pour les ressources de sécurité

Si vous ne souhaitez pas continuer à AWS AppFabric les utiliser pour des raisons de sécurité, veillez à supprimer les données dans les emplacements de sortie que vous avez créés lors de la configuration et dans AppFabric les ressources de sécurité afin d'éviter des frais supplémentaires. Pour nettoyer vos AppFabric ressources, vous devez les supprimer dans l'ordre inverse dans lequel vous les avez créées pour chaque application logicielle en tant que service (SaaS) : destinations d'ingestion > Ingestions > Autorisation des applications > Bundles d'applications

Après avoir supprimé l'autorisation finale de votre application, vous pouvez supprimer le bundle d'applications.

Rubriques

- Supprimer une destination d'ingestion
- Supprimer une ingestion
- Supprimer l'autorisation d'une application

- Supprimer un bundle d'applications

Supprimer une destination d'ingestion

Si vous sélectionnez un emplacement de sortie lorsque vous créez une ingestion, AppFabric pour des raisons de sécurité, elle crée des destinations d'ingestion en votre nom. Pour supprimer une destination d'ingestion, procédez comme suit :

1. Ouvrez la AppFabric console à l'adresse https://console.aws.amazon.com/appfabric/.
2. Sur la page de démarrage, développez le menu de gauche.
3. Choisissez Ingestions.
4. Choisissez une autorisation d'application.
5. Sélectionnez le bouton d'option situé à côté de la destination que vous souhaitez supprimer, puis choisissez Supprimer.
6. Choisissez Supprimer dans la boîte de dialogue de suppression de la destination pour confirmer.
7. Répétez les étapes ci-dessus pour toutes vos destinations.

Supprimer une ingestion

Pour supprimer une ingestion, procédez comme suit :

1. Sur la page de démarrage, développez le menu de gauche.
2. Choisissez Ingestions.
3. Sélectionnez le bouton d'option situé à côté de l'autorisation de votre application.
4. Choisissez le menu déroulant Actions.
5. Sélectionnez Delete (Supprimer).
6. Choisissez Supprimer dans la boîte de dialogue de suppression de l'ingestion pour confirmer.

Supprimer l'autorisation d'une application

Pour supprimer l'autorisation d'une application, procédez comme suit :

1. Sur la page de démarrage, développez le menu de gauche.
2. Choisissez Autorisations de l'application.

3. Sélectionnez le bouton d'option situé à côté de l'autorisation d'application que vous souhaitez supprimer.
4. Choisissez le menu déroulant Actions.
5. Sélectionnez Delete (Supprimer).
6. Choisissez Supprimer dans la boîte de dialogue de suppression de l'ingestion pour confirmer.

Supprimer un bundle d'applications

Pour supprimer votre pack d'applications, procédez comme suit :

1. Sur la page de démarrage, développez le menu de gauche.
2. Choisissez App Bundle.
3. Choisissez le bouton Supprimer.
4. Tapez `delete` pour confirmer, puis choisissez Supprimer.

Qu'est-ce que c'est AWS AppFabric pour la productivité ?

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

> **Note**
>
> Propulsé par Amazon Bedrock : AWS implémente la détection automatique des abus. Parce que AWS AppFabric la productivité repose sur Amazon Bedrock, les utilisateurs héritent des contrôles mis en œuvre dans Amazon Bedrock pour renforcer la sûreté, la sécurité et l'utilisation responsable de l'IA.

AWS AppFabric for productivity (version préliminaire) permet de réinventer la productivité des utilisateurs finaux dans les applications tierces en générant des informations et des actions basées sur le contexte de plusieurs applications. Les développeurs d'applications reconnaissent que l'accès aux données utilisateur depuis d'autres applications est important pour créer une expérience applicative plus productive, mais ils ne souhaitent pas créer et gérer des intégrations avec chaque

application. AppFabric Pour ce qui est de la productivité, les développeurs d'applications ont accès à des API génératives basées sur l'IA qui génèrent des informations et des actions relatives aux données inter-applications afin de fournir une expérience utilisateur plus riche grâce à des assistants d'IA générative nouveaux ou existants. AppFabric pour la productivité intègre les données de plusieurs applications, éliminant ainsi la nécessité pour les développeurs de créer ou de maintenir point-to-point des intégrations. Les développeurs d'applications peuvent intégrer AppFabric la productivité directement dans l'interface utilisateur de leur application, afin de garantir une expérience cohérente à leurs utilisateurs finaux tout en faisant ressortir le contexte pertinent des autres applications.

AppFabric pour la productivité connecte les données provenant d'applications couramment utilisées telles que AsanaAtlassian Jira Suite,Google Workspace,Microsoft 365,Miro,Slack,Smartsheet,,,, etc. AppFabric pour la productivité permet aux développeurs d'applications de créer plus facilement des expériences applicatives plus personnalisées qui améliorent l'adoption, la satisfaction et la fidélité des utilisateurs. Dans le même temps, les utilisateurs finaux bénéficient de l'accès aux informations dont ils ont besoin à partir de leurs applications sans interrompre leur flux de travail.

Rubriques

Avantages

En AppFabric matière de productivité, les développeurs d'applications ont accès à des API qui génèrent des informations et des actions relatives aux données inter-applications afin de fournir une expérience utilisateur plus riche grâce à des assistants d'IA générative nouveaux ou existants.

- Source unique de données utilisateur inter-applications : AppFabric pour la productivité, intègre les données de plusieurs applications, ce qui évite aux développeurs de créer ou de gérer des point-to-point intégrations. Les données des applications SaaS sont traitées pour être utilisées dans

d'autres applications en normalisant automatiquement les types de données disparates dans un format compréhensible par toutes les applications, ce qui permet aux développeurs d'applications d'intégrer davantage de données qui améliorent réellement la productivité des utilisateurs finaux.

- Contrôle total de l'expérience utilisateur : les développeurs intègrent AppFabric la productivité directement dans l'interface utilisateur de leur application, en gardant le contrôle total de l'expérience utilisateur tout en fournissant des informations personnalisées et des actions recommandées aux utilisateurs finaux grâce au contexte de l'ensemble de leurs applications. Cela rend AppFabric la productivité disponible dans l'application SaaS préférée des utilisateurs finaux et est accessible dans l'application qu'ils préfèrent pour accomplir leurs tâches. Les utilisateurs finaux passent moins de temps à passer d'une application à l'autre et peuvent ainsi rester concentrés sur leur travail.
- Accélérez les délais de commercialisation : en un seul appel d'API, les développeurs d'applications peuvent obtenir des informations au niveau de l'utilisateur sur les données d'un utilisateur générées sans avoir à affiner un modèle, à rédiger une invite personnalisée ou à créer des intégrations entre plusieurs applications. AppFabric élimine cette complexité pour permettre aux développeurs d'applications de créer, d'intégrer ou d'enrichir plus rapidement les capacités d'IA générative. Cela permet aux développeurs d'applications de concentrer leurs ressources sur les tâches les plus importantes.
- Des références à des artefacts pour renforcer la confiance des utilisateurs : dans le cadre des résultats, des artefacts pertinents ou AppFabric des fichiers source seront mis en évidence dans le but de générer les informations nécessaires pour renforcer la confiance des utilisateurs finaux dans les résultats du LLM.
- Autorisations utilisateur simplifiées : les artefacts utilisateur utilisés pour générer des informations sont basés sur ce à quoi l'utilisateur a accès. AppFabric pour la productivité utilise les autorisations et le contrôle d'accès d'un éditeur de logiciels indépendants comme source de vérité.

Cas d’utilisation

Les développeurs d'applications peuvent utiliser la notion de productivité AppFabric pour repenser la productivité au sein de leurs applications. AppFabric for productivity propose deux API axées sur les cas d'utilisation suivants pour aider ses utilisateurs finaux à être plus productifs :

- Donnez la priorité à votre journée
  - L'API d'informations exploitables aide les utilisateurs à gérer au mieux leur journée en leur fournissant des informations pertinentes provenant de l'ensemble de leurs applications, notamment les e-mails, le calendrier, les messages, les tâches, etc. En outre, les utilisateurs

peuvent exécuter des actions inter-applications telles que la création d'e-mails, la planification de réunions et la création d'actions à partir de leur application préférée. Par exemple, un employé qui a connu une escalade de clientèle pendant la nuit verra non seulement un résumé des conversations du jour au lendemain, mais pourra également voir une action recommandée pour planifier une réunion avec le responsable de compte du client. Les actions sont préremplies avec les champs obligatoires (tels que le nom et le propriétaire de la tâche, ou l'expéditeur/destinataire de l'e-mail), avec la possibilité de modifier le contenu prérempli avant d'exécuter l'action.

- Préparez-vous pour les prochaines réunions
  - L'API de préparation des réunions aide les utilisateurs à mieux préparer les réunions en résumant l'objectif de la réunion et en mettant en évidence les artefacts pertinents provenant de différentes applications, tels que les e-mails, les messages, etc. Les utilisateurs peuvent désormais se préparer rapidement pour les réunions et ne perdent pas de temps à passer d'une application à l'autre pour trouver du contenu.

Accès à AppFabric des fins de productivité

AppFabric for productivity est actuellement lancé en version préliminaire et disponible dans l'est des États-Unis (Virginie du Nord) Région AWS. Pour plus d'informations sur Régions AWS, consultez la section AWS AppFabric Points de terminaison et quotas dans le Références générales AWS.

Dans chaque région, vous pouvez accéder à AppFabric des fins de productivité de l'une des manières suivantes :

- En tant que développeur d'applications
  - Mise en route AppFabric pour la productivité (version préliminaire) pour les développeurs d'applications
- En tant qu'utilisateur final
  - Mise en route AppFabric pour la productivité (version préliminaire) pour les utilisateurs finaux

Mise en route AppFabric pour la productivité (version préliminaire) pour les développeurs d'applications

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modificat ion.

Cette section aide les développeurs d'applications à intégrer AWS AppFabric des applications à des fins de productivité (version préliminaire). AWS AppFabric for productivity permet aux développeurs de créer des expériences applicatives plus riches pour leurs utilisateurs en générant des informations et des actions basées sur l'IA à partir d'e-mails, d'événements de calendrier, de tâches, de messages, etc. dans de multiples applications. Pour obtenir la liste des applications prises en charge, consultez la section Applications AWS AppFabric prises en charge.

AppFabric for productivity permet aux développeurs d'applications de créer et d'expérimenter dans un environnement sécurisé et contrôlé. Lorsque vous commencez à utiliser AppFabric pour la productivité, vous créez AppClient et enregistrez un seul utilisateur de test. Cette approche est conçue pour vous aider à comprendre et à tester le flux d'authentification et de communication entre votre application et AppFabric. Après avoir effectué le test avec un seul utilisateur, vous pouvez soumettre votre demande à des AppFabric fins de vérification avant d'étendre l'accès à d'autres utilisateurs (voirÉtape 5. Demande AppFabric de vérification de votre candidature). AppFabric vérifiera les informations des applications avant de permettre une adoption généralisée afin de protéger les développeurs d'applications, les utilisateurs finaux et leurs données, ouvrant ainsi la voie à une adoption plus large par les utilisateurs de manière responsable.

Rubriques

Prérequis

Avant de commencer, vous devez créer un Compte AWS. Pour plus d'informations, consultez Inscrivez-vous pour un Compte AWS. Vous devez également créer au moins un utilisateur ayant accès à la politique `"appfabric:CreateAppClient"` IAM répertoriée ci-dessous, qui permet à l'utilisateur d'enregistrer votre application. AppFabric Pour plus d'informations sur

l'octroi d'autorisations AppFabric pour les fonctionnalités de productivité, consultezAppFabric pour des exemples de politiques IAM de productivité. Bien qu'il soit avantageux d'avoir un utilisateur administratif, il n'est pas obligatoire pour la configuration initiale. Pour plus d'informations, consultez Création d'un utilisateur doté d'un accès administratif.

AppFabric pour la productivité, uniquement dans l'est des États-Unis (Virginie du Nord) lors de la prévisualisation. Assurez-vous que vous vous trouvez dans cette région avant de commencer les étapes ci-dessous.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Étape 1. Créez et AppFabric améliorez la productivité AppClient

Avant de pouvoir commencer à faire surface AppFabric pour obtenir des informations sur la productivité au sein de votre application, vous devez créer un AppFabric AppClient. An AppClient est essentiellement votre passerelle vers AppFabric la productivité, fonctionnant comme un client d'application OAuth sécurisé permettant une communication sécurisée entre votre application et. AppFabric Lorsque vous créez un AppClient, vous recevrez un AppClient identifiant, un identifiant unique essentiel pour garantir AppFabric qu'il fonctionne avec votre application et votre Compte AWS.

AppFabric for productivity permet aux développeurs d'applications de créer et d'expérimenter dans un environnement sécurisé et contrôlé. Lorsque vous commencez à utiliser AppFabric pour la productivité, vous créez AppClient et enregistrez un seul utilisateur de test. Cette approche est conçue pour vous aider à comprendre et à tester le flux d'authentification et de communication entre votre application et AppFabric. Après avoir effectué le test avec un seul utilisateur, vous pouvez soumettre votre demande à des AppFabric fins de vérification avant d'étendre l'accès à d'autres utilisateurs (voirÉtape 5. Demande AppFabric de vérification de votre candidature). AppFabric vérifiera les informations des applications avant de permettre une adoption généralisée afin de

protéger les développeurs d'applications, les utilisateurs finaux et leurs données, ouvrant ainsi la voie à une adoption plus large par les utilisateurs de manière responsable.

Pour créer un AppClient, utilisez l'opération AWS AppFabric `CreateAppClient` API. Si vous devez mettre à jour AppClient after, vous pouvez utiliser l'opération `UpdateAppClient` API pour modifier uniquement les URL de redirection. Si vous devez modifier l'un des autres paramètres qui vous sont associés, AppClient tels que AppName ou description, vous devez le supprimer AppClient et en créer un nouveau. Pour plus d'informations, consultez CreateAppClient.

Vous pouvez enregistrer votre application auprès de AWS services à l'aide de l'`CreateAppClient`API en utilisant plusieurs langages de programmation, notamment Python, Node.js, Java, C#, Go et Rust. Pour plus d'informations, consultez la section Demander des exemples de signature dans le guide de l'utilisateur IAM. Vous devez utiliser les informations d'identification de la version 4 de la signature de votre compte pour effectuer cette opération d'API. Pour plus d'informations sur la version 4 de signature, voir Signing AWS API requests dans le guide de l'utilisateur IAM.

Champs de demande

- `appName`- Le nom de l'application qui sera affiché aux utilisateurs sur la page de consentement du portail AppFabric utilisateur. La page de consentement demande aux utilisateurs finaux l'autorisation d'afficher AppFabric des informations dans votre application. Pour plus de détails sur la page de consentement, voirÉtape 2. Donnez votre accord pour que l'application affiche des informations.
- `description`- Une description de l'application.
- `redirectUrls`- L'URI vers lequel rediriger les utilisateurs finaux après autorisation. Vous pouvez ajouter jusqu'à 5 URL de redirection. Par exemple, `https://localhost:8080`.
- `starterUserEmails`- Une adresse e-mail d'utilisateur qui sera autorisée à accéder pour recevoir les informations jusqu'à ce que l'application soit vérifiée. Une seule adresse e-mail est autorisée. Par exemple, `anyuser@example.com`
- `customerManagedKeyIdentifier`(facultatif) - L'ARN de la clé gérée par le client (générée par KMS) à utiliser pour chiffrer les données. Si elle n'est pas spécifiée, la clé AWS AppFabric gérée sera utilisée. Pour plus d'informations sur Clés détenues par AWS les clés gérées par le client, consultez la section Clés et AWS clés client dans le guide du AWS Key Management Service développeur.

Champs de réponse

- `appClientArn`- Le nom de ressource Amazon (ARN) qui inclut l' AppClient ID. Par exemple, l' AppClient identifiant esta`1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `verificationStatus`- L'état AppClient de la vérification.
  - `pending_verification`- La vérification du AppClient est toujours en cours avec AppFabric. Jusqu'à ce que le AppClient soit vérifié, un seul utilisateur (spécifié dans`starterUserEmails`) peut utiliser le AppClient. L'utilisateur verra une notification dans le portail AppFabric utilisateur, introduit dansÉtape 3. Ajoutez l'URL du portail AppFabric utilisateur à votre application, indiquant que l'application n'est pas vérifiée.
  - `verified`- Le processus de vérification a été effectué avec succès AppFabric et AppClient est désormais entièrement vérifié.
  - `rejected`- Le processus de vérification du AppClient a été rejeté par AppFabric. Il AppClient ne peut pas être utilisé par d'autres utilisateurs tant que le processus de vérification n'est pas relancé et terminé avec succès.

```
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>"
}'
```

Si l'action aboutit, le service renvoie une réponse HTTP 200.

```
{
    "appClientConfigSummary": {
        "appClientArn": "arn:aws:appfabric:<region>:<account>:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "verificationStatus": "pending_verification"
    }
}
```

Étape 2. Authentifiez et autorisez votre application

Permettez à votre application d'intégrer les AppFabric informations en toute sécurité en établissant un flux d'autorisation OAuth 2.0. Tout d'abord, vous devez créer un code d'autorisation qui vérifie l'identité de votre application. Pour plus d'informations, consultez Autoriser. Vous échangerez ensuite ce code d'autorisation contre un jeton d'accès, qui accorde à votre application les autorisations nécessaires pour récupérer et afficher AppFabric des informations au sein de votre application. Pour plus d'informations, consultez Jeton.

Pour plus d'informations sur l'octroi de l'autorisation d'autoriser une application, consultezAutoriser l'accès pour autoriser les applications.

1. Pour créer un code d'autorisation, utilisez l'opération AWS AppFabric `oauth2/authorize` API.

   Champs de demande

   - `app_client_id`(obligatoire) - L' AppClient ID du fichier Compte AWS créé à l'étape 1. Créez un AppClient. Par exemple, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
   - `redirect_uri`(obligatoire) - L'URI vers lequel rediriger les utilisateurs finaux après l'autorisation que vous avez utilisée à l'étape 1. Créez un AppClient. Par exemple, `https://localhost:8080`.
   - `state`(obligatoire) - Une valeur unique pour maintenir l'état entre la demande et le rappel. Par exemple, `a8904edc-890c-1005-1996-29a757272a44`.

   ```
   GET https://productivity.appfabric.<region>.amazonaws.com/oauth2/authorize?
   app_client_id=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\
   redirect_uri=https://localhost:8080&state=a8904edc-890c-1005-1996-29a757272a44
   ```

2. Après l'authentification, vous serez redirigé vers l'URI spécifié avec un code d'autorisation renvoyé en tant que paramètre de requête. Par exemple, où`code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`.

   ```
   https://localhost:8080/?code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-
   sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-
   oampc&state=a8904edc-890c-1005-1996-29a757272a44
   ```

3. Échangez ce code d'autorisation contre un jeton d'accès à l'aide de l'opération AppFabric `oauth2/token` API.

Ce jeton est utilisé pour les demandes d'API et est initialement valide `starterUserEmails` jusqu'à ce qu' AppClient il soit vérifié. Une fois AppClient le vérifié, ce jeton peut être utilisé pour n'importe quel utilisateur. Vous devez utiliser les informations d'identification de la version 4 de la signature de votre compte pour effectuer cette opération d'API. Pour plus d'informations sur la version 4 de signature, voir Signing AWS API requests dans le guide de l'utilisateur IAM.

Champs de demande

- `code`(obligatoire) - Le code d'autorisation que vous avez reçu après vous être authentifié à la dernière étape. Par exemple, `mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`.
- `app_client_id`(obligatoire) - L' AppClient ID du fichier Compte AWS créé à l'étape 1. Créez un AppClient. Par exemple, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `grant_type`(obligatoire) - La valeur doit être`authorization_code`.
- `redirect_uri`(obligatoire) - L'URI vers lequel rediriger les utilisateurs après l'autorisation que vous avez utilisée à l'étape 1. Créez un AppClient. Il doit s'agir du même URI de redirection que celui utilisé pour créer un code d'autorisation. Par exemple, `https://localhost:8080`.

