aws

Guía de administración

AWS AppFabric

AWS AppFabric: Guía de administración

Table of Contents

¿Qué es AWS AppFabric? 1
Productos 1
Ventajas 1
Casos de uso 2
¿Cómo funciona AppFabric 2
Precios 3
Disponibilidad 3
¿Qué es AWS AppFabric por seguridad? 3
Ventajas 1
Casos de uso 2
Acceso por motivos de seguridad AppFabric 4
Servicios relacionados 5
Esquema OCSF 6
Requisitos previos y recomendaciones 7
Introducción 13
Aplicaciones compatibles 24
Herramientas de seguridad compatibles 126
Eliminación de recursos 142
¿Qué es AWS AppFabric para la productividad? 143
Ventajas 1
Casos de uso 2
Acceso AppFabric para aumentar la productividad 4
Primeros pasos para desarrolladores de aplicaciones 147
Introducción para los usuarios finales 175
AppFabric API de productividad 192
Procesamiento de datos 218
Terminología y conceptos 219
Seguridad 223
Protección de datos 224
Cifrado en reposo 225
Cifrado en tránsito 225
Administración de claves 225
Política de claves 226
¿Cómo se AppFabric utilizan las subvenciones en AWS KMS 228

Supervisar tus claves de cifrado para AppFabric 229
Administración de identidades y accesos 231
Público 231
Autenticación con identidades 232
Administración de acceso mediante políticas 236
¿Cómo AWS AppFabric funciona con IAM 238
Ejemplos de políticas basadas en identidades 246
Uso de roles vinculados a servicios 257
AWS políticas gestionadas 259
Resolución de problemas 265
Validación de conformidad 267
Prácticas recomendadas de seguridad 268
Cómo supervisar la aplicación sin acceso de administrador 268
Supervise los eventos AppFabric 269
Resiliencia 269
Seguridad de la infraestructura 269
Configuración y análisis de vulnerabilidades 270
Supervisión 271
Monitorización con CloudWatch 271
CloudTrail registros 273
AppFabric información en CloudTrail 273
Descripción de las entradas de los archivos de AppFabric registro 274
Cuotas 277
Historial de documentos 279
..... cclxxxiii

¿Qué es AWS AppFabric?

AWS AppFabric conecta rápidamente las aplicaciones de software como servicio (SaaS) en toda la organización, de modo que los equipos de TI y seguridad puedan gestionar y proteger fácilmente las aplicaciones mediante un esquema estándar, y los empleados puedan completar las tareas diarias con mayor rapidez mediante la IA generativa.

Temas

- Productos
- Ventajas
- Casos de uso
- ¿Cómo funciona AppFabric
- Precios
- Disponibilidad
- ¿Qué es AWS AppFabric por seguridad?
- ¿Qué es AWS AppFabric para la productividad?

Productos

Explore las dos facetas AWS AppFabric: la seguridad, diseñada AppFabric para optimizar la gestión y la seguridad, y AppFabric la productividad (versión preliminar), mejorada con capacidades de IA generativa. Para obtener más información, consulte los temas siguientes:

- ¿Qué es AWS AppFabric por seguridad?
- ¿Qué es AWS AppFabric para la productividad?

Ventajas

Se puede utilizar AppFabric para hacer lo siguiente:

- Conecte sus aplicaciones en cuestión de minutos y reduzca los costos operativos.
- Aumente la visibilidad de los datos de las aplicaciones SaaS para mejorar su seguridad.
- Facilite de forma automática las tareas en todas las aplicaciones con la IA generativa.