Champs de réponse

- `expires_in`- Combien de temps avant l'expiration du jeton. Le délai d'expiration par défaut est de 12 heures.
- `refresh_token`- Le jeton d'actualisation reçu lors de la demande initiale /token.
- `token`- Le jeton reçu lors de la demande initiale /token.
- `token_type`- La valeur sera de`Bearer`.
- `appfabric_user_id`- Le nom AppFabric d'utilisateur. Ceci n'est renvoyé que pour les demandes utilisant le type de `authorization_code` subvention.

```
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\"
}"
```

Si l'action aboutit, le service renvoie une réponse HTTP 200.

```
{
    "expires_in": 43200,
    "refresh_token": "apkaeibaerjr2example",
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "<userId>"
}
```

Étape 3. Ajoutez l'URL du portail AppFabric utilisateur à votre application

Les utilisateurs finaux doivent être autorisés AppFabric à accéder aux données de leurs applications qui sont utilisées pour générer des informations. AppFabric simplifie ce processus pour les développeurs d'applications en créant un portail utilisateur dédié (écran contextuel) permettant aux utilisateurs finaux d'autoriser leurs applications. Lorsque les utilisateurs sont prêts à améliorer leur productivité, ils sont redirigés vers le portail utilisateur qui leur permet de connecter et de gérer les applications utilisées pour générer des informations et des actions inter-applications. AppFabric Une fois connectés, les utilisateurs peuvent connecter des applications à AppFabric des fins de productivité, puis revenir à votre application pour explorer les informations et les actions. Pour intégrer votre application à des AppFabric fins de productivité, vous devez ajouter une AppFabric URL spécifique à votre application. Cette étape est essentielle pour permettre aux utilisateurs d'accéder au portail AppFabric utilisateur directement depuis votre application.

1. Accédez aux paramètres de votre application et recherchez la section permettant d'ajouter des URL de redirection.
2. Une fois que vous avez trouvé la zone appropriée, ajoutez l' AppFabric URL suivante comme URL de redirection vers votre application :

```
https://userportal.appfabric.<region>.amazonaws.com/eup_login
```

Après avoir ajouté l'URL, votre application sera configurée pour diriger les utilisateurs vers le portail AppFabric utilisateur. Ici, les utilisateurs peuvent se connecter, se connecter et gérer leurs applications utilisées AppFabric pour générer des informations sur la productivité.

Étape 4 : AppFabric À utiliser pour mettre en évidence des informations et des actions provenant de différentes applications

Une fois que les utilisateurs ont connecté leurs applications, vous pouvez leur apporter les informations dont ils ont besoin pour améliorer leur productivité en réduisant le changement d'application et de contexte. AppFabric ne génère des informations pour un utilisateur que sur la base des informations auxquelles il est autorisé à accéder. AppFabric stocke les données utilisateur dans un Compte AWS fichier appartenant à AppFabric. Pour plus d'informations sur l' AppFabric utilisation de vos données, consultezTraitement des données.

Vous pouvez utiliser les API basées sur l'IA suivantes pour générer et mettre en évidence des informations et des actions au niveau des utilisateurs au sein de vos applications :

- `ListActionableInsights`— Pour plus d'informations, consultez la section Informations exploitables ci-dessous.
- `ListMeetingInsights`— Pour plus d'informations, consultez la section Préparation de la réunion plus loin dans ce guide.

Informations exploitables () **`ListActionableInsights`**

L'`ListActionableInsights`API aide les utilisateurs à gérer au mieux leur journée en fournissant des informations exploitables basées sur l'activité de leurs applications, notamment les e-mails, le calendrier, les messages, les tâches, etc. Les informations renvoyées afficheront également des liens intégrés vers les artefacts utilisés pour générer les informations, ce qui aidera les utilisateurs à visualiser rapidement les données utilisées pour générer les informations. En outre, l'API peut renvoyer des suggestions d'actions basées sur les informations et permettre aux utilisateurs d'exécuter des actions inter-applications depuis votre application. Plus précisément, l'API s'intègre à des plateformes telles que AsanaGoogle Workspace,Microsoft 365, et Smartsheet pour permettre aux utilisateurs d'envoyer des e-mails, de créer des événements de calendrier et de créer des tâches. Les grands modèles linguistiques (LLM) peuvent prérenseigner les détails d'une action

recommandée (tels que le corps de l'e-mail ou le nom de la tâche), que les utilisateurs peuvent personnaliser avant l'exécution, ce qui simplifie la prise de décision et améliore la productivité. À l'instar de l'expérience utilisée par les utilisateurs finaux pour autoriser les applications, AppFabric utilise le même portail dédié permettant aux utilisateurs de visualiser, de modifier et d'exécuter des actions entre applications. Pour exécuter des actions, AppFabric les ISV doivent rediriger les utilisateurs vers un portail AppFabric utilisateur où ils peuvent voir les détails des actions et les exécuter. Chaque action générée par AppFabric possède une URL unique. Cette URL est disponible dans la réponse de `ListActionableInsights` l'API.

Vous trouverez ci-dessous un résumé des actions inter-applications prises en charge et des applications dans lesquelles :

- Envoyer un e-mail (Google Workspace,Microsoft 365)
- Créer un événement de calendrier (Google Workspace,Microsoft 365)
- Créer une tâche (Asana,Smartsheet)

Champs de demande

- `nextToken`(facultatif) - Le jeton de pagination pour récupérer le prochain ensemble d'informations.
- `includeActionExecutionStatus`- Un filtre qui accepte la liste des statuts d'exécution des actions. Les actions sont filtrées en fonction des valeurs de statut transmises. Valeurs possibles : `NOT_EXECUTED` | `EXECUTED`

En-tête de demande

- L'en-tête d'autorisation doit être transmis avec la `Bearer Token` valeur.

Champs de réponse

- `insightId`- L'identifiant unique de l'aperçu généré.
- `insightContent`- Cela renvoie un résumé de l'aperçu et des liens intégrés vers les artefacts utilisés pour générer l'aperçu. Remarque : Il s'agirait d'un contenu HTML contenant des liens intégrés (<a>balises).
- `insightTitle`- Le titre de l'aperçu généré.
- `createdAt`- Quand les informations ont été générées.
- `actions`- Une liste d'actions recommandées pour les informations générées. Objet de l'action :

- `actionId`- L'identifiant unique de l'action générée.
- `actionIconUrl`- L'URL de l'icône de l'application dans laquelle il est suggéré d'exécuter l'action.
- `actionTitle`- Le titre de l'action générée.
- `actionUrl`- L'URL unique permettant à l'utilisateur final de visualiser et d'exécuter l'action dans AppFabric le portail utilisateur. Remarque : pour exécuter des actions, les applications ISV redirigeront les utilisateurs vers le portail AppFabric utilisateur (écran contextuel) à l'aide de cette URL.
- `actionExecutionStatus`- Une énumération indiquant le statut de l'action. Les valeurs possibles sont les suivantes : `EXECUTED` | `NOT_EXECUTED`

- `nextToken`(facultatif) - Le jeton de pagination pour récupérer le prochain ensemble d'informations. Il s'agit d'un champ facultatif qui, s'il est renvoyé nul, signifie qu'il n'y a plus d'informations à charger.

Pour plus d'informations, consultez ActionableInsights.

```
curl -v --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/actionableInsights" \
  --header "Authorization: Bearer <token>"
```

Si l'action aboutit, le service renvoie une réponse HTTP 200.

```
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
}
```

Préparation des réunions (**`ListMeetingInsights`**)

L'`ListMeetingInsights`API aide les utilisateurs à mieux préparer les réunions à venir en résumant l'objectif de la réunion et en mettant en évidence les éléments pertinents provenant de différentes applications, tels que les e-mails, les messages, etc. Les utilisateurs peuvent désormais se préparer rapidement pour les réunions et ne perdent pas de temps à passer d'une application à l'autre pour trouver du contenu.

Champs de demande

- `nextToken`(facultatif) - Le jeton de pagination pour récupérer le prochain ensemble d'informations.

En-tête de demande

- L'en-tête d'autorisation doit être transmis avec la `Bearer Token` valeur.

Champs de réponse

- `insightId`- L'identifiant unique de l'aperçu généré.
- `insightContent`- La description de l'aperçu mettant en évidence les détails sous forme de chaîne. Par exemple, pourquoi cette information est-elle importante ?
- `insightTitle`- Le titre de l'aperçu généré.
- `createdAt`- Quand les informations ont été générées.
- `calendarEvent`- L'événement ou la réunion importante du calendrier sur laquelle l'utilisateur doit se concentrer. Objet d'événement du calendrier :
  - `startTime`- L'heure de début de l'événement.
  - `endTime`- L'heure de fin de l'événement.
  - `eventUrl`- L'URL de l'événement du calendrier sur l'application ISV.
- `resources`- La liste contenant les autres ressources liées à la génération de l'aperçu. Objet de ressource :
  - `appName`- Le nom de l'application à laquelle appartient la ressource.
  - `resourceTitle`- Le titre de la ressource.
  - `resourceType`- Le type de ressource. Les valeurs possibles sont les suivantes : `EMAIL` | `EVENT` | `MESSAGE` | `TASK`
  - `resourceUrl`- L'URL de la ressource dans l'application.
  - `appIconUrl`- L'URL de l'image de l'application à laquelle appartient la ressource.
- `nextToken`(facultatif) - Le jeton de pagination pour récupérer le prochain ensemble d'informations. Il s'agit d'un champ facultatif qui, s'il est renvoyé nul, signifie qu'il n'y a plus d'informations à charger.

Pour plus d'informations, consultez MeetingInsights.

```
curl --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/meetingContexts" \
  --header "Authorization: Bearer <token>"
```

Si l'action aboutit, le service renvoie une réponse HTTP 201.

```
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
}
```

Fournissez des commentaires sur vos idées ou vos actions

Utilisez l'opération AppFabric `PutFeedback` API pour fournir des commentaires sur les informations et les actions générées. Vous pouvez intégrer cette fonctionnalité dans vos applications pour fournir un moyen de soumettre une évaluation (de 1 à 5, la note la plus élevée étant la meilleure) pour un InsightId ou ActionId.

Champs de demande

- `id`- L'identifiant de l'objet pour lequel le commentaire est soumis. Cela peut être le InsightId ou le ActionId.
- `feedbackFor`- Le type de ressource pour lequel les commentaires sont soumis. Valeurs possibles : `ACTIONABLE_INSIGHT` | `MEETING_INSIGHT` | `ACTION`
- `feedbackRating`- Évaluation des commentaires allant de 1 à`5`. Plus la note est élevée, mieux c'est.

Champs de réponse

- Il n'y a aucun champ de réponse.

Pour plus d'informations, consultez PutFeedback.

```
curl --request POST \
  --url "https://productivity.appfabric.<region>.amazonaws.com"\
"/feedback" \
  --header "Authorization: Bearer <token>" \
  --header "Content-Type: application/json" \
  --data '{
    "id": "1234-5678-9012",
    "feedbackFor": "ACTIONABLE_INSIGHT"
    "feedbackRating": 3
}'
```

Si l'action aboutit, le service renvoie une réponse HTTP 201 avec un corps HTTP vide.

Étape 5. Demande AppFabric de vérification de votre candidature

À ce stade, vous avez mis à jour l'interface utilisateur de votre application pour intégrer des informations et des actions AppFabric inter-applications, et vous avez reçu des informations pour un seul utilisateur. Une fois que vous êtes satisfait des tests et que vous souhaitez étendre votre expérience AppFabric enrichie à d'autres utilisateurs, vous pouvez soumettre votre candidature AppFabric pour examen et vérification. AppFabric vérifiera les informations des applications avant de permettre une adoption généralisée afin de protéger les développeurs d'applications, les utilisateurs finaux et leurs données, ouvrant ainsi la voie à une adoption plus large par les utilisateurs de manière responsable.

Lancer le processus de vérification

Commencez le processus de vérification en envoyant un e-mail à appfabric-appverification@amazon.com et en demandant que votre application soit vérifiée.

Incluez les informations suivantes dans votre e-mail :

- Votre Compte AWS identifiant
- Le nom de l'application pour laquelle vous souhaitez obtenir une vérification
- Votre AppClient identifiant
- Vos coordonnées

En outre, veuillez fournir les informations suivantes, si elles sont disponibles, pour nous aider à évaluer la priorité et l'impact :

- Nombre estimatif d'utilisateurs auxquels vous comptez accorder l'accès
- Votre date de lancement cible

> **Note**
>
> Si vous avez un Compte AWS responsable ou un responsable du développement des AWS partenaires, veuillez le copier sur votre e-mail. L'inclusion de ces contacts peut contribuer à accélérer le processus de vérification.

Critères de vérification

Avant de lancer le processus de vérification, vous devez répondre aux critères suivants :

- Vous devez utiliser un code valide Compte AWS pour être utilisé AppFabric pour des raisons de productivité

De plus, vous répondez à au moins l'un des critères suivants :

- Votre organisation est un AWS partenaire doté d'au moins un niveau « AWS Select ». AWS Partner Network Pour plus d'informations, consultez la section Niveaux de services aux AWS partenaires.
- Votre organisation doit avoir dépensé au moins 10 000$ en AppFabric services au cours des trois dernières années.
- Votre candidature doit être répertoriée sur le AWS Marketplace. Pour plus d'informations, consultez le AWS Marketplace.

Attendez la mise à jour du statut de vérification

Une fois votre candidature examinée, nous vous répondrons par e-mail et le statut de votre candidature AppClient passera de `pending_verification` à`verified`. Si votre demande est rejetée, vous devrez relancer le processus de vérification.

Gestion axée sur AppFabric la productivité AppClients

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Vous pouvez gérer votre productivité AppClients afin AppFabric de garantir le bon fonctionnement et la maintenance des processus d'authentification et d'autorisation.

Obtenez les détails d'un AppClient

Utilisez le fonctionnement de l' AppFabric `GetAppClient`API pour afficher les informations vous concernant AppClient, notamment pour vérifier AppClient son statut. Pour plus d'informations, consultez GetAppClient.

Pour obtenir des informations sur un AppClient, vous devez disposer, au minimum, des autorisations de politique `"appfabric:GetAppClient"` IAM. Pour plus d'informations, consultez Autoriser l'accès pour obtenir des informations sur AppClients.

Champs de demande

- `appClientId`- L' AppClient identifiant.

Champs de réponse

- `appName`- Le nom de l'application qui sera affiché aux utilisateurs sur la page de consentement du portail AppFabric utilisateur.
- `customerManagedKeyIdentifier`(facultatif) - L'ARN de la clé gérée par le client (générée par KMS) à utiliser pour chiffrer les données. Si elle n'est pas spécifiée, la clé AWS AppFabric gérée sera utilisée.
- `description`- Une description de l'application.
- `redirectUrls`- L'URI vers lequel rediriger les utilisateurs finaux après autorisation. Vous pouvez ajouter jusqu'à 5 URL de redirection. Par exemple, `https://localhost:8080`.
- `starterUserEmails`- Une adresse e-mail d'utilisateur qui sera autorisée à accéder pour recevoir les informations jusqu'à ce que l'application soit vérifiée. Une seule adresse e-mail est autorisée. Par exemple, `anyuser@example.com`.
- `verificationStatus`- L'état AppClient de la vérification.

- `pending_verification`- La vérification du AppClient est toujours en cours avec AppFabric. Jusqu'à ce que le AppClient soit vérifié, un seul utilisateur (spécifié dans`starterUserEmails`) peut utiliser le AppClient.
- `verified`- Le processus de vérification a été effectué avec succès AppFabric et AppClient est maintenant entièrement vérifié.
- `rejected`- Le processus de vérification du AppClient a été rejeté par AppFabric. Il AppClient ne peut pas être utilisé par d'autres utilisateurs tant que le processus de vérification n'est pas relancé et terminé avec succès.

```
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
```

Si l'action aboutit, le service renvoie une réponse HTTP 200.

```
200 OK

{
    "appClient": {
        "appName": "Test App",
        "arn": "arn:aws:appfabric:<region>:111122223333:appclient/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "customerManagedKeyArn": "arn:aws:kms:<region>:111122223333:key/<key>",
        "description": "This is a test app",
        "redirectUrls": [
            "https://localhost:8080"
        ],
        "starterUserEmails": [
            "anyuser@example.com"
        ],
        "verificationDetails": {
            "verificationStatus": "pending_verification"
        }
    }
```

```
}
```

Liste AppClients

Utilisez l'opération AppFabric `ListAppClients` API pour afficher la liste de vos AppClients. AppFabric n'en autorise qu'un AppClient par Compte AWS. Ceci est sujet à modification dans le futur. Pour plus d'informations, consultez ListAppClients.

Pour créer une liste AppClients, vous devez disposer, au minimum, des autorisations de politique `"appfabric:ListAppClients"` IAM. Pour plus d'informations, consultez Autoriser l'accès à la liste AppClients.

Champs de demande

- Il n'y a aucun champ obligatoire.

Champs de réponse

- `appClientARN`- Le nom de ressource Amazon (ARN) qui inclut l' AppClient ID. Par exemple, l' AppClient identifiant est`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `verificationStatus`- L'état AppClient de la vérification.
  - `pending_verification`- La vérification du AppClient est toujours en cours avec AppFabric. Jusqu'à ce que le AppClient soit vérifié, un seul utilisateur (spécifié dans`starterUserEmails`) peut utiliser le AppClient.
  - `verified`- Le processus de vérification a été effectué avec succès AppFabric et AppClient est maintenant entièrement vérifié.
  - `rejected`- Le processus de vérification du AppClient a été rejeté par AppFabric. Il AppClient ne peut pas être utilisé par d'autres utilisateurs tant que le processus de vérification n'est pas relancé et terminé avec succès.

```
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
```

Si l'action aboutit, le service renvoie une réponse HTTP 200.

```
200 OK

{
    "appClientList": [
        {
            "appClientArn": "arn:aws:appfabric:<region>:111122223333:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "verificationStatus": "pending_verification"
        }
    ]
}
```

Mettre à jour un AppClient

Utilisez l'opération AppFabric `UpdateAppClient` API pour mettre à jour les URL de redirection mappées à votre. AppClient Si vous devez modifier d'autres paramètres, tels que AppName starterUserEmails, ou autre, vous devez les supprimer AppClient et en créer un nouveau. Pour plus d'informations, consultez UpdateAppClient.

Pour mettre à jour un AppClient, vous devez disposer, au minimum, des autorisations de politique `"appfabric:UpdateAppClient"` IAM. Pour plus d'informations, consultez Autoriser l'accès à la mise à jour AppClients.

Champs de demande

- `appClientId`(obligatoire) - L' AppClient ID avec lequel vous mettez à jour les URL de redirection.
- `redirectUrls`(obligatoire) - La liste mise à jour des URL de redirection. Vous pouvez ajouter jusqu'à 5 URL de redirection.

Champs de réponse

- `appName`- Le nom de l'application qui sera affiché aux utilisateurs sur la page de consentement du portail AppFabric utilisateur.
- `customerManagedKeyIdentifier`(facultatif) - L'ARN de la clé gérée par le client (générée par KMS) à utiliser pour chiffrer les données. Si elle n'est pas spécifiée, la clé AWS AppFabric gérée sera utilisée.
- `description`- Une description de l'application.

- `redirectUrls`- L'URI vers lequel rediriger les utilisateurs finaux après autorisation. Par exemple, `https://localhost:8080`.
- `starterUserEmails`- Une adresse e-mail d'utilisateur qui sera autorisée à accéder pour recevoir les informations jusqu'à ce que l'application soit vérifiée. Une seule adresse e-mail est autorisée. Par exemple, `anyuser@example.com`.
- `verificationStatus`- L'état AppClient de la vérification.
  - `pending_verification`- La vérification du AppClient est toujours en cours avec AppFabric. Jusqu'à ce que le AppClient soit vérifié, un seul utilisateur (spécifié dans`starterUserEmails`) peut utiliser le AppClient.
  - `verified`- Le processus de vérification a été effectué avec succès AppFabric et AppClient est maintenant entièrement vérifié.
  - `rejected`- Le processus de vérification du AppClient a été rejeté par AppFabric. Il AppClient ne peut pas être utilisé par d'autres utilisateurs tant que le processus de vérification n'est pas relancé et terminé avec succès.

```
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"]
}'
```

Si l'action aboutit, le service renvoie une réponse HTTP 200.

```
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"
        }
    }
}
```

Supprimer un AppClient

Utilisez l'opération AppFabric `DeleteAppClient` API pour supprimer celles dont AppClients vous n'avez plus besoin. Pour plus d'informations, consultez DeleteAppClient.

Pour supprimer un AppClient, vous devez disposer, au minimum, des autorisations de politique `"appfabric:DeleteAppClient"` IAM. Pour plus d'informations, consultez Autoriser l'accès pour supprimer AppClients.

Champs de demande

- `appClientId`- L' AppClient identifiant.

Champs de réponse

- Il n'y a aucun champ de réponse.

```
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
```

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

Actualiser les jetons pour les utilisateurs finaux

Les jetons que vous AppClient obtenez pour les utilisateurs finaux peuvent être actualisés à leur expiration. Cela peut être fait à l'aide de l'JetonAPI avec le grant_type`refresh_token`. Le `refresh_token` à utiliser est renvoyé dans le cadre de la réponse de l'API token lorsque le grant_type est. `authorization_code` Le délai d'expiration par défaut est de 12 heures. Pour appeler l'API d'actualisation, vous devez disposer de l'autorisation de politique `"appfabric:Token"` IAM. Pour plus d'informations, consultez Jeton et Autoriser l'accès à la mise à jour AppClients.