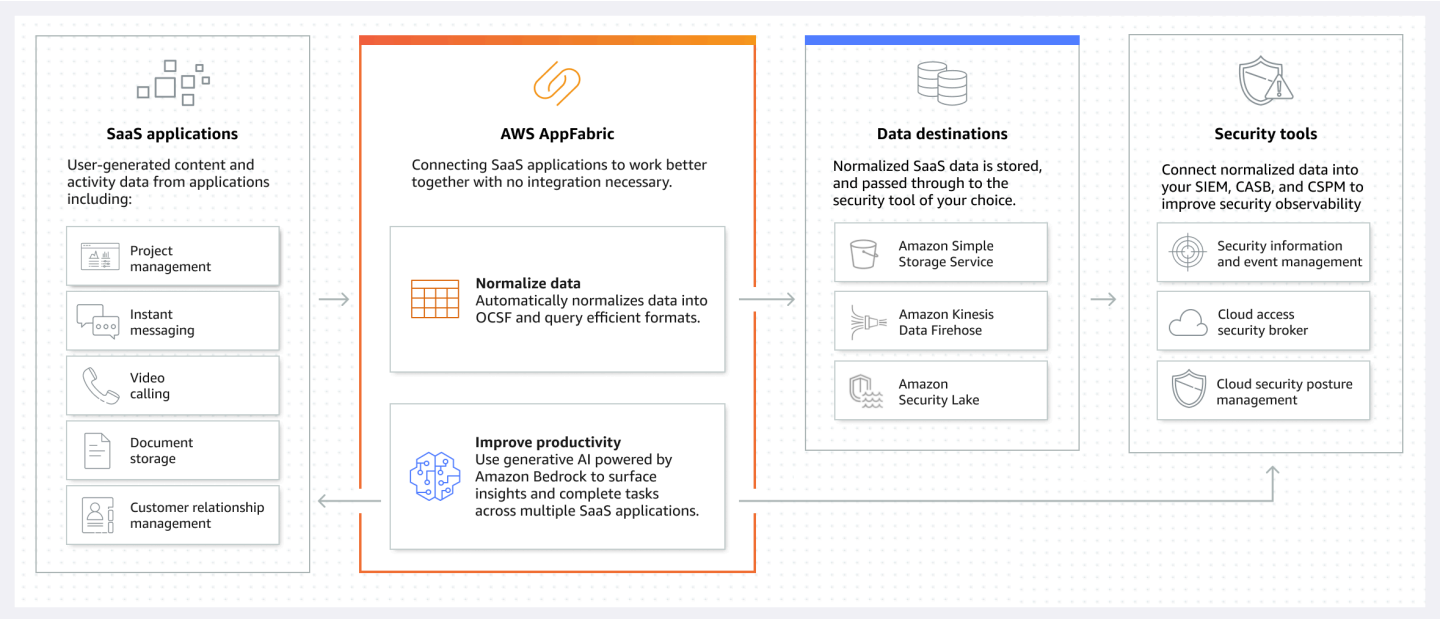
Casos de uso

Se puede utilizar AppFabric para:

- Conectarse a sus aplicaciones SaaS rápidamente
  - AppFabric for security conecta de forma nativa las principales aplicaciones de productividad y seguridad de SaaS entre sí, proporcionando una solución de interoperabilidad SaaS totalmente gestionada.
- Aumentar su seguridad
  - Los datos de las aplicaciones se normalizan automáticamente, lo que permite a los administradores establecer políticas comunes, estandarizar las alertas de seguridad y administrar fácilmente el acceso de los usuarios a varias aplicaciones.
- Reinventar la productividad
  - Con un asistente de IA generativo común, AppFabric for productivity permite a los empleados obtener respuestas rápidamente, automatizar la gestión de tareas y generar información sobre sus aplicaciones de productividad de SaaS.

¿Cómo funciona AppFabric

AppFabric conecta rápidamente múltiples aplicaciones SaaS sin necesidad de codificación para aumentar la productividad y la seguridad. El siguiente diagrama muestra las ventajas de AppFabric.



> **Note**
>
> AppFabric for productivity se ha lanzado actualmente como versión preliminar y está disponible en el este de EE. UU. (Virginia del Norte) Región de AWS. Para obtener más información al respecto Regiones de AWS, consulte AWS AppFabric los puntos finales y las cuotas en. Referencia general de AWS

Precios

Para obtener detalles y ejemplos de AppFabric precios, consulte AWS AppFabric Precios.

Disponibilidad

Para ver las AWS regiones y los puntos de conexión compatibles actualmente AppFabric, consulte los puntos de AWS AppFabric conexión y las cuotas en la referencia AWS general.

¿Qué es AWS AppFabric por seguridad?

AWS AppFabric for security conecta rápidamente las aplicaciones de software como servicio (SaaS) en toda la organización, de modo que los equipos de TI y seguridad puedan gestionar y proteger fácilmente las aplicaciones mediante un esquema estándar.

Temas

- Ventajas
- Casos de uso
- Acceso por motivos de seguridad AppFabric
- Servicios relacionados
- Marco de esquema de ciberseguridad abierto
- Requisitos previos y recomendaciones
- Primeros pasos AWS AppFabric por seguridad
- Aplicaciones compatibles
- Herramientas y servicios de seguridad compatibles

- Eliminar AWS AppFabric para recursos de seguridad

Ventajas

Con AppFabric fines de seguridad, puede hacer lo siguiente:

- Conecte sus aplicaciones en cuestión de minutos y reduzca los costos operativos.
- Aumente la visibilidad de los datos de las aplicaciones SaaS para mejorar su seguridad.