Champs de demande

- `refresh_token`(obligatoire) - Le jeton d'actualisation reçu lors de la `/token` demande initiale.
- `app_client_id`(obligatoire) - L'ID de la AppClient ressource créée pour Compte AWS.
- `grant_type`(obligatoire) - Cela doit être le cas`refresh_token`.

Champs de réponse

- `expires_in`- Combien de temps avant l'expiration du jeton. Le délai d'expiration par défaut est de 12 heures.
- `refresh_token`- Le jeton d'actualisation reçu lors de la demande initiale /token.
- `token`- Le jeton reçu lors de la demande initiale /token.
- `token_type`- La valeur sera de`Bearer`.
- `appfabric_user_id`- L'identifiant de AppFabric l'utilisateur. Ceci n'est renvoyé que pour les demandes utilisant le type de `authorization_code` subvention.

```
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\"
}"
```

Si l’action aboutit, le service renvoie une réponse HTTP 200.

```
200 OK

{
    "expires_in": 43200,
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "${UserID}"
}
```

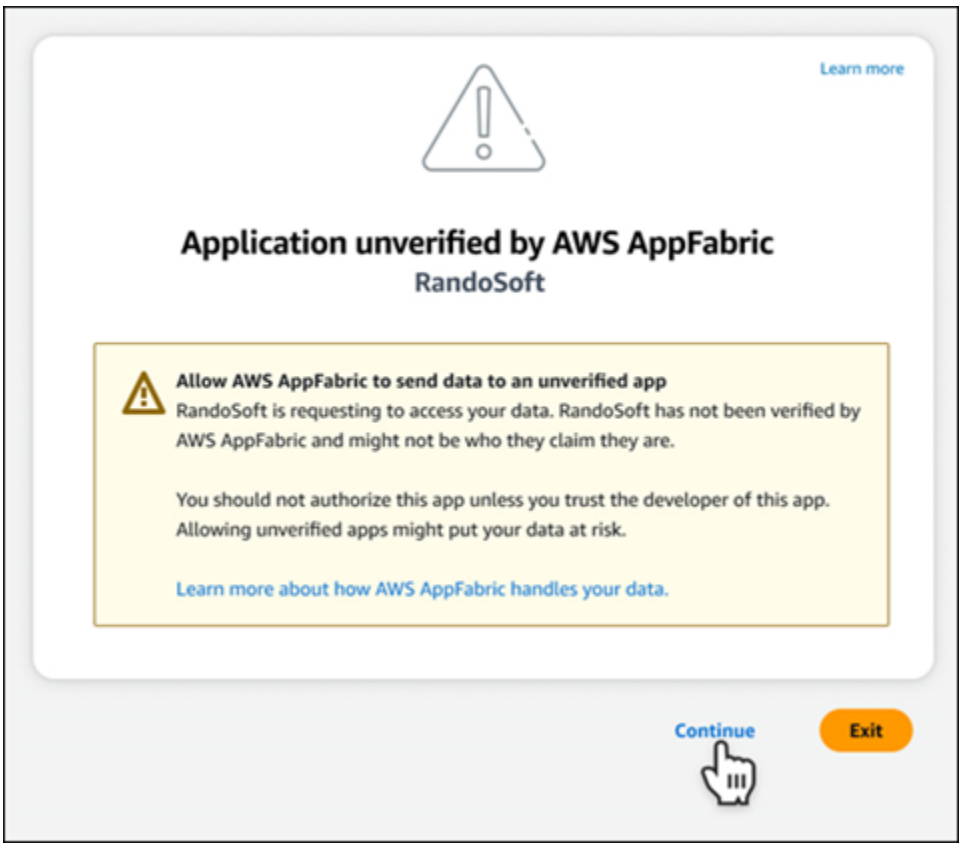
Résolution des problèmes

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Cette section décrit les erreurs courantes et les solutions de résolution des problèmes liés AppFabric à la productivité.

Candidature non vérifiée

Les développeurs d'applications qui utilisent AppFabric des outils de productivité pour enrichir leurs expériences applicatives passeront par un processus de vérification avant de lancer leurs fonctionnalités aux utilisateurs finaux. Toutes les applications commencent comme non vérifiées et ne deviennent vérifiées que lorsque le processus de vérification est terminé. Cela signifie que le message que `starterUserEmails` vous avez utilisé lors de la création d'un AppClient sera affiché.



Erreurs **`CreateAppClient`**

ServiceQuotaExceededException

Si vous recevez l'exception suivante lors de la création d'un AppClient, vous avez dépassé le nombre d'exceptions AppClients pouvant être créées par Compte AWS. La limite est de 1. Code d'état HTTP : 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
```

Erreurs **`GetAppClient`**

ResourceNotFoundException

Si vous recevez l'exception suivante lorsque vous obtenez les détails d'un AppClient, assurez-vous d'avoir saisi le bon AppClient identifiant. Cette erreur signifie que le fichier spécifié n' AppClient a pas été trouvé.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you’ve entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Erreurs **`DeleteAppClient`**

ConflictException

Si vous recevez l'exception suivante lors de la suppression d'une AppClient, une autre demande de suppression est en cours. Patientez jusqu'à ce qu'il soit terminé, puis réessayez. Code d’état HTTP : 409

```
ConflictException
Another delete request is in progress. Wait until it completes then try again.
HTTP Status Code: 409
```

ResourceNotFoundException

Si vous recevez l'exception suivante lors de la suppression d'un AppClient, assurez-vous d'avoir saisi le bon AppClient identifiant. Cette erreur signifie que le fichier spécifié n' AppClient a pas été trouvé.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you’ve entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Erreurs **`UpdateAppClient`**

ResourceNotFoundException

Si vous recevez l'exception suivante lors de la mise à jour d'un AppClient, assurez-vous d'avoir saisi le bon AppClient identifiant. Cette erreur signifie que le fichier spécifié n' AppClient a pas été trouvé.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you’ve entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Erreurs **`Authorize`**

ValidationException

L'exception suivante peut s'afficher si l'un des paramètres de l'API ne répond pas aux contraintes définies dans les spécifications de l'API.

```
ValidationException
HTTP Status Code: 400
```

Raison 1 : Lorsque AppClient l'identifiant n'est pas spécifié

Le `app_client_id` est absent dans les paramètres de la demande. Créez-le AppClient s'il n'a pas encore été créé ou utilisez le vôtre existant `app_client_id` et réessayez. Pour trouver l' AppClient ID, utilisez l'opération ListAppClientAPI.

Raison 2 : Quand AppFabric n'a pas accès à la clé gérée par le client

```
Message: AppFabric couldn't access the customer managed key configured for AppClient.
```

AppFabric n'est actuellement pas en mesure d'accéder aux clés gérées par le client, probablement en raison de récentes modifications de ses autorisations. Vérifiez que la clé spécifiée existe et que AppFabric les autorisations d'accès appropriées sont accordées.

Raison 3 : L'URL de redirection spécifiée n'est pas valide

```
Message: Redirect url invalid
```

Assurez-vous que l'URL de redirection figurant dans votre demande est correcte. Il doit correspondre à l'une des URL de redirection spécifiées lors de la création ou de la mise à jour du AppClient. Pour afficher la liste des URL de redirection autorisées, utilisez l'opération GetAppClientAPI.

Erreurs **`Token`**

TokenException

Vous pouvez bénéficier de l'exception suivante pour plusieurs raisons.

```
TokenException
HTTP Status Code: 400
```

Raison 1 : Lorsqu'un e-mail non valide est spécifié

```
Message: Invalid Email used
```

Assurez-vous que l'adresse e-mail que vous utilisez correspond à celle répertoriée pour l'`starterUserEmails`attribut lorsque vous avez créé le AppClient. Si les e-mails ne correspondent pas, utilisez l'adresse e-mail correspondante et réessayez. Pour afficher l'e-mail utilisé, utilisez l'opération GetAppClientAPI.

Raison 2 : Pour grant_type en tant que refresh_token lorsque le jeton n'est pas spécifié.

```
Message: refresh_token must be non-null for Refresh Token Grant-type
```

Le jeton d'actualisation spécifié dans la demande est nul ou vide. Spécifiez une réponse d'appel active `refresh_token` reçue dans l'API Token.

ThrottlingException

Vous pouvez recevoir l'exception suivante si l'API est appelée à un taux supérieur au quota autorisé.

```
ThrottlingException
HTTP Status Code: 429
```

`ListActionableInsightsListMeetingInsights`, et **`PutFeedback`** erreurs

ValidationException

L'exception suivante peut s'afficher si l'un des paramètres de l'API ne satisfait pas à la contrainte définie dans les spécifications de l'API.

```
ValidationException
HTTP Status Code: 400
```

ThrottlingException

Vous pouvez recevoir l'exception suivante si l'API est appelée à un taux supérieur au quota autorisé.