Casos de uso

Puede usarlo como AppFabric medida de seguridad para:

- Conectarse a sus aplicaciones SaaS rápidamente
  - AppFabric for security conecta de forma nativa las principales aplicaciones de productividad y seguridad de SaaS entre sí, proporcionando una solución de interoperabilidad SaaS totalmente gestionada.
- Aumentar su seguridad
  - Los datos de las aplicaciones se normalizan automáticamente, lo que permite a los administradores establecer políticas comunes, estandarizar las alertas de seguridad y administrar fácilmente el acceso de los usuarios a varias aplicaciones.

Acceso por motivos de seguridad AppFabric

AppFabric por motivos de seguridad está disponible en EE. UU. Este (Virginia del Norte), Europa (Irlanda) y Asia Pacífico (Tokio) Regiones de AWS. Para obtener más información al respecto Regiones de AWS, consulte AWS AppFabric los puntos finales y las cuotas en. Referencia general de AWS

En cada región, puede acceder AppFabric por motivos de seguridad de cualquiera de las siguientes maneras:

AWS Management Console

AWS Management Console Se trata de una interfaz basada en un navegador que puede utilizar para crear y administrar AWS recursos. La AppFabric consola proporciona acceso a sus recursos. AppFabric Puede usar la AppFabric consola para crear y administrar todos los AppFabric recursos.

AppFabric API

Para acceder AppFabric mediante programación, usa la AppFabric API y envía solicitudes HTTPS directamente al servicio. Para obtener más información, consulta la referencia de la AWS AppFabric API.

AWS Command Line Interface (AWS CLI)

Con el AWS CLI, puede emitir comandos en la línea de comandos de su sistema para interactuar con ellos AppFabric y otros Servicios de AWS. Si desea crear scripts que realicen tareas, las herramientas de línea de comandos también son útiles. Para obtener información sobre la instalación y el uso del AWS CLI, consulte la Guía del AWS Command Line Interface usuario de la versión 2. Para obtener información sobre los AWS CLI comandos de AppFabric, consulte la AppFabric sección de la AWS CLI Referencia.

Servicios relacionados

AppFabric Por motivos de seguridad, puede utilizar lo siguiente Servicios de AWS :

Amazon Data Firehose

Amazon Data Firehose es un servicio de extracción, transformación y carga (ETL) que captura, transforma y entrega datos de forma fiable a lagos de datos, almacenes de datos y servicios de análisis. Cuando lo utilice AppFabric, puede elegir enviar sus registros de auditoría normalizados o sin procesar de Open Cybersecurity Schema Framework (OCSF) en formato JSON a una transmisión de Firehose como destino. Para obtener más información, consulte Crear una ubicación de salida en Firehose.

Amazon Security Lake

Amazon Security Lake centraliza automáticamente los datos de seguridad de los AWS entornos, los proveedores de SaaS y las fuentes locales y en la nube en un lago de datos diseñado específicamente y almacenado en su cuenta. Puede integrar los datos del registro de AppFabric auditoría con Security Lake seleccionando Amazon Data Firehose como destino y configurando Firehose para que entregue los datos en el formato y la ruta correctos en Security Lake. Para obtener más información, consulte Recopilación de datos de fuentes personalizadas en la Guía del usuario de Amazon Security Lake.

Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes del sector. Cuando lo utilice AppFabric, puede elegir enviar sus registros de auditoría OCSF normalizados (JSON oApache Parquet) o sin procesar (JSON) a un bucket de Amazon S3 nuevo o existente como destino. Para obtener más información, consulte Crear una ubicación de salida en Amazon S3).

Amazon QuickSight

Amazon QuickSight impulsa a las organizaciones basadas en datos con inteligencia empresarial (BI) unificada a hiperescala. De este QuickSight modo, todos los usuarios pueden satisfacer diferentes necesidades analíticas partiendo de la misma fuente de información mediante modernos paneles interactivos, informes paginados, análisis integrados y consultas en lenguaje natural. Para analizar los datos de los registros de AppFabric auditoría QuickSight, elija el depósito de Amazon S3 en el que se almacenan AppFabric los registros como fuente. Para obtener más información, consulte Creación de un conjunto de datos con archivos de Amazon S3 en la Guía del QuickSight usuario de Amazon. También puede importar AppFabric datos de Amazon S3 a Amazon Athena y seleccionar Amazon Athena como fuente de datos en. QuickSight Para obtener más información, consulte Creación de un conjunto de datos con datos de Amazon Athena en la Guía QuickSight del usuario de Amazon.

AWS Key Management Service

Con AWS Key Management Service (AWS KMS), puede crear, administrar y controlar las claves criptográficas en todas sus aplicaciones y. Servicios de AWS Al crear un paquete de aplicaciones AppFabric, se configura una clave de cifrado para proteger de forma segura los datos de la aplicación autorizada. Esta clave cifra tus datos dentro del AppFabric servicio. AppFabric puede usar una clave Clave propiedad de AWS creada y gestionada por usted AppFabric en su nombre, o una clave gestionada por el cliente que usted cree y gestione. AWS KMS Para obtener más información, consulte Crear una AWS KMS clave.

Marco de esquema de ciberseguridad abierto

El Open Cybersecurity Schema Framework (OCSF) es un esfuerzo colaborativo AWS y de código abierto realizado por socios líderes de la industria de la ciberseguridad. El OCSF proporciona un esquema estándar para los eventos de seguridad comunes, define los criterios de control de versiones para facilitar la evolución del esquema e incluye un proceso de autogobierno para los productores y consumidores de registros de seguridad. El código fuente público de OCSF está alojado en. GitHub

Esquema basado en OCSF en AppFabric

El esquema basado en OCSF 1.0.0-rc.3 AWS AppFabric para la seguridad está diseñado específicamente para satisfacer sus necesidades de observabilidad normalizada, consistente y de bajo esfuerzo de su cartera de software como servicio (SaaS). AppFabric, en colaboración con la comunidad de código abierto de OCSF, introdujo nuevas categorías de eventos, clases de eventos, actividades y objetos de OCSF para que OCSF sea aplicable a los eventos de aplicaciones SaaS. AppFabric normaliza automáticamente los eventos de auditoría que recibe de las aplicaciones SaaS y entrega estos datos a los servicios Amazon Simple Storage Service (Amazon S3) o Amazon Data Firehose de su empresa. Cuenta de AWS Para un destino de Amazon S3, puede elegir entre dos opciones de normalización (OCSF o Raw) y dos opciones de formato de datos (JSON o Parquet). Al realizar envíos a Firehose, también puedes elegir entre dos opciones de normalización (OCSF o Raw), pero el formato de datos se limita a JSON.

Categorías y clases de eventos de OCSF

AppFabric utiliza las dos categorías de eventos de OCSF siguientes:

- Identity and Access Management: AppFabric por motivos de seguridad, utiliza las siguientes clases de eventos dentro de esta categoría:
  - Cambio de cuenta
  - Autenticación
  - Administración de acceso de usuarios
  - Administración de grupos
- Actividad de la aplicación: AppFabric por motivos de seguridad, utiliza las siguientes clases de eventos dentro de esta categoría:
  - Actividad de recursos web
  - Actividad de acceso a recursos web

Requisitos previos y recomendaciones

Si es un AWS cliente nuevo, complete los requisitos previos de configuración que se indican en esta página antes de empezar a utilizarlos AWS AppFabric por motivos de seguridad. Para estos procedimientos de configuración, utilice el servicio AWS Identity and Access Management (IAM). Para obtener información completa sobre IAM, consulte la Guía del usuario de IAM.

Temas

- Inscríbase en una Cuenta de AWS
- Creación de un usuario con acceso administrativo
- (Obligatorio) Cómo completar los requisitos previos de la aplicación
- (Opcional) Cómo crear una ubicación de salida
- (Opcional) Cree una clave AWS KMS

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

(Obligatorio) Cómo completar los requisitos previos de la aplicación

Como medida de seguridad AppFabric para recibir información de usuario y registros de auditoría de las aplicaciones, muchas aplicaciones requieren que tenga un rol y un tipo de plan específicos. Asegúrese de haber revisado los requisitos previos de cada aplicación que desee autorizar AppFabric por motivos de seguridad y de contar con los planes y funciones adecuados. Para obtener más información sobre los requisitos previos específicos de cada aplicación, consulte Aplicaciones compatibles o elija uno de los siguientes temas específicos de aplicación.