```
ThrottlingException
HTTP Status Code: 429
```

Mise en route AppFabric pour la productivité (version préliminaire) pour les utilisateurs finaux

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Cette section est destinée aux utilisateurs finaux d'applications SaaS qui souhaitent améliorer la productivité (version préliminaire) afin AWS AppFabric d'améliorer la gestion des tâches et l'efficacité de leurs flux de travail. Suivez ces étapes pour connecter vos applications et autoriser AppFabric la diffusion d'informations croisées entre applications et vous aider à effectuer des actions (telles que l'envoi d'un e-mail ou la planification d'une réunion) à partir de vos applications préférées. Vous pouvez connecter des applications telles queAsana,,Atlassian Jira Suite,,Google Workspace,Microsoft 365,Miro, SlackSmartsheet, et bien d'autres encore. Une fois que vous avez autorisé l'accès AppFabric à votre contenu, AppFabric vous bénéficiez d'informations et d'actions inter-applications directement dans vos applications préférées, ce qui vous permet de travailler plus efficacement et de respecter vos flux de travail actuels.

AppFabric pour la productivité, utilise une IA générative alimentée par Amazon Bedrock. AppFabric ne générera des informations et des actions qu'après avoir reçu votre autorisation explicite. Vous autorisez chaque application individuelle à garder le contrôle total du contenu utilisé. AppFabric n'utilisera pas vos données pour entraîner ou améliorer les grands modèles linguistiques sous-jacents utilisés pour générer des informations. Pour plus d'informations, consultez les FAQ d'Amazon Bedrock.

Rubriques

Prérequis

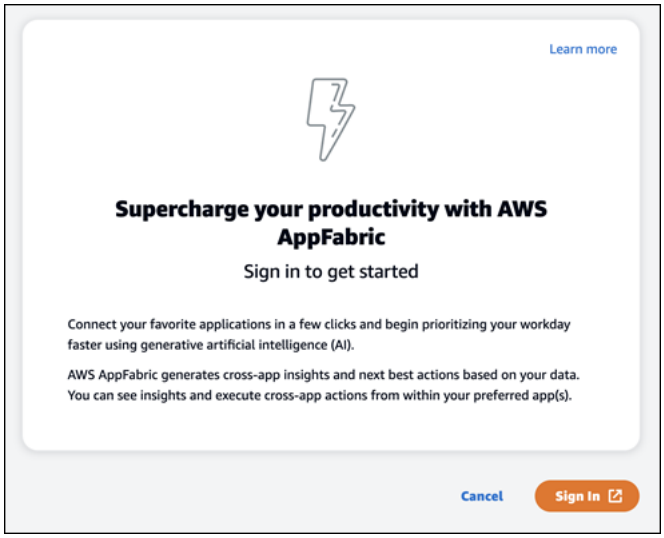
Avant de commencer, assurez-vous que vous disposez des éléments suivants :

- Informations d'identification auxquelles vous connecter AppFabric : pour commencer à utiliser à des AppFabric fins de productivité, vous aurez besoin d'informations d'identification fédérées (nom d'utilisateur et mot de passe) pour l'un des fournisseurs suivants :Asana, Google WorkspaceMicrosoft 365, ou. Slack La connexion à nous AppFabric permet de vous identifier en tant qu'utilisateur dans chaque application que vous activez AppFabric pour des raisons de productivité. Une fois connecté, vous pouvez connecter vos applications pour commencer à générer des informations.
- Informations d'identification pour connecter vos applications : les informations et actions inter-applications ne sont générées que sur la base des applications que vous autorisez. Vous aurez besoin d'informations d'identification (nom d'utilisateur et mot de passe) pour chacune des applications que vous souhaitez autoriser. Les applications prises en charge incluent Asana Atlassian Jira SuiteGoogle Workspace,Microsoft 365,Miro,Slack, etSmartsheet.

Étape 1. Connectez-vous à AppFabric

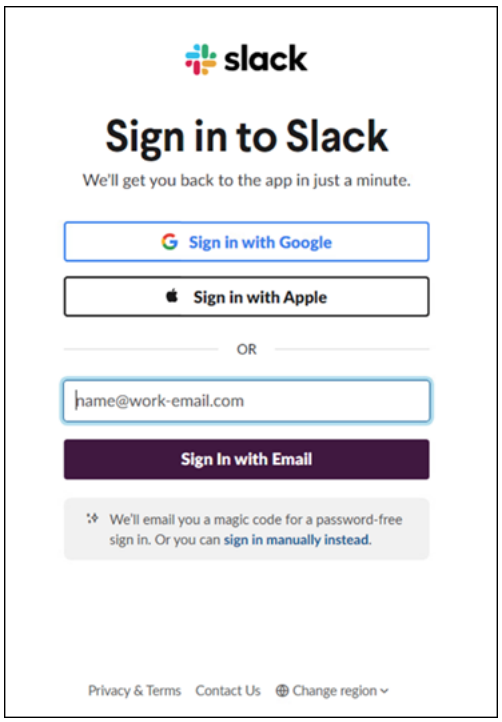
Connectez les applications AppFabric pour intégrer votre contenu et vos informations directement dans vos applications préférées.

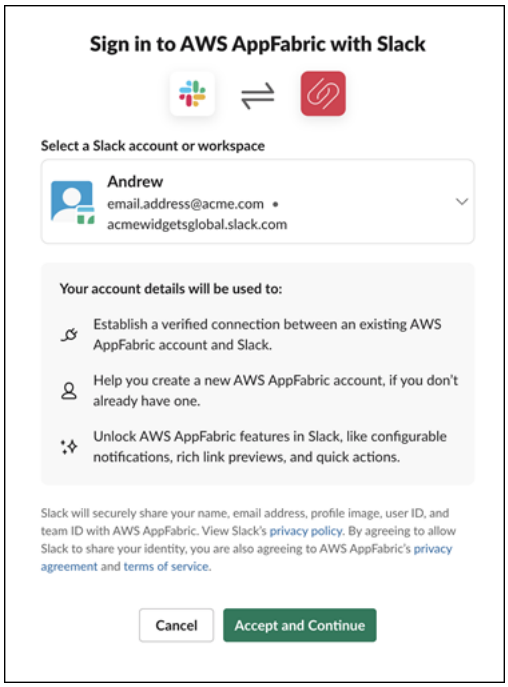
1. Chaque application sera utilisée AppFabric pour améliorer la productivité de différentes manières afin de vous offrir des expériences applicatives plus riches. De ce fait, chaque application aura un point d'entrée différent AppFabric pour accéder à la page d'accueil dédiée à la productivité ci-dessous. La page d'accueil définit le contexte du processus à activer AppFabric et vous invite d'abord à vous connecter. Toutes les applications que vous souhaitez activer AppFabric accèderont à cet écran.



2. Connectez-vous à l'aide des informations d'identification de l'un de ces fournisseurs : AsanaGoogle Workspace,Microsoft 365, ouSlack. Pour une expérience optimale, nous vous recommandons de vous connecter en utilisant le même fournisseur pour chaque application que vous activez AppFabric . Par exemple, si vous choisissez les informations d'identification Google Workspace dans App1, nous vous recommandons de choisir Google Workspace dans App2, ainsi que chaque fois que vous devez vous reconnecter. Si vous vous connectez auprès d'un autre fournisseur, vous devez recommencer le processus de connexion des applications.

3. Si vous y êtes invité, entrez vos informations de connexion et acceptez de vous connecter AppFabric depuis ce fournisseur.

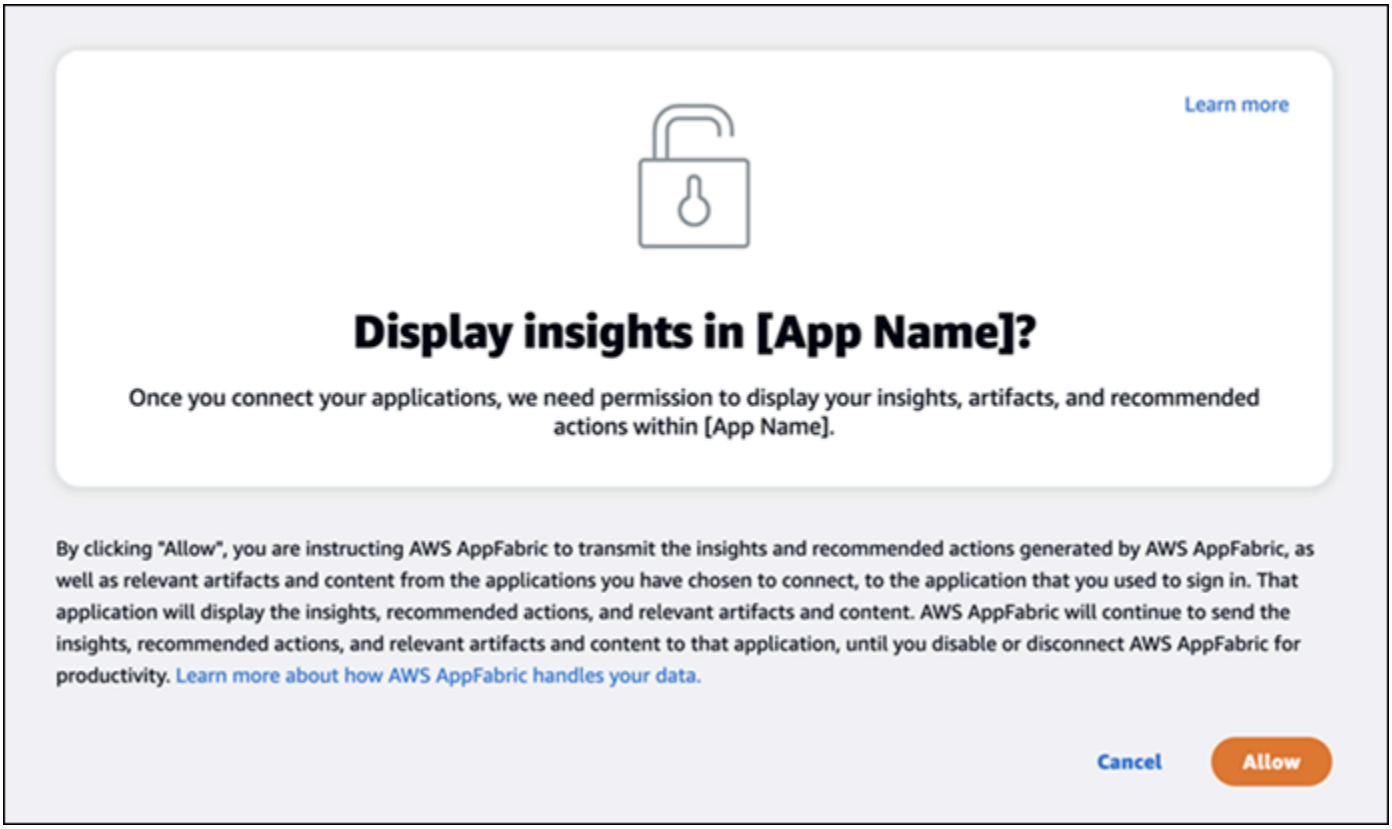




Étape 2. Donnez votre accord pour que l'application affiche des informations

Une fois connecté, une page de consentement s' AppFabric affichera vous demandant si vous autorisez l'affichage AppFabric d'informations et d'actions inter-applications dans l'application dans laquelle vous activez AppFabric la productivité. Par exemple, autorisez-vous AppFabric à prendre

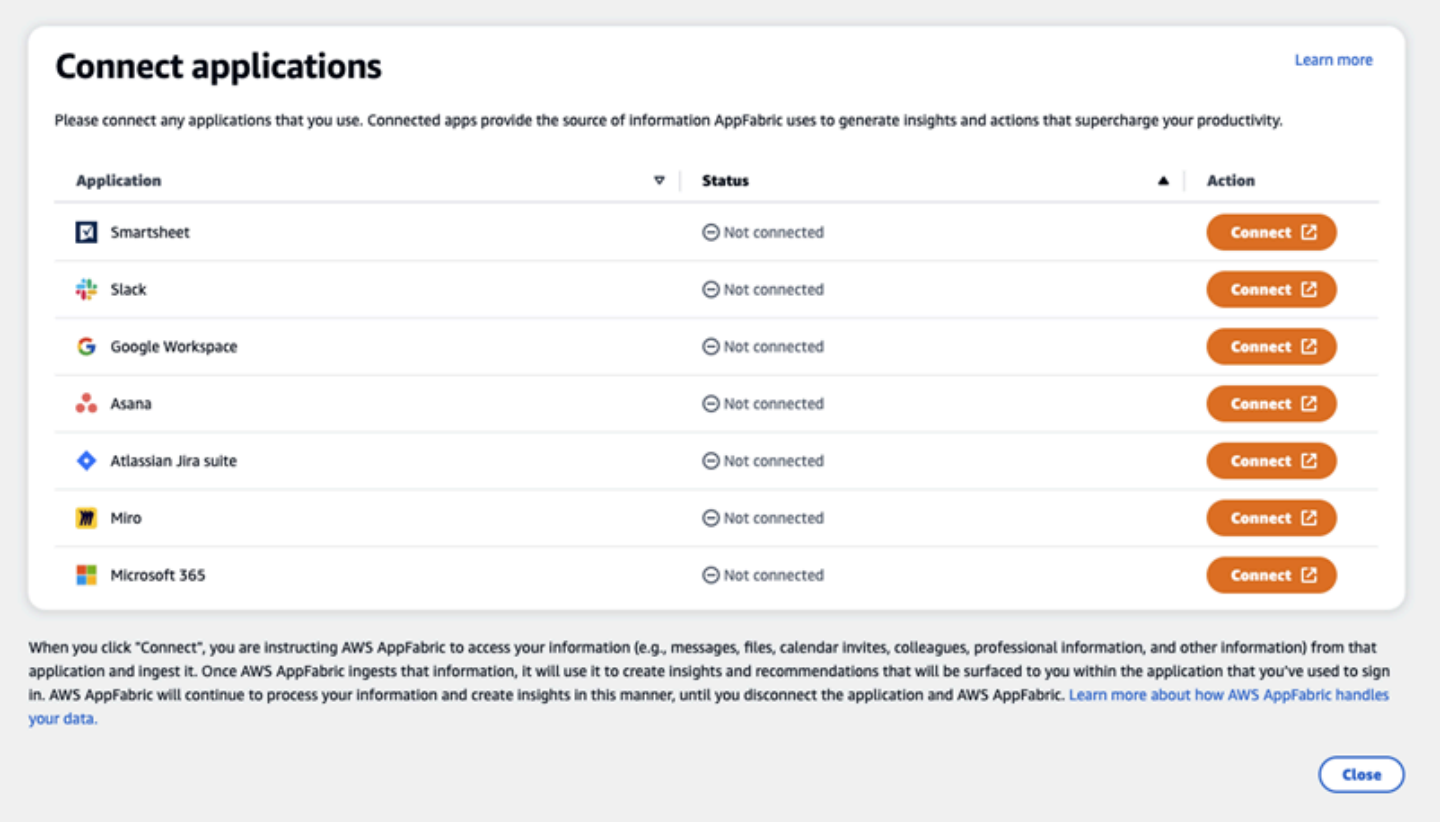
vos Google Workspace e-mails et les événements de votre calendrier et à les afficherAsana. Vous ne devez effectuer cette étape de consentement qu'une seule fois par application que vous activez AppFabric .



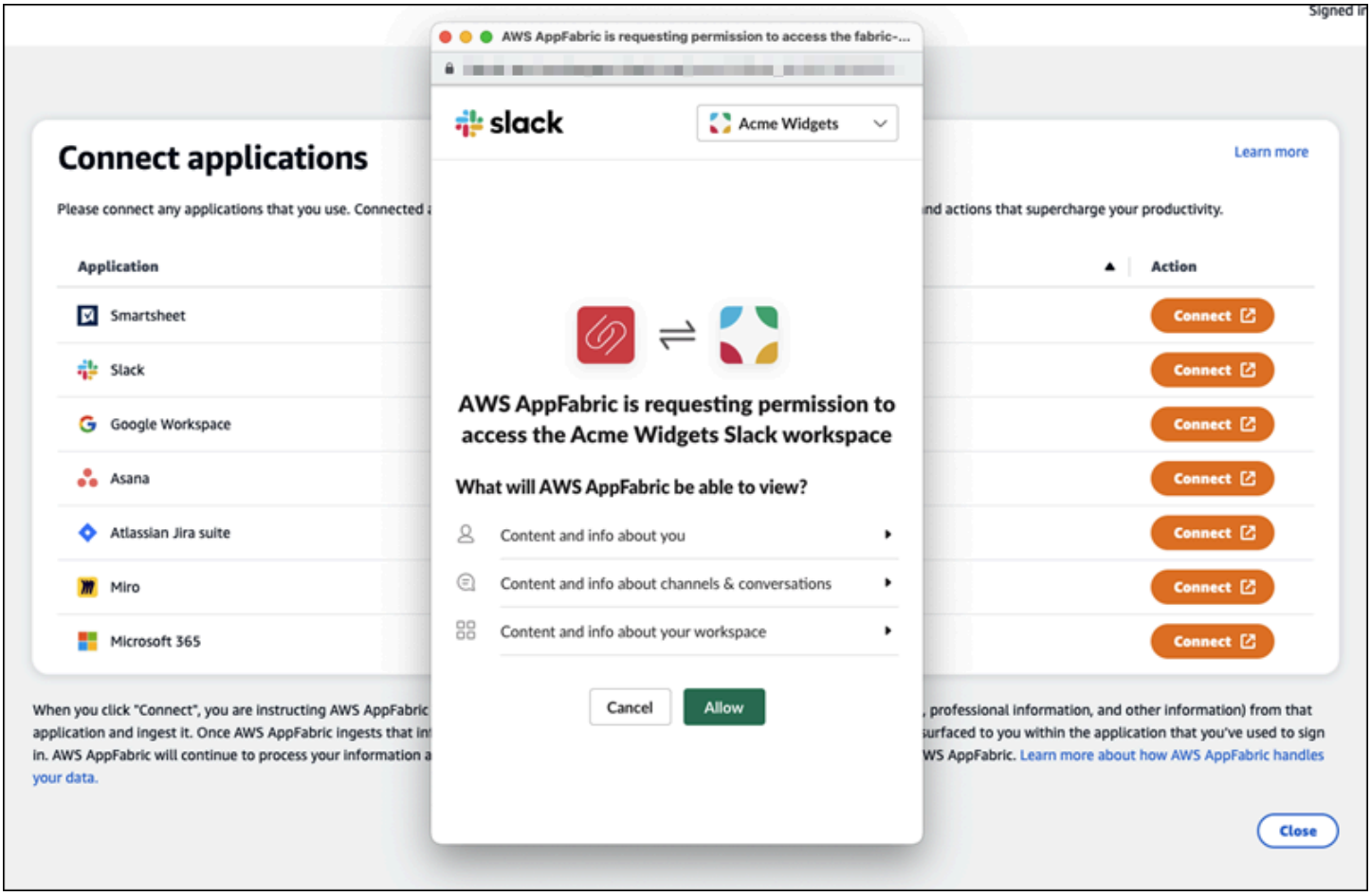
Étape 3. Connectez vos applications pour générer des informations et des actions

Une fois que vous avez rempli la page de consentement, vous êtes redirigé vers la page des applications Connect où vous pouvez connecter, déconnecter ou reconnecter des applications individuelles qui sont finalement utilisées pour générer des informations et des actions entre applications. Dans la plupart des cas, après vous être connecté et avoir donné votre accord, vous continuerez à utiliser cette page pour gérer vos applications connectées.

Pour connecter une application, cliquez sur le bouton Connect situé à côté de l'application que vous utilisez.



Vous devrez fournir vos informations de connexion à l'application et AppFabric autoriser l'accès à vos données pour générer des informations et effectuer des actions.

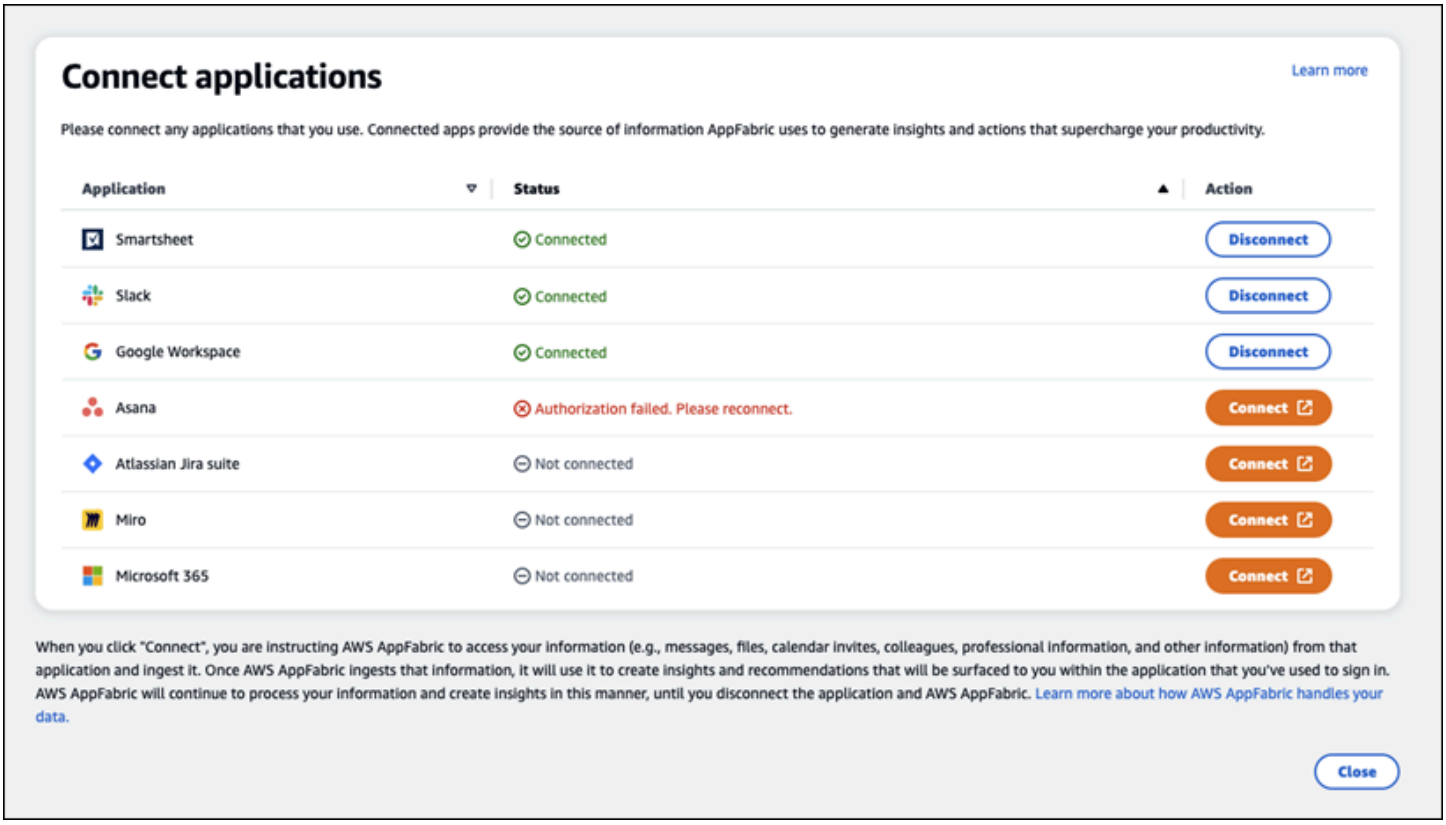


Une fois que vous avez connecté une application avec succès, le statut de cette application passe de « Non connecté » à « Connecté ». Rappel : vous devez effectuer cette étape d'autorisation pour chaque application que vous souhaitez utiliser pour générer des informations et des actions.

Une fois que vous avez connecté une application, elle n'est pas connectée pour toujours. Vous devrez régulièrement reconnecter les applications. Nous faisons cela pour nous assurer que nous avons toujours votre autorisation pour générer des informations.

Les statuts possibles des applications sont les suivants :

- Connecté : AppFabric est autorisé et génère des informations à l'aide de vos données à partir de cette application.
- Non connecté : ne génère AppFabric pas d'informations à partir des données de cette application. Vous pouvez vous connecter pour commencer à générer des informations.
- L'autorisation a échoué. Veuillez vous reconnecter. - Il peut y avoir un échec d'autorisation avec une application spécifique. Si cette erreur s'affiche, essayez de reconnecter votre application à l'aide du bouton Connect.



La configuration est terminée et vous pouvez retourner à votre application. Au moins quelques heures peuvent être nécessaires pour commencer à obtenir des informations au sein de vos applications.

Le cas échéant, vous pouvez revenir à cette page pour gérer vos applications connectées. Si vous choisissez de déconnecter une application, vous AppFabric cesserez d'utiliser les données de cette application ou de collecter de nouvelles données pour générer de nouvelles informations. Les données des applications déconnectées seront automatiquement supprimées dans les 7 jours si vous choisissez de ne pas reconnecter l'application dans ce délai.

Étape 4 : Commencez à obtenir des informations et à exécuter des actions inter-applications dans votre application

Une fois que vous aurez connecté vos applications AppFabric, vous aurez accès à des informations précieuses et pourrez effectuer des actions inter-applications directement depuis votre application préférée. Remarque : cette fonctionnalité n'est pas garantie dans chaque application et dépend entièrement des fonctionnalités AppFabric de productivité que le développeur de l'application a choisi d'activer.

Informations croisées entre les applications

AppFabric for productivity propose deux types d'informations :

- Informations exploitables : AppFabric analyse les informations contenues dans vos e-mails, les événements de votre calendrier, vos tâches et vos messages sur l'ensemble de vos applications connectées et génère des informations clés qu'il peut être important de prioriser. En outre, AppFabric peut générer des actions recommandées (telles que l'envoi d'un e-mail, la planification d'une réunion et la création d'une tâche) que vous pouvez modifier et exécuter tout en restant dans votre application préférée. Par exemple, vous pouvez recevoir un message indiquant qu'il y a une escalade de clientèle à gérer et une suggestion d'action suivante pour planifier un rendez-vous avec votre client.
- Informations sur la préparation des réunions : cette fonctionnalité vous aide à préparer au mieux les réunions à venir. AppFabric analysera vos prochaines réunions et générera un résumé concis de l'objectif de la réunion. En outre, il fera apparaître des artefacts pertinents (tels que des e-mails, des messages et des tâches) provenant de vos applications connectées, qui vous seront utiles pour vous aider à préparer efficacement la réunion sans avoir à passer d'une application à l'autre pour rechercher du contenu.

Actions entre applications

Pour certaines informations, cela AppFabric peut également générer des actions recommandées telles que l'envoi d'un e-mail, la planification d'une réunion ou la création d'une tâche. Lorsque vous générez des actions, vous AppFabric pouvez préremplir certains champs en fonction du contenu et du contexte de vos applications connectées. Par exemple, AppFabric peut générer une réponse par e-mail ou un nom de tâche suggéré en fonction des informations. Lorsque vous cliquez sur une action suggérée, vous êtes redirigé vers une AppFabric interface utilisateur personnalisée dans laquelle vous pouvez modifier le contenu prérempli avant d'exécuter l'action. AppFabric n'exécutera pas d'actions sans l'avis de l'utilisateur et sans l'intervention préalable de l'utilisateur, car l'IA générative et les grands modèles linguistiques sous-jacents (LLM) peuvent halluciner de temps à autre.

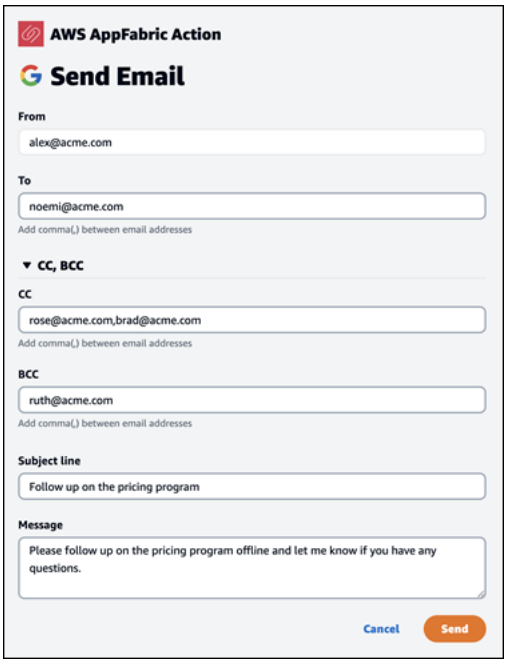
> **Note**
>
> Vous avez la responsabilité de valider et de confirmer les résultats du AppFabric LLM. AppFabric ne garantit pas l'exactitude ou la qualité de ses sorties LLM. Pour plus d'informations, consultez la section Politique en matière d'IA AWS responsable.

Créez des e-mails (Google Workspace,Microsoft 365)

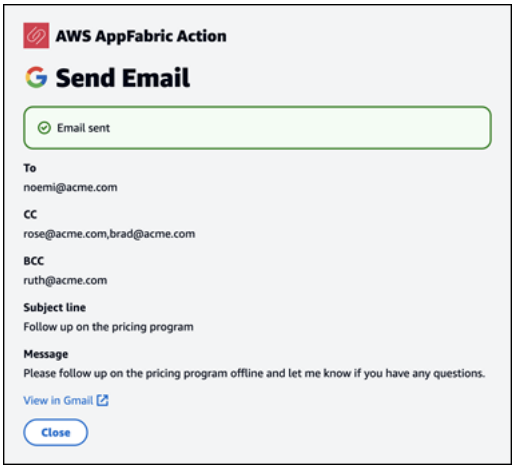
AppFabric vous permet de modifier et d'envoyer un e-mail depuis votre application préférée. Nous prenons en charge les champs de courrier électronique de base, notamment les champs From, To, Cc/Bcc, la ligne d'objet de l'e-mail et le corps du message. AppFabric peut générer du contenu dans ces champs pour vous aider à réduire le temps nécessaire à l'exécution de la tâche. Une fois que vous avez terminé de modifier l'e-mail, choisissez Envoyer pour envoyer l'e-mail.

Les champs suivants sont obligatoires pour envoyer un e-mail :

- Au moins un des e-mails des destinataires (To, CC et BCC) est requis et doit être une adresse e-mail valide.
- Ligne d'objet et champs de message.



Une fois l'e-mail envoyé, vous verrez une confirmation indiquant qu'il a été envoyé. De plus, vous verrez un lien permettant de consulter l'e-mail dans l'application désignée. Vous pouvez utiliser ce lien pour accéder rapidement à l'application et vérifier que l'e-mail a bien été envoyé.

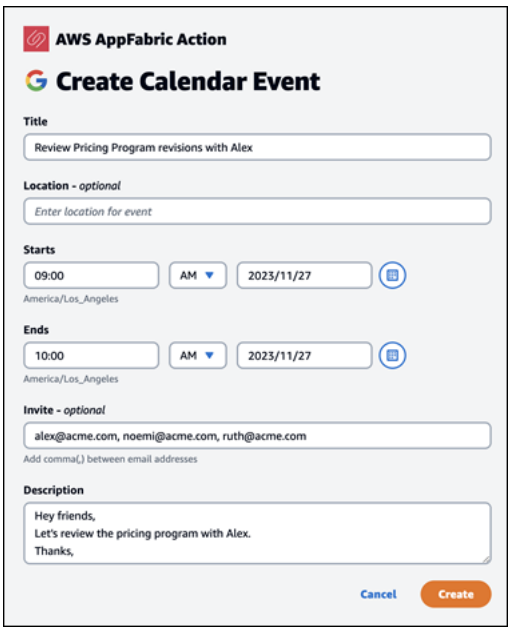


Créer des événements de calendrier (Google Workspace,Microsoft 365)

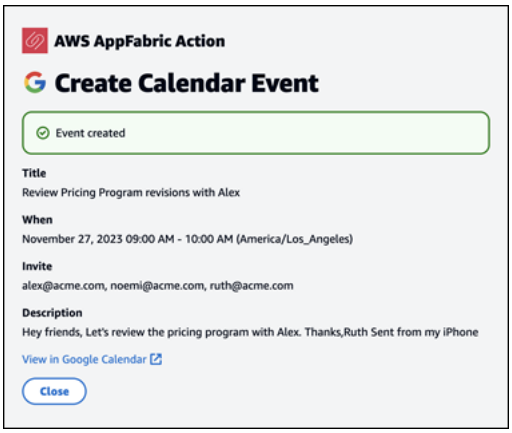
AppFabric vous permet de modifier et de créer un événement de calendrier depuis votre application préférée. Nous prenons en charge les champs d'événements de base du calendrier, notamment le titre de l'événement, le lieu, l'heure et la date de début/fin, la liste des invités et les détails de l'événement. AppFabric peut générer du contenu dans ces champs pour vous aider à réduire le temps nécessaire à l'exécution de la tâche. Une fois que vous avez terminé de modifier l'événement du calendrier, choisissez Créer pour créer l'événement.

Les champs suivants sont obligatoires pour créer un événement de calendrier :

- Champs de titre, de début, de fin et de description.
- L'heure et la date de début ne doivent pas être antérieures à l'heure et la date de fin.
- Le champ d'invitation est facultatif, mais nécessite des adresses e-mail valides si elles sont fournies.



Une fois l'événement du calendrier envoyé, vous verrez une confirmation indiquant que l'événement a été créé. De plus, vous verrez un lien vous permettant de consulter l'événement dans l'application prévue à cet effet. Vous pouvez utiliser ce lien pour accéder rapidement à l'application et vérifier que l'événement a été créé.

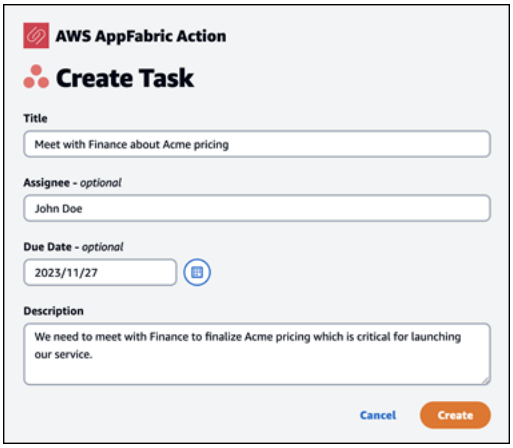


Créer des tâches (Asana)

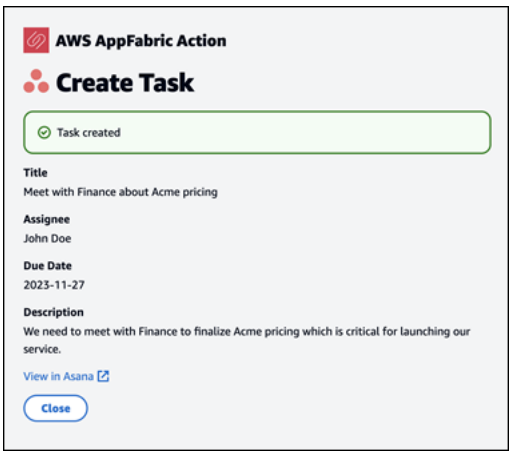
AppFabric vous permet de modifier et de créer une tâche Asana depuis votre application préférée. Nous prenons en charge les champs de tâches de base tels que le nom de la tâche, le propriétaire de la tâche, la date d'échéance et la description de la tâche. AppFabric peut générer du contenu dans ces champs afin de vous aider à réduire le temps de création de la tâche. Une fois que vous avez terminé de modifier la tâche, choisissez Créer pour créer la tâche. Les tâches sont créées dans l'Asanaespace de travail, le projet ou la tâche applicable, comme suggéré par le LLM.

Les champs suivants sont obligatoires pour créer une Asana tâche :

- Champs de titre et de description.
- L'adresse e-mail du destinataire doit être valide en cas de modification.



Une fois la tâche créée, vous verrez une confirmation indiquant qu'elle a été créée dansAsana. En outre, vous verrez un lien permettant d'afficher la tâcheAsana. Vous pouvez utiliser ce lien pour accéder rapidement à l'application afin de vérifier que la tâche a été créée, ou pour la déplacer vers l'Asanaespace de travail, le projet ou la tâche appropriés.



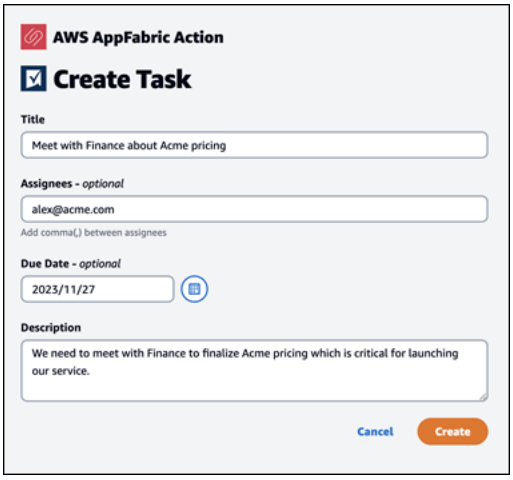
Créer des tâches (Smartsheet)

AppFabric vous permet de modifier et de créer une tâche Smartsheet depuis votre application préférée. Nous prenons en charge les champs de tâches de base tels que le nom de la tâche, le propriétaire de la tâche, la date d'échéance et la description de la tâche. AppFabric peut générer du contenu dans ces champs afin de vous aider à réduire le temps de création de la tâche. Une fois que vous avez terminé de modifier la tâche, choisissez Créer pour créer la tâche. Pour les Smartsheet tâches, AppFabric créera une nouvelle Smartsheet feuille privée et renseignera toutes les tâches

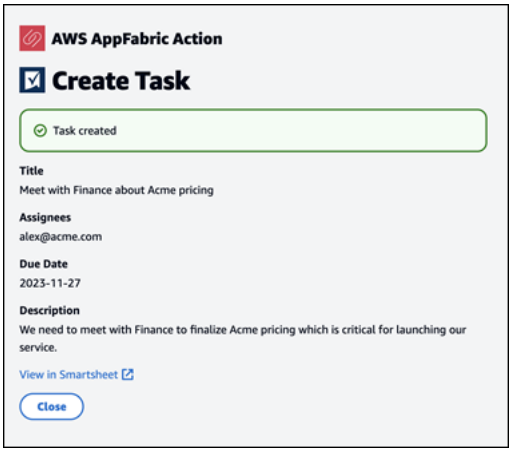
créées. Cela permet de centraliser les actions AppFabric générées en un seul endroit de manière structurée.

Les champs suivants sont obligatoires pour créer une Smartsheet tâche :

- Champs de titre et de description.
- L'adresse e-mail du destinataire doit être valide si elle est fournie.



Une fois la tâche créée, vous verrez une confirmation indiquant qu'elle a été créée dansSmartsheet. En outre, vous verrez un lien permettant d'afficher la tâcheSmartsheet. Vous pouvez utiliser ce lien pour accéder rapidement à l'application afin d'afficher la tâche dans la Smartsheet feuille créée. Toutes les Smartsheet tâches futures seront renseignées dans cette feuille. Si la feuille est supprimée, AppFabric il en créera une nouvelle.



À l'attention des administrateurs informatiques et de sécurité : gestion de l'accès aux fonctionnalités à AppFabric des fins de productivité (version préliminaire)

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Le portail utilisateur AppFabric pour la productivité est accessible au public à tous les utilisateurs d'applications SaaS qui ont intégré AppFabric les fonctionnalités de productivité (version préliminaire). Si vous êtes un administrateur informatique qui souhaite gérer l'accès à ces fonctionnalités d'IA générative au sein de votre organisation, envisagez les options suivantes :

- Restreindre la connexion au fournisseur d'identité (IdP) : vous pouvez bloquer l'accès à la connexion via votre fournisseur d'identité pour contrôler l'accès des utilisateurs aux fonctionnalités génératives de l'IA.
- Désactiver OAuth pour des applications spécifiques : implémentez des restrictions en aval en désactivant OAuth. Cette action empêche les utilisateurs de connecter des applications nécessitant une authentification OAuth à l'espace de travail de l'entreprise.

Résolution des problèmes

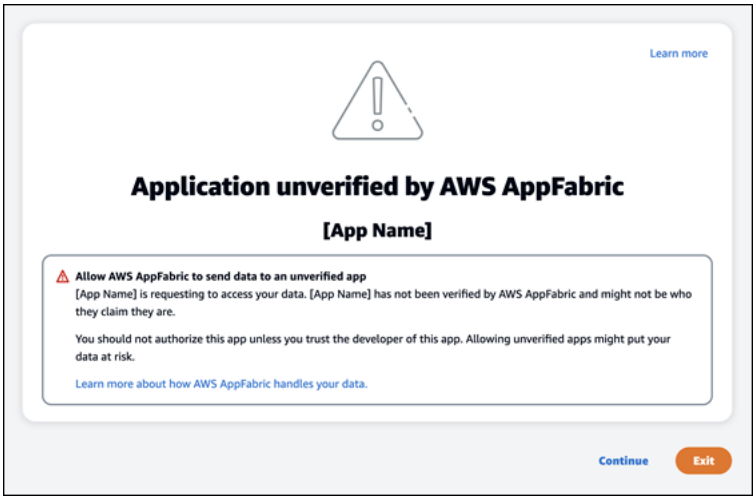
La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Cette section décrit les erreurs courantes et les solutions de résolution des problèmes liés AppFabric à la productivité.

Candidature non vérifiée

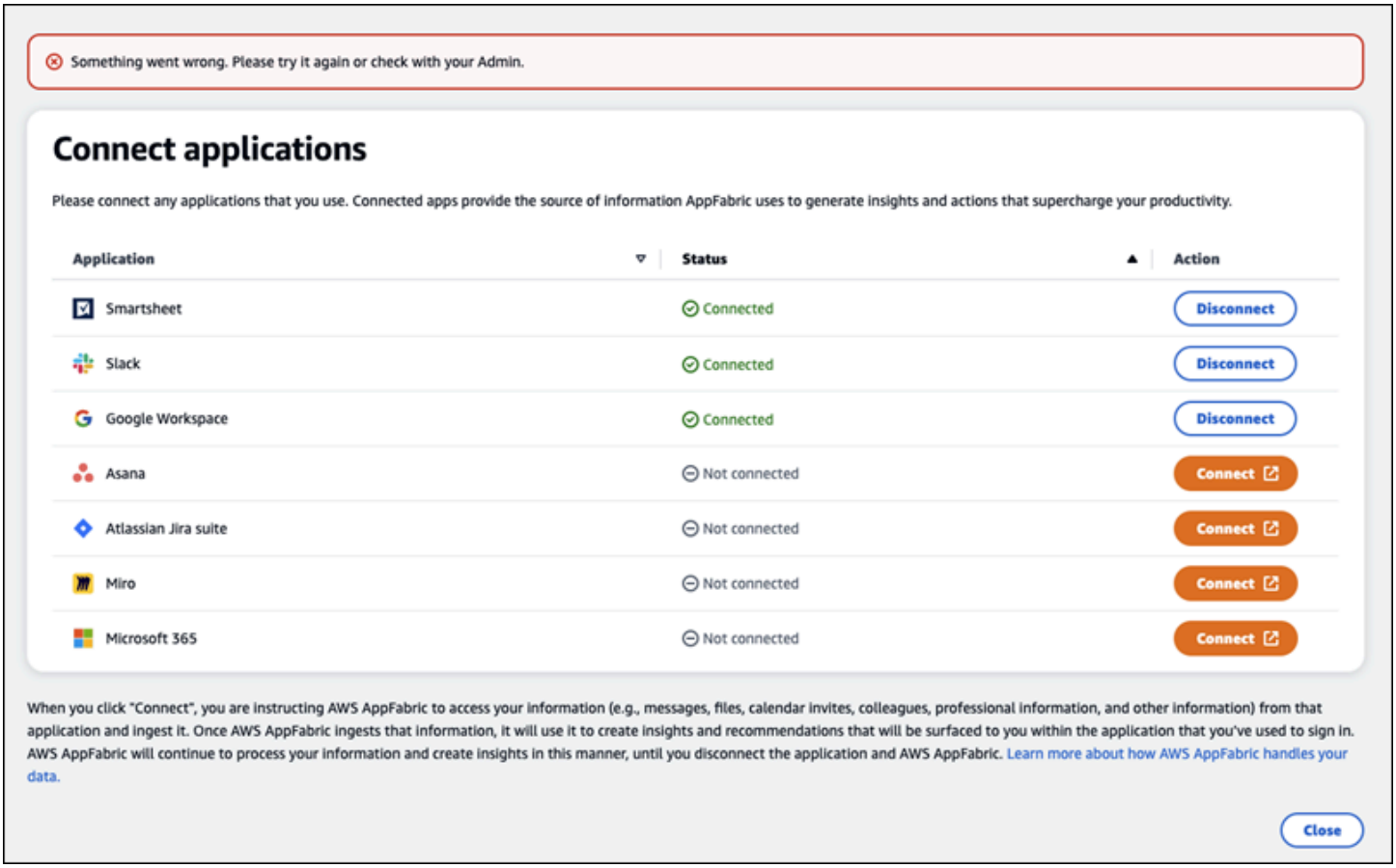
Les applications dont AppFabric la productivité permet d'enrichir leur expérience applicative seront soumises à un processus de vérification avant de lancer leurs fonctionnalités aux utilisateurs finaux. Si vous voyez apparaître une bannière « non vérifiée » lorsque vous essayez de vous connecter AppFabric, cela signifie que l'application n'a pas été soumise au processus AppFabric de vérification qui confirme l'identité du développeur de l'application et l'exactitude des informations d'enregistrement de l'application. Toutes les applications commencent comme non vérifiées et ne deviennent vérifiées que lorsque le processus de vérification est terminé.

Soyez prudent lorsque vous utilisez une application non vérifiée. Si vous n'êtes pas sûr des développeurs de l'application, vous pouvez attendre que l'application atteigne le statut vérifié avant de continuer.



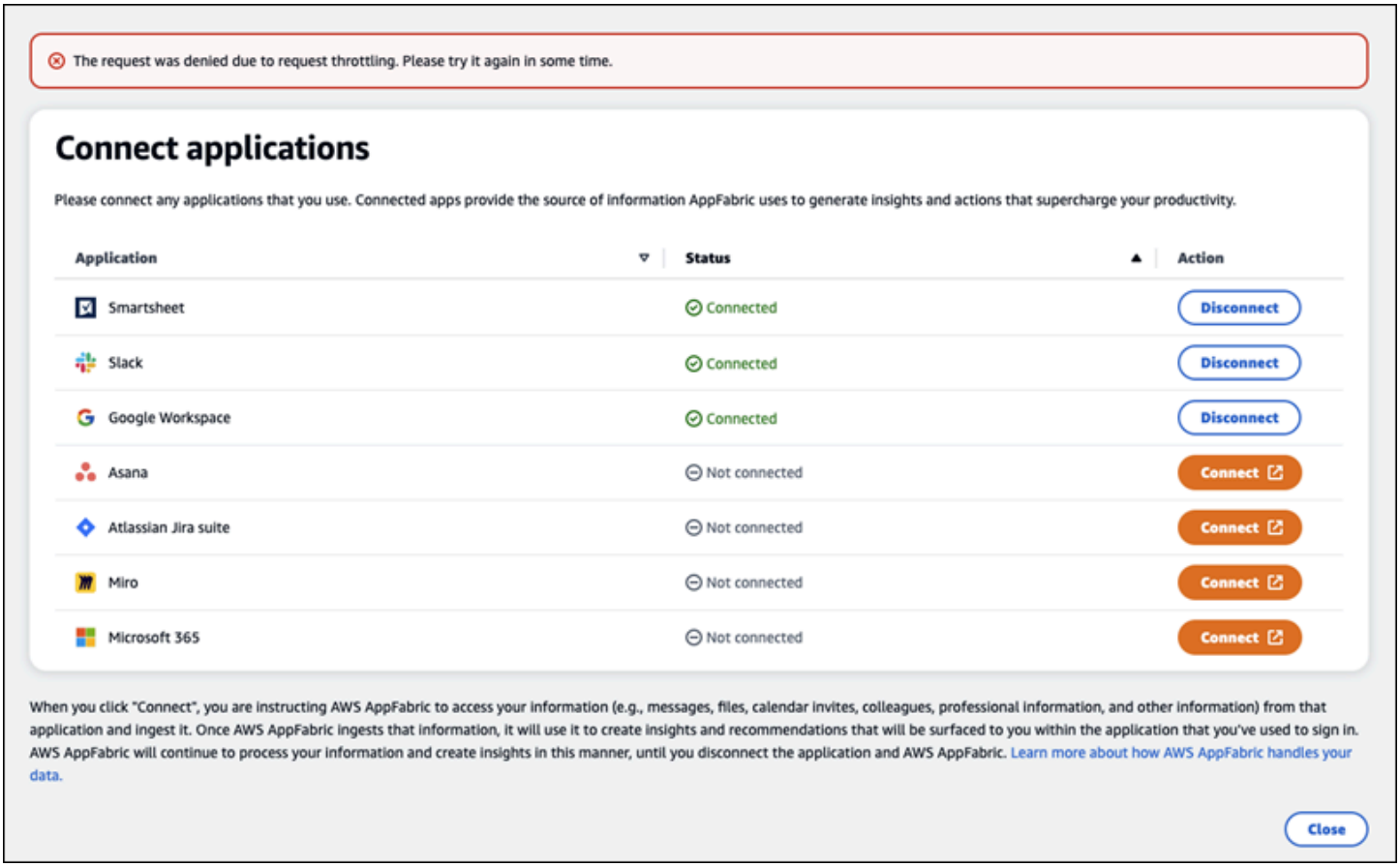
Quelque chose s'est mal passé. Réessayez ou contactez votre administrateur (**`InternalServerException`**)

Ce message peut s'afficher lorsque le portail AppFabric utilisateur ne répertorie pas les applications ou déconnecte une application en raison d'une erreur, d'une exception ou d'un échec inconnu. Réessayez ultérieurement.



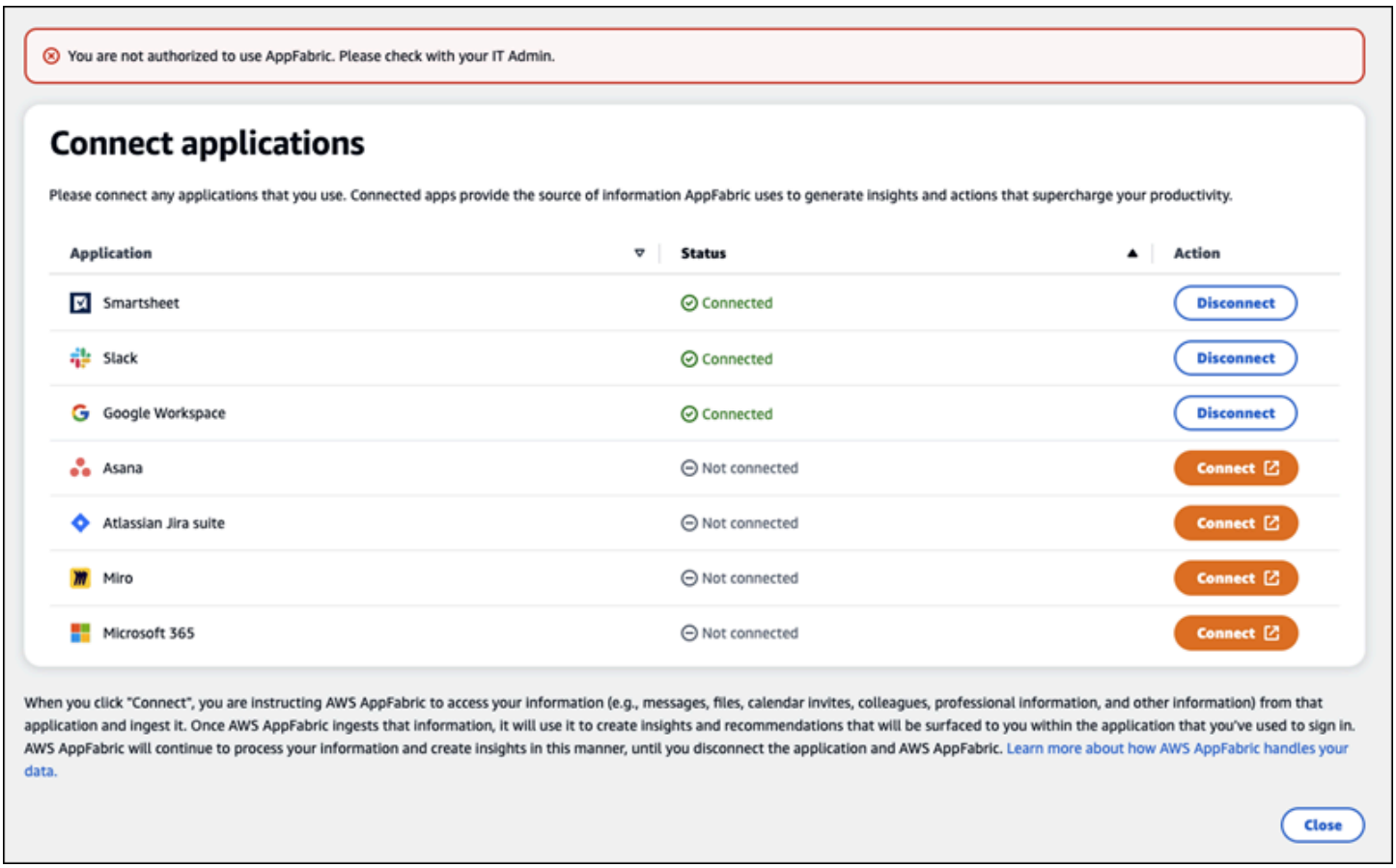
La demande a été refusée suite à une limitation des demandes. Veuillez réessayer dans quelques temps (**`ThrottlingException`**)

Ce message peut s'afficher lorsque le portail AppFabric utilisateur ne répertorie pas les applications ou déconnecte une application en raison d'un problème de régulation. Réessayez ultérieurement.



Vous n'êtes pas autorisé à utiliser AppFabric. Veuillez vous AppFabric reconnecter (**`AccessDeniedException`**)

Ce message peut s'afficher lorsque le portail AppFabric utilisateur ne répertorie pas les applications ou déconnecte une application en raison d'une exception de refus d'accès. Connectez-vous à AppFabric nouveau à.



AppFabric API de productivité

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Cette section fournit les opérations d'API, les types de données et les erreurs courantes pour les fonctionnalités de AWS AppFabric productivité.

> **Note**
>
> Pour toutes les autres AppFabric API, consultez la référence des AWS AppFabric API.

Rubriques

- Actions
- Types de données

- Erreurs courantes

Actions

> La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Les actions suivantes sont prises en charge pour les fonctionnalités de AppFabric productivité.

Pour toutes les autres actions d' AppFabric API, consultez les actions AWS AppFabric d'API.

Rubriques

- Autoriser
- CreateAppClient
- DeleteAppClient
- GetAppClient
- ListActionableInsights
- ListAppClients
- ListMeetingInsights
- PutFeedback
- Jeton
- UpdateAppClient

Autoriser

> La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Autorise un AppClient.

Rubriques

- Corps de la demande

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Paramètre	Description
ID du client de l'application	L'ID du AppClient à autoriser.
redirect_uri	L'URI vers lequel rediriger les utilisateurs finaux après autorisation.
state	Une valeur unique pour maintenir l'état entre la demande et le rappel.

CreateAppClient

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Crée un AppClient.

Rubriques

- Corps de la demande
- Éléments de réponse

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Paramètre	Description
Nom de l'application	Nom de l'application. Type : chaîne Contraintes de longueur : longueur minimum de 1. Longueur maximale de 255.

Paramètre	Description
	Obligatoire : oui
ClientToken	Spécifie un identifiant unique distinguant majuscules et minuscules que vous fournissez pour garantir l'idempuissance de la demande. Cela vous permet de réessayer la demande en toute sécurité sans effectuer accidentellement la même opération une deuxième fois. Pour transmettre la même valeur à un appel ultérieur à une opération, vous devez également transmettre la même valeur pour tous les autres paramètres. Nous vous recommandons d'utiliser une valeur de type UUID. Si vous ne fournissez pas cette valeur, il en AWS génère une au hasard pour vous. Si vous réessayez l'opération avec les mêmes paramètre `sClientToken` , mais avec des paramètres différents, la nouvelle tentative échoue avec une `IdempotentParameterMismatch` erreur. Type : chaîne Modèle : `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatoire : non

Paramètre	Description
customerManagedKeyIdentifiant	L'ARN du clé gérée par le client produit généré par AWS Key Management Service. La clé est utilisée pour chiffrer les données. Si aucune clé n'est spécifiée, une Clé gérée par AWS est utilisée. Carte des paires clé-valeur de la balise ou des balises à attribuer à la ressource. Pour plus d'informations sur Clés détenues par AWS les clés gérées par le client, consultez la section Clés et AWS clés client dans le guide du AWS Key Management Service développeur. Type : chaîne Contraintes de longueur : longueur minimum de 1. Longueur maximale de 1011. Modèle : `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatoire : non
description	Description de l'application. Type : chaîne Obligatoire : oui
URL de l'icône	URL de l'icône ou du logo du AppClient. Type : chaîne Obligatoire : non

Paramètre	Description
URL de redirection	L'URI vers lequel rediriger les utilisateurs finaux après autorisation. Vous pouvez ajouter jusqu'à 5 URL de redirection. Par exemple, `https://localhost:8080` . Type : tableau de chaînes Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments. Contraintes de longueur : longueur minimum de 1. Longueur maximale de 2048. Modèle : `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` Obligatoire : oui
starterUserEmails	Adresses e-mail de démarrage pour les utilisateurs autorisés à recevoir des informations jusqu'à ce qu'elles soient vérifiées. AppClient Type : tableau de chaînes Membres du tableau : nombre fixe de 1 élément. Contraintes de longueur : longueur minimale de 0. Longueur maximale de 320. Modèle : `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Obligatoire : oui

Paramètre	Description
tags	Carte des paires clé-valeur de la balise ou des balises à attribuer à la ressource. Type : Tableau d'objets Tag Membres du tableau : nombre minimum de 0 élément. Nombre maximal de 50 éléments. Obligatoire : non

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 201.

Les données suivantes sont renvoyées au format JSON par le service.

Paramètre	Description
appClientSummary	Contient un résumé du AppClient. Type : objet AppClientSummary

DeleteAppClient

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Supprime un client d'application.

Rubriques

- Corps de la demande
- Éléments de réponse

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Paramètre	Description
appClientIdentifier	Le nom de ressource Amazon (ARN) ou l'identifiant unique universel (UUID) AppClient à utiliser pour la demande. Contraintes de longueur : longueur minimum de 1. Longueur maximale de 1011. Modèle : `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 204 avec un corps HTTP vide.

GetAppClient

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Renvoie des informations sur un AppClient.

Rubriques

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Paramètre	Description
appClientIdentifier	Le nom de ressource Amazon (ARN) ou l'identifiant unique universel (UUID) AppClient à utiliser pour la demande. Contraintes de longueur : longueur minimum de 1. Longueur maximale de 1011. Modèle : `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatoire : oui

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Paramètre	Description
Client de l'application	Contient des informations sur un AppClient. Type : objet AppClient

ListActionableInsights

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Répertorie les e-mails, tâches et autres mises à jour exploitables les plus importants.

Rubriques

- Corps de la demande
- Éléments de réponse

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Paramètre	Description
nextToken	S'il `nextToken` est renvoyé, d'autres résultats sont disponibles. La valeur de `nextToken` est un jeton de pagination unique pour chaque page. Réappelez en utilisant le jeton renvoyé pour récupérer la page suivante. Gardez tous les autres arguments inchangés. Chaque jeton de pagination expire au bout de 24 heures. L'utilisation d'un jeton de pagination expiré renverra une InvalidToken erreur HTTP 400.

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 201.

Les données suivantes sont renvoyées au format JSON par le service.

Paramètre	Description
ActionableInsightsList	Répertorie les informations exploitables, y compris le titre, la description, les actions et l'horodatage créé. Pour plus d'informations, consultez ActionableInsights.
nextToken	S'il `nextToken` est renvoyé, d'autres résultats sont disponibles. La valeur de `nextToken` est un jeton de pagination unique pour chaque page. Réappelez en utilisant le jeton renvoyé pour récupérer la page suivante. Gardez tous les autres arguments inchangés. Chaque jeton de pagination expire au bout de 24 heures. L'utilisation d'un jeton de pagination expiré renverra une InvalidToken erreur HTTP 400. Type : chaîne

ListAppClients

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Renvoie une liste de tous les éléments AppClients.

Rubriques

- Corps de la demande
- Éléments de réponse

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Paramètre	Description
maxResults	Le nombre maximum de résultats renvoyés par appel. Vous pouvez l'utiliser `nextToken` pour obtenir d'autres pages de résultats. Il ne s'agit que d'une limite supérieure. Le nombre réel de résultats renvoyés par appel peut être inférieur au maximum spécifié. Plage valide : valeur minimum de 1. Valeur maximale fixée à 100.
nextToken	S'il `nextToken` est renvoyé, d'autres résultats sont disponibles. La valeur de `nextToken` est un jeton de pagination unique pour chaque page. Réappelez en utilisant le jeton renvoyé pour récupérer la page suivante. Gardez tous les autres arguments inchangés. Chaque jeton de pagination expire au bout de 24 heures. L'utilisation d'un jeton de pagination expiré renverra une InvalidToken erreur HTTP 400.

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Paramètre	Description
appClientList	Contient une liste de AppClient résultats. Type : tableau d'objets AppClientSummary
nextToken	S'il `nextToken` est renvoyé, d'autres résultats sont disponibles. La valeur de `nextToken` est un jeton de pagination unique pour chaque page. Réappelez en utilisant le jeton renvoyé pour récupérer la page suivante. Gardez tous les autres arguments inchangés. Chaque jeton de pagination expire au bout de 24 heures. L'utilisation d'un jeton de pagination expiré renverra une InvalidToken erreur HTTP 400. Type : chaîne

ListMeetingInsights

> La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Répertorie les événements du calendrier actionnables les plus importants.

Rubriques

- Corps de la demande
- Éléments de réponse

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Paramètre	Description
nextToken	S'il `nextToken` est renvoyé, d'autres résultats sont disponibles. La valeur de `nextToken` est un jeton de pagination unique pour chaque page. Réappelez en utilisant le jeton renvoyé pour récupérer la page suivante. Gardez tous les autres arguments inchangés. Chaque jeton de pagination expire au bout de 24 heures. L'utilisation d'un jeton de pagination expiré renverra une InvalidToken erreur HTTP 400.

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 201.

Les données suivantes sont renvoyées au format JSON par le service.

Paramètre	Description
MeetingInsightList	Répertorie les informations exploitables sur les réunions. Pour plus d'informations, consultez MeetingInsights.
nextToken	S'il `nextToken` est renvoyé, d'autres résultats sont disponibles. La valeur de `nextToken` est un jeton de pagination unique pour chaque page. Réappelez en utilisant le jeton renvoyé pour récupérer la page suivante. Gardez tous les autres arguments inchangés. Chaque jeton de pagination expire au bout de 24 heures. L'utilisation d'un jeton de pagination expiré renverra une InvalidToken erreur HTTP 400. Type : chaîne

PutFeedback

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Permet aux utilisateurs de soumettre des commentaires pour une idée ou une action donnée.

Rubriques

- Corps de la demande
- Éléments de réponse

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Paramètre	Description
id	ID de l'objet pour lequel le commentaire est envoyé. Cela peut être le InsightId ou le ActionId.
Feedback pour	Type d'aperçu pour lequel le commentaire est soumis. Valeurs possibles : `ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION`
Évaluation des commentaires	Évaluation des commentaires de 1 à5. Plus la note est élevée, mieux c'est.

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 201 avec un corps HTTP vide.

Jeton

> La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Contient des informations permettant d' AppClients échanger un code d'autorisation contre un jeton d'accès.

Rubriques

- Corps de la demande

- Éléments de réponse

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Paramètre	Description
code	Le code d'autorisation reçu du point de terminaison d'autorisation. Type : chaîne Contraintes de longueur : longueur minimum de 1. Longueur maximale de 2048. Obligatoire : non
type de subvention	Type de subvention pour le jeton. Doit être `authorization_code` ou `refresh_token` . Type : chaîne Obligatoire : oui
ID du client de l'application	ID du AppClient. Type : chaîne Modèle : `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatoire : oui
redirect_uri	L'URI de redirection transmis au point de terminaison d'autorisation. Type : chaîne Obligatoire : non

Paramètre	Description
jeton de rafraîchissement	Le jeton d'actualisation reçu suite à la demande de jeton initiale. Type : chaîne Contraintes de longueur : longueur minimum de 1. Longueur maximum de 4096. Obligatoire : non

Éléments de réponse

Si l’action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Paramètre	Description
appfabric_user_id	L'ID de l'utilisateur pour le jeton. Ceci est renvoyé uniquement pour les demandes qui utilisent le type de `authorization_code` subvention. Type : chaîne
expirer_in	Le nombre de secondes avant l'expiration du jeton. Type : long
jeton de rafraîchissement	Le jeton d'actualisation à utiliser pour une demande ultérieure. Type : chaîne Contraintes de longueur : longueur minimum de 1. Longueur maximale de 2048.
token	Le jeton d'accès. Type : chaîne

Paramètre	Description
	Contraintes de longueur : longueur minimum de 1. Longueur maximale de 2048.
type_jeton	Type de jeton. Type : chaîne

UpdateAppClient

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Met à jour un AppClient.

Rubriques

- Corps de la demande
- Éléments de réponse

Corps de la demande

Cette demande accepte les données suivantes au format JSON.

Paramètre	Description
appClientIdentifier	Le nom de ressource Amazon (ARN) ou l'identifiant unique universel (UUID) AppClient à utiliser pour la demande. Contraintes de longueur : longueur minimum de 1. Longueur maximale de 1011. Modèle : `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatoire : oui

Paramètre	Description
URL de redirection	L'URI vers lequel rediriger les utilisateurs finaux après autorisation. Vous pouvez ajouter jusqu'à 5 URL de redirection. Par exemple, `https://localhost:8080` . Type : tableau de chaînes Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments. Contraintes de longueur : longueur minimum de 1. Longueur maximale de 2048. Modèle : `(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

Éléments de réponse

Si l'action aboutit, le service renvoie une réponse HTTP 200.

Les données suivantes sont renvoyées au format JSON par le service.

Paramètre	Description
Client de l'application	Contient des informations sur un AppClient. Type : objet AppClient

Types de données

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

L' AppFabric API contient plusieurs types de données utilisés par diverses actions. Cette section décrit en détail les types de données pour les fonctionnalités de AppFabric productivité.

Pour tous les autres types de données d' AppFabric API, consultez les types de données d'AWS AppFabric API.

> **Important**
>
> L'ordre de chaque élément dans une structure de type de données n'est pas garanti. Les candidatures ne doivent pas être soumises à un ordre particulier.

Rubriques

- ActionableInsights
- AppClient
- AppClientSummary
- MeetingInsights
- VerificationDetails

ActionableInsights

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modificat ion.

Contient un résumé des actions importantes et appropriées pour un utilisateur en fonction des e-mails, des invitations du calendrier, des messages et des tâches de son portefeuille d'applications. Les utilisateurs peuvent consulter des informations proactives provenant de l'ensemble de leurs applications pour les aider à mieux orienter leur journée. Ces informations justifient pourquoi un utilisateur doit s'intéresser au résumé des informations, ainsi que des références, telles que des liens intégrés, aux applications individuelles et aux artefacts qui ont généré les informations.

Paramètre	Description
ID d'Insight	L'identifiant unique de l'aperçu généré.
Contenu Insight	Cela renvoie un résumé de l'aperçu et des liens intégrés vers les artefacts utilisés pour générer l'aperçu.

Paramètre	Description
	Il s'agirait d'un contenu HTML contenant des liens intégrés (<a>balises).
Titre d'Insight	Titre de l'aperçu généré.
Créé à CreatedAt	Quand l'aperçu a été généré.
actions	Une liste d'actions recommandées pour les informations générées. L'objet action contient les paramètres suivants : • `actionId`— L'identifiant unique de l'action générée. • `actionIconUrl` — L'URL de l'icône de l'application dans laquelle il est suggéré d'exécuter l'action. • `actionTitle` — Le titre de l'action générée. • `actionUrl` — URL unique permettant à l'utilisateur final de visualiser et d'exécuter l'action dans AppFabric le portail utilisateur. Pour exécuter des actions, les applications ISV redirigeront les utilisateurs vers le portail AppFabric utilisateur (écran contextuel) à l'aide de cette URL. • `actionExecutionStatus` — Une énumération indiquant le statut de l'action. Les valeurs possibles sont : `EXECUTED | NOT_EXECUTED`

AppClient

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modificat ion.

Contient des informations sur un AppClient.

Paramètre	Description
Nom de l'application	Nom de l'application. Type : chaîne Obligatoire : oui
arn	Le nom de ressource Amazon (ARN) du AppClient. Type : chaîne Contraintes de longueur : longueur minimum de 1. Longueur maximale de 1011. Modèle : `arn:.+` Obligatoire : oui
description	Description de l'application. Type : chaîne Obligatoire : oui
URL de l'icône	URL de l'icône ou du logo du AppClient. Type : chaîne Obligatoire : non
URL de redirection	Les URL de redirection autorisées pour. AppClient Type : tableau de chaînes Membres du tableau : Nombre minimum de 1 élément. Nombre maximum de 5 éléments. Contraintes de longueur : longueur minimum de 1. Longueur maximale de 2048. Modèle : `(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

Paramètre	Description
	Obligatoire : oui
starterUserEmails	Adresses e-mail de démarrage pour les utilisateurs autorisés à recevoir des informations jusqu'à ce qu'elles soient vérifiées. AppClient Type : tableau de chaînes Membres du tableau : nombre fixe de 1 élément. Contraintes de longueur : longueur minimale de 0. Longueur maximale de 320. Modèle : `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Obligatoire : oui
Détails de vérification	Contient le statut et le motif de la AppClient vérification. Type : objet VerificationDetails Obligatoire : oui
customerManagedKeyArn	Le nom de ressource Amazon (ARN) du fichier clé gérée par le client généré par AWS Key Management Service pour le AppClient. Type : chaîne Contraintes de longueur : longueur minimum de 1. Longueur maximale de 1011. Modèle : `arn:.+` Obligatoire : non

Paramètre	Description
appClientId	ID du AppClient. Destiné à être utilisé dans les flux o-auth pour le client d'application. Type : chaîne Modèle : `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatoire : non

AppClientSummary

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Contient des informations sur un AppClient.

Paramètre	Description
arn	Le nom de ressource Amazon (ARN) du AppClient. Type : chaîne Contraintes de longueur : longueur minimum de 1. Longueur maximale de 1011. Modèle : `arn:.+` Obligatoire : oui
État de la vérification	État AppClient de la vérification. Type : chaîne Valeurs valides : `pending_verification | verified | rejected`

Paramètre	Description
	Obligatoire : oui
appClientId	ID du AppClient. Destiné à être utilisé dans les flux o-auth pour le client d'application. Type : chaîne Modèle : `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatoire : non

MeetingInsights

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Contient un résumé des 3 principales réunions ainsi que l'objectif de la réunion, les artefacts inter-applications associés et les activités liées aux tâches, aux e-mails, aux messages et aux événements du calendrier.

Paramètre	Description
ID d'Insight	L'identifiant unique de l'aperçu généré.
Contenu Insight	Description de l'aperçu mettant en évidence les détails sous forme de chaîne. Par exemple, pourquoi cette information est-elle importante ?
Titre d'Insight	Titre de l'aperçu généré.
Créé à CreatedAt	Quand l'aperçu a été généré.
Évènement du calendrier	Événement ou réunion important du calendrier sur lequel l'utilisateur doit se concentrer.

Paramètre	Description
	Objet d'événement du calendrier : • `startTime` — L'heure de début de l'événement. • `endTime`— L'heure de fin de l'événement. • `eventUrl`— L'URL de l'événement du calendrier sur l'application ISV.
resources	La liste contenant les autres ressources liées à la génération de l'aperçu. Objet de ressource : • `appName`— Le nom de l'application à laquelle appartient la ressource. • `resourceTitle` — Le titre de la ressource. • `resourceType` — Le type de ressource. Les valeurs possibles sont : `EMAIL | EVENT | MESSAGE | TASK` • `resourceUrl` — L'URL de la ressource dans l'application. • `appIconUrl` — URL de l'image de l'application à laquelle appartient la ressource.
nextToken	Le jeton de pagination pour récupérer le prochain ensemble d'informations. Il s'agit d'un champ facultatif qui, s'il est renvoyé nul, signifie qu'il n'y a plus d'informations à charger.

VerificationDetails

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Contient le statut et le motif de la AppClient vérification.

Paramètre	Description
État de la vérification	État AppClient de la vérification. Type : chaîne Valeurs valides : `pending_verification | verified | rejected` Obligatoire : oui
Motif du statut	La raison du statut de AppClient vérification. Type : chaîne Contraintes de longueur : Longueur minimum de 1. Longueur maximale de 1024. Obligatoire : non

Erreurs courantes

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Cette section répertorie les erreurs communes aux actions d'API relatives aux fonctionnalités de AWS AppFabric productivité.

Pour toutes les autres erreurs d'API AppFabric courantes, consultez Résolution des problèmes la section « Erreurs courantes d'AWS AppFabric API » dans la référence des AWS AppFabric API.

Nom de l'exception	Description
TokenException	La demande de jeton n'est pas valide. Code d'état HTTP : 400

Traitement des données

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

AppFabric prend des mesures pour stocker le contenu utilisateur individuellement, dans un compartiment Amazon S3 géré par et séparément AppFabric, ce qui nous permet de générer des informations spécifiques aux utilisateurs. Nous utilisons des mesures de protection raisonnables pour protéger votre contenu, qui peuvent inclure le chiffrement au repos et en transit. Nous avons configuré nos systèmes pour supprimer automatiquement le contenu client dans les 30 jours suivant son ingestion. AppFabric ne génère pas d'informations à l'aide d'artefacts de données auxquels l'utilisateur n'a plus accès. Par exemple, lorsqu'un utilisateur déconnecte une source de données (une application), AppFabric arrête de collecter des données depuis cette application et n'utilise aucun artefact persistant provenant des applications déconnectées pour générer des informations. AppFabricLes systèmes sont configurés pour supprimer ces données dans un délai de 30 jours.

AppFabric n'utilise pas le contenu utilisateur pour entraîner ou améliorer les grands modèles linguistiques sous-jacents utilisés pour générer des informations. Pour plus d'informations sur AppFabric la fonctionnalité d'IA générative, consultez les FAQ d'Amazon Bedrock.

Chiffrement au repos

AWS AppFabric prend en charge le chiffrement au repos, une fonctionnalité de chiffrement côté serveur qui chiffre de AppFabric manière transparente toutes les données relatives aux utilisateurs lorsqu'elles sont conservées sur le disque, et les déchiffre lorsque vous accédez aux données.

Chiffrement en transit

AppFabric sécurise tout le contenu en transit à l'aide de TLS 1.2 et signe les demandes d'API pour les AWS services avec AWS Signature Version 4.

Terminologie et concepts

Cette rubrique décrit la terminologie et les concepts clés AWS AppFabric pour vous aider à démarrer.

Bundle d'applications

Un bundle d' AppFabric applications stocke toutes vos autorisations et ingestions d' AppFabric applications (voir la définition des ingestions suivante). Vous pouvez créer un bundle d'applications Compte AWS par application Région AWS.

AppClient (également client d'application et client d'application)

Un OAuth AppClient pour l'application destinataire des données. Chaque application destinataire de données doit s'enregistrer et accéder AppClient aux AppFabric données. Un utilisateur développeur a besoin d'un AWS compte pour s'inscrire AppClient. Chaque AWS compte ne peut en enregistrer qu'un seul AppClient. AppFabric vendra des jetons d'accès en fonction de AppClient. AppClient contiendra des informations sur l'application destinataire des données qui accèdera aux AppFabric données par ce biais AppClient.

Autorisation de l'application

Une autorisation d'application donne AppFabric l'autorisation de se connecter et d'interagir avec vos applications. Il permet l'ingestion des journaux d'audit de vos applications, avec des informations d'identification OAuth (Open Authorization, une norme ouverte de délégation d'accès pour accorder l'accès aux applications) ou des jetons d'accès personnels (PAT). Vous pouvez configurer plusieurs autorisations d'applications (jusqu'à 50) par bundle d'applications. Cela permet d' AppFabric ingérer les journaux d'audit de plusieurs locataires d'applications, en répétant l'étape de création de l'autorisation de l'application selon les besoins de chaque locataire de l'application. Les informations d'identification partagées sont chiffrées à l'aide d'une clé Clé détenue par AWS ou d'une clé gérée par le client à partir du AWS Key Management Service (AWS KMS) et sont stockées dans AppFabric.

Ingestion

Une AppFabric ingestion utilise une autorisation d'application pour extraire les journaux d'audit d'une application via les API publiques de l'application. Il fournit ensuite les journaux d'audit à une ou plusieurs destinations (jusqu'à cinq).

ID de client

Lorsque vous créez une autorisation d'application pour vous connecter à une application qui utilise le flux OAuth, vous pouvez AppFabric être invité à fournir l'ID client et le secret du client. L'ID client et le secret du client se trouvent dans l'application d'authentification de votre application. Pour savoir où trouver l'ID client dans une application d'authentification donnée, consultez la section Applications prises en charge. L'identifiant client et le secret client partagés sont chiffrés à l'aide d'une clé Clé détenue par AWS ou d'une AWS KMS clé gérée par le client et stockés dans AppFabric.

Secret client

Lorsque vous créez une autorisation d'application pour vous connecter à une application qui utilise le flux OAuth, vous pouvez AppFabric être invité à fournir l'ID client et le secret du client. L'ID client et le secret du client se trouvent dans l'application d'authentification de votre application. Pour savoir où trouver le secret du client dans une application d'authentification donnée, consultez la section Applications prises en charge. L'identifiant client et le secret client partagés sont chiffrés à l'aide d'une clé Clé détenue par AWS ou d'une AWS KMS clé gérée par le client et stockés dans AppFabric.

Destination d'ingestion

Une destination d'ingestion définit l'endroit où les journaux d'audit extraits d'une ingestion doivent être stockés. Chaque ingestion peut envoyer des journaux d'audit vers une ou plusieurs destinations (jusqu'à cinq), à savoir un bucket Amazon Simple Storage Service (Amazon S3) ou un Amazon Data Firehose dans votre Compte AWS Pour chaque destination, vous pouvez définir si vous souhaitez que les journaux soient sous forme brute ou normalisés dans un schéma OCSF (Open Cybersecurity Schema Framework). Lorsque vous sélectionnez le schéma OCSF, vous pouvez définir le format des journaux (JSON ou ApacheParquet). Le Apache Parquet format ne peut être utilisé que si Amazon S3 est sélectionné comme destination.

Applications destinées aux destinataires de données

Des applications qui appelleront AppFabric pour obtenir des informations générées à partir de AppFabric.

OAuth

OAuth est un protocole ouvert qui permet une autorisation sécurisée de manière simple et standard à partir d'applications Web, mobiles et de bureau. AppFabric utilise OAuth pour créer certaines autorisations d'applications.

Cadre de schéma de cybersécurité ouvert (OCSF)

L'Open Cybersecurity Schema Framework (OCSF) est un projet open source fournissant un cadre extensible pour le développement de schémas, ainsi qu'un schéma de sécurité de base indépendant du fournisseur. Les fournisseurs et autres producteurs de données peuvent adopter et étendre le schéma pour leurs domaines spécifiques. L'objectif est de fournir un standard ouvert, adopté dans n'importe quel environnement, application ou solution, tout en complétant les normes et processus de sécurité existants. AppFabric a étendu ce schéma pour créer une structure d'événements centrée sur le logiciel en tant que service (SaaS) selon laquelle tous les journaux d'audit des applications SaaS pris en charge AppFabric seront normalisés. Pour plus d'informations, consultez Cadre de schéma de cybersécurité ouvert.

Jeton d'accès personnel (PAT)

Un jeton d'accès personnel (PAT) est une chaîne de caractères qui peut être utilisée pour accéder à un système informatique au lieu du mot de passe habituel. Lorsque vous créez une autorisation d'application pour vous connecter à une application qui utilise le flux PAT, AppFabric vous pouvez vous demander une PAT. Le PAT se trouve dans l'application d'authentification de votre application. Pour savoir où trouver le PAT dans une application d'authentification spécifique, consultez la section Applications prises en charge. Les jetons de compte de service partagés sont chiffrés à l'aide d'une clé Clé détenue par AWS ou d'une AWS KMS clé gérée par le client et stockés dans AppFabric.

Jeton de compte de service

Lorsque vous créez une autorisation d' AppFabric application pour vous connecter à une application, certaines applications nécessitent la création d'un compte de service pour l'authentification des applications. AppFabric peut demander le jeton du compte de service dans le cadre du processus d'autorisation de l'application. Pour savoir où trouver le jeton du compte de service dans une application d'authentification donnée, consultez la section Applications prises en charge. Les jetons de compte de service partagés sont chiffrés à l'aide d'une clé Clé détenue par AWS ou d'une AWS KMS clé gérée par le client et stockés dans AppFabric.

ID de locataire

Lorsque vous créez une autorisation d'application, AppFabric vous pouvez vous demander l'ID du locataire et le nom du locataire de votre application. L'ID de locataire est un identifiant unique pour le locataire de votre application. Chaque application peut avoir des termes différents pour un locataire, tels que l'ID d'espace de travail pour Slack ou l'ID de domaine pourAsana. Pour savoir où trouver l'ID du locataire dans une application spécifique, consultez la section Applications prises en charge.

Nom du locataire

Lorsque vous créez une autorisation d'application, AppFabric vous pouvez vous demander l'ID du locataire et le nom du locataire de votre application. Le nom du locataire est un nom unique que vous attribuez à l'ID du locataire, à utiliser dans un bundle d'applications. Cette valeur est utilisée pour étiqueter l'autorisation de l'application et toute ingestion associée.

Sécurité dans AWS AppFabric

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui s'exécute Services AWS dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS AppFabric, voir AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par Service AWS ce que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AppFabric. Les rubriques suivantes expliquent comment procéder à la configuration AppFabric pour atteindre vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres outils Services AWS qui vous aident à surveiller et à sécuriser vos AppFabric ressources.

Rubriques

Protection des données dans AWS AppFabric

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS AppFabric. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec AppFabric ou d'autres Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous

entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

> **Note**
>
> Pour plus d'informations sur la protection des données appliquée AppFabric à la sécurité, consultezTraitement des données.

Chiffrement au repos

AWS AppFabric prend en charge le chiffrement au repos, une fonctionnalité de chiffrement côté serveur qui chiffre de AppFabric manière transparente toutes les données relatives à vos ensembles d'applications lorsqu'elles sont conservées sur le disque, et les déchiffre lorsque vous accédez aux données. Par défaut, AppFabric chiffre vos données à l'aide d'un Clé détenue par AWS from AWS Key Management Service (AWS KMS). Vous pouvez également choisir de chiffrer vos données à l'aide de votre propre clé gérée par le client à partir de AWS KMS.

Lorsque vous supprimez un ensemble d'applications, toutes ses métadonnées sont définitivement supprimées.

Chiffrement en transit

Lorsque vous configurez un ensemble d'applications, vous pouvez choisir une clé gérée par le client Clé détenue par AWS ou une clé gérée par le client. Lors de la collecte et de la normalisation des données pour l'ingestion d'un journal d'audit, AppFabric les données sont stockées temporairement dans un compartiment Amazon Simple Storage Service (Amazon S3) intermédiaire et les chiffre à l'aide de cette clé. Ce compartiment intermédiaire est supprimé au bout de 30 jours, conformément à une politique de cycle de vie du compartiment.

AppFabric sécurise toutes les données en transit à l'aide du protocole TLS 1.2 et signe les demandes d'API Services AWS avec AWS Signature V4.

Gestion des clés

AppFabric prend en charge le chiffrement des données à l'aide d'une clé Clé détenue par AWS ou d'une clé gérée par le client. Nous vous recommandons d'utiliser une clé gérée par le client, car elle

vous permet de contrôler totalement vos données chiffrées. Lorsque vous choisissez une clé gérée par le client, vous AppFabric associez une politique de ressources à la clé gérée par le client qui lui donne accès à la clé gérée par le client.

Clé gérée par le client

Pour créer une clé gérée par le client, suivez les étapes de création de clés KMS de chiffrement symétriques dans le guide du AWS KMS développeur.

Stratégie de clé

Les politiques clés contrôlent l'accès aux clés gérées par vos clients. Chaque clé gérée par le client doit avoir exactement une stratégie de clé, qui contient des instructions qui déterminent les personnes pouvant utiliser la clé et comment elles peuvent l'utiliser. Lorsque vous créez votre clé gérée par le client, vous pouvez spécifier une stratégie de clé. Pour plus d'informations sur la création d'une stratégie clé, consultez la section Création d'une politique clé dans le Guide du AWS KMS développeur.

Pour utiliser une clé gérée par le client AppFabric, l'utilisateur ou le rôle AWS Identity and Access Management (IAM) qui crée vos AppFabric ressources doit être autorisé à utiliser votre clé gérée par le client. Nous vous recommandons de créer une clé que vous utiliserez uniquement avec AppFabric et d'ajouter vos AppFabric utilisateurs en tant qu'utilisateurs de la clé. Cette approche limite l'étendue de l'accès à vos données. Les autorisations dont vos utilisateurs ont besoin sont les suivantes :

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Decrypt`

La AWS KMS console vous guide tout au long de la création d'une clé avec la politique de clé appropriée. Pour plus d'informations sur les politiques clés, consultez la section Politiques clés du Guide du AWS KMS développeur. AWS KMS

Voici un exemple de politique clé qui permet :

- Le contrôle Utilisateur racine d'un compte AWS total de la clé.
- Utilisateurs autorisés AppFabric à utiliser votre clé gérée par le client avec AppFabric.
- Une politique clé pour la configuration d'un bundle d'applications dans`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"
                }
            }
        }
    ]
```

```
}
```

Comment AppFabric utilise les subventions dans AWS KMS

AppFabric nécessite une autorisation pour utiliser votre clé gérée par le client. Pour plus d'informations, consultez la section Subventions AWS KMS dans le guide du AWS KMS développeur.

Lorsque vous créez un bundle d'applications, AppFabric crée une subvention en votre nom en envoyant une `CreateGrant` demande à AWS KMS. Les subventions AWS KMS sont utilisées pour donner AppFabric accès à une AWS KMS clé dans un compte client. AppFabric exige que l'autorisation utilise votre clé gérée par le client pour les opérations internes suivantes :

- Envoyez `GenerateDataKey` des demandes AWS KMS à pour générer des clés de données chiffrées par votre clé gérée par le client.
- Envoyez `Decrypt` des demandes AWS KMS à pour déchiffrer les clés de données chiffrées afin qu'elles puissent être utilisées pour chiffrer vos données et pour déchiffrer les jetons d'accès aux applications en transit.
- Envoyez `Encrypt` des demandes à AWS KMS pour chiffrer les jetons d'accès aux applications en transit.

Voici un exemple de subvention.

```
{
  "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"
```

```
    }
  }
},
```

Lorsque vous supprimez un bundle d'applications, les AppFabric subventions accordées sont supprimées sur votre clé gérée par le client.

Surveillance de vos clés de chiffrement pour AppFabric

Lorsque vous utilisez des clés gérées par le AWS KMS client avec AppFabric, vous pouvez utiliser AWS CloudTrail les journaux pour suivre les demandes AppFabric envoyées à AWS KMS.

Voici un exemple d' CloudTrail événement enregistré lors de l' AppFabric utilisation `CreateGrant` de votre clé gérée par le client.

```
{
    "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"
```

```
    }
}
```

Gestion des identités et des accès pour AWS AppFabric

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser AppFabric les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez. AppFabric

Utilisateur du service : si vous utilisez le AppFabric service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles AppFabric fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AppFabric, consultezRésolution des problèmes AWS AppFabric d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des AppFabric ressources de votre entreprise, vous avez probablement un accès complet à AppFabric. C'est à vous de déterminer les AppFabric fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous

devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec AppFabric, voirComment AWS AppFabric fonctionne avec IAM.

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à. AppFabric Pour consulter des exemples de politiques AppFabric basées sur l'identité que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour AWS AppFabric

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir

plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer

des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage

des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces

politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser

une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS AppFabric fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AppFabric, découvrez les fonctionnalités IAM disponibles. AppFabric

Fonctionnalités IAM que vous pouvez utiliser avec AWS AppFabric

Fonction IAM	AppFabric soutien
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Non
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Non
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble du fonctionnement de la plupart des fonctionnalités IAM AppFabric et des autres Services AWS fonctionnalités, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour AppFabric

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour AppFabric

Pour consulter des exemples de politiques AppFabric basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS AppFabric

Politiques basées sur les ressources au sein de AppFabric

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les

ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

Actions politiques pour AppFabric

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des AppFabric actions, voir Actions définies par AWS AppFabric dans la référence d'autorisation de service.

Les actions de politique en AppFabric cours utilisent le préfixe suivant avant l'action :

```
appfabric
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "appfabric:action1",
      "appfabric:action2"
         ]
```

Vous pouvez définir plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `List`, incluez l'action suivante.

```
"Action": "appfabric:List*"
```

Pour consulter des exemples de politiques AppFabric basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS AppFabric

Ressources politiques pour AppFabric

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de AppFabric ressources et de leurs ARN, consultez la section Types de ressources définis par AWS AppFabric dans la référence d'autorisation de service. Pour

savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, voir Actions définies par. AWS AppFabric

Pour consulter des exemples de politiques AppFabric basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS AppFabric

Clés de conditions de politique pour AppFabric

Prend en charge les clés de condition de politique spécifiques au service	Non

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de AppFabric condition, reportez-vous à la section Clés de condition pour AWS AppFabric la référence d'autorisation de service. Pour savoir avec quelles actions et

ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS AppFabric.

Pour consulter des exemples de politiques AppFabric basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS AppFabric

ACL dans AppFabric

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec AppFabric

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec AppFabric

Prend en charge les informations d'identification temporaires	Non

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour AppFabric

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une

action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Fonctions du service pour AppFabric

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber AppFabric les fonctionnalités. Modifiez les rôles de service uniquement lorsque AppFabric vous recevez des instructions à cet effet.

Rôles liés à un service pour AppFabric

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles AppFabric liés à un service, consultez. Utilisation des rôles liés aux services pour AppFabric

Exemples de politiques basées sur l'identité pour AWS AppFabric

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier AppFabric des ressources. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AppFabric, y compris le format des ARN pour chacun des types de ressources, voir Actions, ressources et clés de condition AWS AppFabric dans la référence d'autorisation de service.

Table des matières

- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer AppFabric des ressources dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.

- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console AppFabric

Associez la politique `AWSAppFabricReadOnlyAccess` AWS gérée à vos identités IAM pour leur accorder une autorisation en lecture seule sur le AppFabric service, y compris la AppFabric console du. AWS Management Console Vous pouvez également associer la politique `AWSAppFabricFullAccess` AWS gérée à vos identités IAM pour leur accorder des autorisations administratives complètes sur le AppFabric service. Pour plus d'informations, consultez AWS politiques gérées pour AWS AppFabric.

AppFabric pour des exemples de politique de sécurité IAM

Les exemples de politique suivants s'appliquent AppFabric aux fonctionnalités de sécurité.

Autoriser l'accès aux ensembles d'applications

L'exemple de politique suivant autorise l'accès aux ensembles d'applications du AppFabric service.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Restreindre l'accès aux ensembles d'applications

L'exemple de politique suivant restreint l'accès aux ensembles d'applications du AppFabric service.

```
{
    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Restreindre la suppression ou l'arrêt des ingestions

L'exemple de politique suivant restreint la suppression ou l'arrêt des ingestions dans le service. AppFabric

```
{
    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StopIngestion",
                "appfabric:DeleteIngestion",
                "appfabric:DeleteIngestionDestination"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
```

```
        }
    ],
    "Version": "2012-10-17"
}
```

AppFabric pour des exemples de politiques IAM de productivité

La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Les exemples de politique suivants s'appliquent AppFabric aux fonctionnalités de productivité.

Autoriser l'accès en lecture seule aux fonctionnalités de productivité

L'exemple de politique suivant accorde un accès en lecture seule aux fonctionnalités AppFabric de productivité.

> **Important**
>
> Une erreur d'action non valide peut s'afficher lors de l'ajout de cette politique dans l'éditeur de stratégie JSON de la console IAM. Cela est dû au fait que AppFabric les fonctionnalités de productivité sont actuellement en version préliminaire. Vous devez ignorer l'erreur et procéder à la création de la politique.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
                "appfabric:ListActionableInsights",
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights"
            ],
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
```

```
}
```

Permettre un accès complet aux fonctionnalités de productivité

L'exemple de politique suivant accorde un accès complet AppFabric aux fonctionnalités de productivité.

> **Important**
>
> Une erreur d'action non valide peut s'afficher lors de l'ajout de cette politique dans l'éditeur de stratégie JSON de la console IAM. Cela est dû au fait que AppFabric les fonctionnalités de productivité sont actuellement en version préliminaire. Vous devez ignorer l'erreur et procéder à la création de la politique.

```
{
    "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"
}
```

Autoriser l'accès pour créer AppClients

L'exemple de politique suivant autorise l'accès à la création AppClients. Pour plus d'informations, voir Créer un outil AppFabric de productivité AppClient.

> **Important**
>
> Une erreur d'action non valide peut s'afficher lors de l'ajout de cette politique dans l'éditeur de stratégie JSON de la console IAM. Cela est dû au fait que AppFabric les fonctionnalités de productivité sont actuellement en version préliminaire. Vous devez ignorer l'erreur et procéder à la création de la politique.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Autoriser l'accès pour obtenir des informations sur AppClients

L'exemple de politique suivant autorise l'accès pour obtenir des informations sur AppClients. Pour plus d'informations, voir Obtenir les détails d'un AppClient.

> **Important**
>
> Une erreur d'action non valide peut s'afficher lors de l'ajout de cette politique dans l'éditeur de stratégie JSON de la console IAM. Cela est dû au fait que AppFabric les fonctionnalités de productivité sont actuellement en version préliminaire. Vous devez ignorer l'erreur et procéder à la création de la politique.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "appfabric:GetAppClient",
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Autoriser l'accès à la liste AppClients

L'exemple de politique suivant autorise l'accès à une liste AppClients. Pour plus d'informations, voir Obtenir les détails d'un AppClient.

> **Important**
>
> Une erreur d'action non valide peut s'afficher lors de l'ajout de cette politique dans l'éditeur de stratégie JSON de la console IAM. Cela est dû au fait que AppFabric les fonctionnalités de productivité sont actuellement en version préliminaire. Vous devez ignorer l'erreur et procéder à la création de la politique.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:ListAppClients"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Autoriser l'accès à la mise à jour AppClients

L'exemple de politique suivant autorise l'accès à la mise à jour AppClients. Pour plus d'informations, voir Mettre à jour un AppClient.

> **Important**
>
> Une erreur d'action non valide peut s'afficher lors de l'ajout de cette politique dans l'éditeur de stratégie JSON de la console IAM. Cela est dû au fait que AppFabric les fonctionnalités de productivité sont actuellement en version préliminaire. Vous devez ignorer l'erreur et procéder à la création de la politique.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:UpdateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Autoriser l'accès pour supprimer AppClients

L'exemple de politique suivant autorise l'accès à la suppression AppClients. Pour plus d'informations, voir Mettre à jour un AppClient.

> **Important**
>
> Une erreur d'action non valide peut s'afficher lors de l'ajout de cette politique dans l'éditeur de stratégie JSON de la console IAM. Cela est dû au fait que AppFabric les fonctionnalités de productivité sont actuellement en version préliminaire. Vous devez ignorer l'erreur et procéder à la création de la politique.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "appfabric:DeleteAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Autoriser l'accès pour autoriser les applications

L'exemple de politique suivant accorde l'accès aux applications autorisées à l'aide de l'API Token. Pour plus d'informations, consultez Authentifier et autoriser votre application.

> **Important**
>
> Une erreur d'action non valide peut s'afficher lors de l'ajout de cette politique dans l'éditeur de stratégie JSON de la console IAM. Cela est dû au fait que AppFabric les fonctionnalités de productivité sont actuellement en version préliminaire. Vous devez ignorer l'erreur et procéder à la création de la politique.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:Token"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Autres exemples de politiques IAM

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les

autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "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": "*"
        }
    ]
}
```

Utilisation des rôles liés aux services pour AppFabric

AWS AppFabric utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AppFabric Les rôles liés au

service sont prédéfinis AppFabric et incluent toutes les autorisations dont le service a besoin pour appeler d'autres personnes en votre Services AWS nom.

Un rôle lié à un service facilite la configuration AppFabric car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AppFabric définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AppFabric peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos AppFabric ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez les AWS services opérationnels avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour AppFabric

AppFabric utilise le rôle lié au service nommé `AWSServiceRoleForAppFabric` — Permet de AppFabric placer des données dans une ressource de destination d'ingestion, telle qu'un bucket Amazon S3 ou un flux de diffusion Amazon Data Firehose. Cela permet également de AppFabric mettre des données CloudWatch métriques dans l'espace de `AWS/AppFabric` noms.

Le rôle lié à un service `AWSServiceRoleForAppFabric` approuve les services suivants pour endosser le rôle :

- `appfabric.amazonaws.com`

La politique d'autorisations de rôle nommée `AWSAppFabricServiceRolePolicy` AppFabric permet d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `cloudwatch:PutMetricData` dans l'espace de `AWS/AppFabric` noms. Cette action autorise le placement AppFabric de données métriques dans l'espace de CloudWatch `AWS/AppFabric` noms Amazon. Pour plus d'informations sur les AppFabric métriques disponibles dans CloudWatch, consultezSurveillance AWS AppFabric avec Amazon CloudWatch.
- Action : `s3:PutObject` dans un compartiment Amazon S3. Cette action autorise le placement AppFabric des données ingérées dans un compartiment Amazon S3 que vous spécifiez.

- Action : `firehose:PutRecordBatch` dans un flux de diffusion Amazon Data Firehose. Cette action autorise le transfert AppFabric des données ingérées dans un flux de diffusion Amazon Data Firehose que vous spécifiez.

Pour plus d'informations, consultez la section Politiques AWS gérées pour AppFabric.

Vous devez configurer les autorisations de manière à permettre à vos utilisateurs, groupes ou rôles de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour AppFabric

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un bundle d' AppFabric applications dans l'API AWS Management Console AWS CLI, le ou l' AWS API, vous AppFabric créez le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour AppFabric

AppFabric ne vous permet pas de modifier le rôle `AWSServiceRoleForAppFabric` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour AppFabric

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Toutefois, vous devez supprimer tous vos ensembles d' AppFabric applications avant de pouvoir supprimer le rôle lié à un service.

Nettoyer un rôle lié à un service

Avant de pouvoir utiliser IAM pour supprimer un rôle lié à un service, vous devez supprimer toutes les ressources utilisées par le rôle. Les ensembles d'applications que vous créez AppFabric sont utilisés par le rôle. Pour plus d'informations, consultez Supprimer AWS AppFabric pour les ressources de sécurité.

> **Note**
>
> Si le AppFabric service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Suppression manuelle du rôle lié au service

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForAppFabric` service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles AppFabric liés à un service

AppFabric prend en charge l'utilisation de rôles liés au service partout Régions AWS où le service est disponible. Pour plus d'informations, consultez la section AppFabric Points de terminaison et quotas dans le Références générales AWS.

AWS politiques gérées pour AWS AppFabric

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

Services AWS maintenir et mettre à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture

seule à toutes Services AWS les ressources. Lorsqu'un service lance une nouvelle fonctionnalité, il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSAppFabricReadOnlyAccess

Vous pouvez associer la politique `AWSAppFabricReadOnlyAccess` à vos identités IAM. Cette politique accorde des autorisations de lecture seule au AppFabric service.

> **Note**
>
> La `AWSAppFabricReadOnlyAccess` politique n'accorde pas d'accès en lecture seule aux fonctionnalités AppFabric de productivité.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `appfabric`— Accorde l'autorisation d'obtenir un ensemble d'applications, de répertorier les ensembles d'applications, d'obtenir une autorisation d'application, de répertorier les autorisations d'applications, d'obtenir une ingestion, de répertorier les ingestions, d'obtenir une destination d'ingestion, de répertorier les destinations d'ingestion et de répertorier les balises de ressources.

```
{
    "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 politique gérée : AWSAppFabricFullAccess

Vous pouvez associer la politique `AWSAppFabricFullAccess` à vos identités IAM. Cette politique accorde des autorisations administratives au AppFabric service.

> **Important**
>
> La `AWSAppFabricFullAccess` politique n'autorise pas l'accès AppFabric aux fonctionnalités de productivité car elles sont actuellement en version préliminaire. Pour plus d'informations sur l'octroi de l'accès AppFabric aux fonctionnalités de productivité, voirAppFabric pour des exemples de politiques IAM de productivité.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `appfabric`— Accorde une autorisation administrative complète à AppFabric.
- `kms`— Accorde l'autorisation de répertorier les alias.
- `s3`— Accorde l'autorisation de répertorier tous vos compartiments Amazon S3 et d'obtenir leur emplacement.
- `firehose`— Accorde l'autorisation de répertorier les flux de diffusion Amazon Data Firehose et de décrire les flux de diffusion.
- `iam`— Accorde l'autorisation de créer le rôle `AWSServiceRoleForAppFabric` lié au service pour. AppFabric Pour plus d'informations, consultez Utilisation des rôles liés aux services pour AppFabric.

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

```
            "Action": ["appfabric:*"],
            "Resource": "*"
        },
        {
            "Sid": "KMSListAccess",
            "Effect": "Allow",
            "Action": ["kms:ListAliases"],
            "Resource": "*"
        },
        {
            "Sid": "S3ReadAccess",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "FirehoseReadAccess",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:ListDeliveryStreams"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUseOfServiceLinkedRole",
            "Effect": "Allow",
            "Action": ["iam:CreateServiceLinkedRole"],
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "appfabric.amazonaws.com"}
            },
            "Resource": "arn:aws:iam::*:role/aws-service-role/appfabric.amazonaws.com/
AWSServiceRoleForAppFabric"
        }
    ]
}
```

AWS politique gérée : AWSAppFabricServiceRolePolicy

Vous ne pouvez pas associer `AWSAppFabricServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet d' AppFabric effectuer des actions en votre nom. Pour plus d'informations, consultez Utilisation des rôles liés aux services pour AppFabric.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `cloudwatch`— Accorde l'autorisation AppFabric de placer des données métriques dans l'espace de CloudWatch `AWS/AppFabric` noms Amazon. Pour plus d'informations sur les AppFabric métriques disponibles dans CloudWatch, consultezSurveillance AWS AppFabric avec Amazon CloudWatch.
- `s3`— Accorde l'autorisation AppFabric de placer les données ingérées dans un compartiment Amazon S3 que vous spécifiez.
- `firehose`— Accorde l'autorisation AppFabric de placer les données ingérées dans un flux de diffusion Amazon Data Firehose que vous spécifiez.

```
{
    "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 mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AppFabric depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du AppFabric document.

Modification	Description	Date
AWSAppFabricReadOnlyAccess : nouvelle politique	AppFabric a ajouté une nouvelle politique pour accorder des autorisations de lecture seule au AppFabric service.	27 juin 2023
AWSAppFabricFullAccess : nouvelle politique	AppFabric a ajouté une nouvelle politique pour accorder des autorisations administratives au AppFabric service.	27 juin 2023
AWSAppFabricServiceRolePolicy : nouvelle politique	AppFabric a ajouté une nouvelle politique pour le rôle `AWSServiceRoleForAppFabric` lié au service.	27 juin 2023

Modification	Description	Date
AppFabric a commencé à suivre les modifications	AppFabric a commencé à suivre les modifications apportées AWS à ses politique s gérées.	27 juin 2023

Résolution des problèmes AWS AppFabric d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AppFabric IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AppFabric
- Je ne suis pas autorisé à effectuer iam:PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AppFabric ressources

Je ne suis pas autorisé à effectuer une action dans AppFabric

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `appfabric:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 appfabric:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `appfabric:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam:PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle AppFabric.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans AppFabric. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AppFabric ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AppFabric en charge, consultezComment AWS AppFabric fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.

- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Validation de conformité pour AWS AppFabric

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Bonnes pratiques en matière de sécurité pour AWS AppFabric

AWS AppFabric fournit plusieurs fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Surveiller les applications sans accès administrateur

Avec l'autorisation de lecture seule AWS Identity and Access Management (IAM), tout le monde peut s'intégrer à AppFabric Amazon QuickSight et à d'autres outils de gestion des informations et des événements de sécurité (SIEM), tels que. Splunk Pour surveiller la sécurité des applications, les données sont transmises à un bucket Amazon Simple Storage Service (Amazon S3) ou à un flux de diffusion Amazon Data Firehose.

Surveillez les AppFabric événements

Vous pouvez effectuer un suivi AppFabric à l'aide CloudWatch des métriques Amazon. CloudWatch collecte les données de AppFabric chaque minute et les transforme en métriques. Vous pouvez définir des alarmes qui déclenchent des notifications lorsque les mesures atteignent des seuils spécifiés. Pour plus d'informations, consultez Surveillance AWS AppFabric avec Amazon CloudWatch.

Résilience dans AWS AppFabric

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l'infrastructure dans AWS AppFabric

En tant que service géré, AWS AppFabric il est protégé par les procédures de sécurité du réseau AWS mondial décrites dans le livre blanc Amazon Web Services : présentation des processus de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder AppFabric via le réseau. Les clients doivent prendre en charge le protocole TLS 1.0 ou version ultérieure. Nous recommandons TLS 1.2 ou version ultérieure. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Ou, pour générer des informations de sécurité temporaires afin de signer les demandes, vous pouvez utiliser le AWS Security Token Service(AWS STS).

Analyse de configuration et de vulnérabilité dans AWS AppFabric

La configuration et les contrôles informatiques sont une responsabilité partagée entre vous AWS et vous, notre client. Pour plus d'informations, consultez le modèle de responsabilité AWS partagée.

Surveillance AWS AppFabric

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité AWS AppFabric et des performances de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller AppFabric, signaler tout problème et prendre des mesures automatiques le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos instances Amazon EC2 et lancer automatiquement de nouvelles instances en cas de besoin. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- Amazon CloudWatch Logs vous permet de surveiller, de stocker et d'accéder à vos fichiers journaux à partir d'instances Amazon EC2 et d'autres sources. AWS CloudTrail CloudWatch Les journaux peuvent surveiller les informations contenues dans les fichiers journaux et vous avertir lorsque certains seuils sont atteints. Vous pouvez également archiver vos données de journaux dans une solution de stockage hautement durable. Pour plus d'informations, consultez le guide de l'utilisateur d'Amazon CloudWatch Logs.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par vous ou en votre nom Compte AWS et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

Surveillance AWS AppFabric avec Amazon CloudWatch

Vous pouvez surveiller AWS AppFabric l'utilisation CloudWatch, qui collecte les données brutes et les transforme en indicateurs lisibles en temps quasi réel. Ces statistiques sont enregistrées pour une durée de 15 mois ; par conséquent, vous pouvez accéder aux informations historiques et acquérir un meilleur point de vue de la façon dont votre service ou application web s'exécute. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Le AppFabric service indique les métriques suivantes dans l'espace de `AWS/AppFabric` noms.

Métrique	Description
AppFabric État de l'autorisation de l'application	État de l'autorisation de l'application (`1`pour les personnes connectées, `0` pour toute autre application).
AppFabric Latence de livraison des données	Temps (en secondes) nécessaire AppFabric pour collecter les journaux d'audit depuis l'application SaaS et les envoyer à la destinati on configurée (Amazon S3 ou Amazon Data Firehose).
État de la destination d'ingestion	État de la destination 1 d'ingestion (active ou autre). `0`
Retard global des données	La différence de temps (en secondes) entre le moment où les événements se sont produits sur l'application SaaS et le moment où les journaux d'audit correspondants ont été envoyés à la destination configurée (Amazon S3 ou Amazon Data Firehose) par. AppFabric
Volume de données ingérées	Taille des données fournies à Amazon Simple Storage Service (Amazon S3) ou Amazon Data Firehose.

La dimension suivante est prise en charge pour AppFabric les métriques.

Dimension	Description
Arne de destination d'ingestion	Le nom de ressource Amazon (ARN) de la destination d'ingestion.

Journalisation des appels AWS AppFabric d'API à l'aide AWS CloudTrail

AWS AppFabric est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS utilisateur AppFabric. CloudTrail capture tous les appels d'API AppFabric sous forme d'événements. Les appels capturés incluent des appels provenant de la AppFabric console et des appels de code vers les opérations de l' AppFabric API. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrailévénements vers un compartiment Amazon S3, y compris les événements pour AppFabric. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AppFabric, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour plus d'informations CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

AppFabric informations dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans AppFabric, cette activité est enregistrée dans un CloudTrail événement avec d'autres Service AWS événements dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements dans le Guide de AWS CloudTrail l'utilisateur.

Pour un enregistrement continu des événements de votre région Compte AWS, y compris des événements pour AppFabric, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez en configurer d'autres Services AWS pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les rubriques suivantes dans le AWS CloudTrail Guide de l'utilisateur :

- Présentation de la création d'un journal d'activité
- CloudTrail services et intégrations pris en charge

- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les AppFabric actions sont enregistrées CloudTrail et documentées dans la référence de l'AWS AppFabric API. Par exemple, les appels aux `CreateAppBundle`, `UpdateAppBundle`, et `GetAppBundle` les actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

Pour plus d'informations, voir CloudTrail userIdentityl'élément dans le guide de AWS CloudTrail l'utilisateur.

Comprendre les entrées du fichier AppFabric journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`CreateAppBundle`action.

```
{
    "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"
    }
}
```

Quotas pour AWS AppFabric

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux Service AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Pour consulter les quotas pour AppFabric, ouvrez la console Service Quotas. Dans le volet de navigation, choisissez AWS les services, puis sélectionnez AppFabric.

Pour demander une augmentation de quota, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le Formulaire d'augmentation de limite de service.

Les quotas correspondants AppFabric Compte AWS sont indiqués dans le tableau suivant.

Nom	Par défaut	Ajusta	Description
Bundles d'applications	Par région prise en charge : 1	Non	Le nombre maximum de packs d'applications que vous pouvez créer dans un compte dans la AWS région actuelle.
Autorisations d'application	Chaque région prise en charge : 50	Non	Le nombre maximum d'autorisations d'application que vous pouvez créer dans un compte dans la AWS région actuelle.
Ingestions	Chaque région prise en charge : 50	Non	Le nombre maximum d'ingestions que vous pouvez créer dans un compte dans la région actuelle AWS .

Nom	Par défaut	Ajusta	Description
Destinations d'ingestion	Chaque région prise en charge : 5	Non	Le nombre maximum de destinations d'ingestion que vous pouvez créer par ingestion dans un compte dans la AWS région actuelle.
AppClient	Par région prise en charge : 1	Non	Le nombre maximum AppClients que vous pouvez créer dans un compte dans la AWS région actuelle. La fonctionnalité AWS AppFabric de productivité est en cours d'aperçu et est sujette à modification.

Historique du document pour le guide AppFabric d'administration

Le tableau suivant décrit les versions de documentation pour AWS AppFabric.

Modification	Description	Date
Nouvelle application prise en charge	Ajouté SentinelOne en tant qu'application prise en charge. Pour plus d'informations, consultez la section Applications prises en charge dans AWS AppFabric.	25 avril 2024
Nouvelle application prise en charge	Ajouté 1Password en tant qu'application prise en charge. Pour plus d'informations, consultez la section Applications prises en charge dans AWS AppFabric.	23 avril 2024
Nouvel outil de sécurité pris en charge	Ajouté Dynatrace en tant qu'outil de sécurité compatible. Pour plus d'informations, consultez la section Outils de sécurité compatibles.	26 mars 2024
Nouvelle métrique	Ajout de la métrique d'état d'autorisation de l' AppFabric application. Pour plus d'informations, consultez la section Surveillance AWS AppFabric avec Amazon CloudWatch Logs.	8 mars 2024
Nouvelle application prise en charge	Ajouté IBM Security® Verify en tant qu'application prise en	6 mars 2024

	charge. Pour plus d'informations, consultez la section Applications prises en charge dans AWS AppFabric.	
Nouvelle application prise en charge	Ajouté Box en tant qu'application prise en charge. Pour plus d'informations, consultez la section Applications prises en charge dans AWS AppFabric.	28 février 2024
Nouvelles applications et indicateurs pris en charge	Ajouté Cisco DuoSalesforce, et en Terraform Cloud tant qu'applications prises en charge. Pour plus d'informations à leur sujet, consultez la section Applications prises en charge dans AWS AppFabric. Ajout AppFabric des métriques de latence de livraison des données et de délai global des données. Pour plus d'informations, consultez la section Surveillance AWS AppFabric avec Amazon CloudWatch Logs.	1 février 2024
AjoutéAtlassian Confluence,,Genesys Cloud,HubSpot, OneLogin by One IdentityPagerDuty, et en Ping Identity tant qu'applications prises en charge et Barracuda XDR en tant qu'outil de sécurité compatible	Pour plus d'informations sur les nouvelles applications prises en charge, voir Applications prises en charge dans AWS AppFabric et Outils de sécurité compatibles.	15 décembre 2023

AjoutéAtlassian Confluence,,Genesys Cloud,HubSpot, OneLogin by One IdentityPagerDuty, et en Ping Identity tant qu'applications prises en charge et Barracuda XDR en tant qu'outil de sécurité compatible	Pour plus d'informations sur les nouvelles applications prises en charge, voir Applications prises en charge dans AWS AppFabric et Outils de sécurité compatibles.	15 décembre 2023
Ajout de la documentation d'aperçu AWS AppFabric pour la productivité	Pour plus d'informations sur AppFabric la productivité, voir Qu'est-ce que AWS AppFabric la productivité ?	27 novembre 2023
Applications ajoutées GitHub et prises ServiceNow en charge	Pour plus d'informations sur les nouvelles applications prises en charge, consultez la section Applications prises en charge.	31 octobre 2023
A commencé à suivre les politiques AWS gérées pour AWS AppFabric	Pour plus d'informations sur les politiques AWS gérées pour AppFabric, consultez la section stratégies AWS gérées pour AWS AppFabric.	27 juin 2023
Première version	Première publication du guide AWS AppFabric d'administration.	27 juin 2023

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.