- 1Password
- Asana
- Azure Monitor
- Atlassian Confluence
- Atlassian Jira suite
- Box
- Cisco Duo
- Dropbox
- Genesys Cloud
- GitHub
- Google Analytics
- Google Workspace
- HubSpot
- IBM Security® Verify
- JumpCloud
- Microsoft365
- Miro
- Okta
- OneLogin by One Identity
- PagerDuty

- Ping Identity
- Salesforce
- ServiceNow
- Singularity Cloud
- Slack
- Smartsheet
- Terraform Cloud
- Webex by Cisco
- Zendesk
- Zoom

(Opcional) Cómo crear una ubicación de salida

AppFabric por motivos de seguridad, admite Amazon Simple Storage Service (Amazon S3) y Amazon Data Firehose como destinos de ingesta de registros de auditoría.

Amazon S3

Puede crear un nuevo bucket de Amazon S3 mediante la AppFabric consola al crear un destino de ingesta. También puede crear un bucket usando el servicio Amazon S3. Si decide crear su depósito mediante el servicio Amazon S3, debe crear el depósito antes de crear el destino de AppFabric ingesta y, a continuación, seleccionar el depósito al crear el destino de ingesta. Puede optar por utilizar un depósito de Amazon S3 existente en su depósito Cuenta de AWS, siempre que cumpla los siguientes requisitos para los depósitos existentes:

- AppFabric por motivos de seguridad, requiere que su bucket de Amazon S3 esté en el Región de AWS mismo lugar que sus recursos de Amazon S3.
- Puede cifrar su bucket mediante una de las siguientes opciones:
  - Cifrado del servidor con claves administradas por Amazon S3 (SSE-S3)
  - Cifrado del lado del servidor con claves AWS Key Management Service (AWS KMS) (SSE-KMS) utilizando el valor predeterminado (). Clave administrada de AWS `aws/s3`

Amazon Data Firehose

Puede optar por utilizar Amazon Data Firehose como destino de ingestión de datos AppFabric de seguridad. Para usar Firehose, puedes crear el flujo de entrega de Firehose en tu Cuenta de AWS antes de crear una ingestión o mientras creas un destino de ingestión en. AppFabric Puedes crear una transmisión de entrega de Firehose mediante AWS Management Console, AWS CLI, o las AWS API o los SDK. Para saber cómo configurar el flujo, consulte los siguientes temas:

- AWS Management Console instrucciones — Creación de un flujo de entrega de Amazon Data Firehose en la guía para desarrolladores de Amazon Data Firehose
- AWS CLI instrucciones: create-delivery-streamen la Referencia de comandos AWS CLI
- AWS Instrucciones sobre las API y los SDK: CreateDeliveryStreamen la referencia de las API de Amazon Data Firehose

Los requisitos para utilizar Amazon Data Firehose como destino de salida AppFabric de seguridad son los siguientes:

- Debe crear la transmisión en la Región de AWS misma forma que sus recursos AppFabric de seguridad.
- Debe seleccionar PUT directo como fuente.
- Adjunta la política AmazonKinesisFirehoseFullAccess AWS gestionada a tu usuario o adjunta los siguientes permisos a tu usuario:

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

Firehose admite la integración con una variedad de herramientas de seguridad de terceros, como Splunk y. Logz.io Para obtener información sobre cómo configurar correctamente Amazon Kinesis para que envíe datos a estas herramientas, consulte Destination Settings en la Guía para desarrolladores de Amazon Data Firehose.

(Opcional) Cree una clave AWS KMS

En el proceso de creación de un paquete AppFabric de aplicaciones de seguridad, seleccionará o configurará una clave de cifrado para proteger sus datos de forma segura de todas las aplicaciones autorizadas. Esta clave se utilizará para cifrar sus datos dentro del AppFabric servicio.

AppFabric por motivos de seguridad, cifra los datos de forma predeterminada. AppFabric por motivos de seguridad, puede utilizar una clave Clave propiedad de AWS creada y AppFabric gestionada por usted o una clave gestionada por el cliente que usted cree y gestione en AWS Key Management Service (AWS KMS). Claves propiedad de AWS son una colección de AWS KMS claves que AN Servicio de AWS posee y administra para su uso en múltiples ocasiones Cuentas de AWS. Las claves administradas por el cliente son AWS KMS claves Cuenta de AWS tuyas que tú creas, posees y administras. Para obtener más información sobre Claves propiedad de AWS las claves administradas por el cliente, consulte Claves y AWS claves del cliente en la Guía para AWS Key Management Service desarrolladores.

Si desea utilizar una clave gestionada por el cliente para cifrar sus datos, como los tokens de autorización, AppFabric por motivos de seguridad, puede crear una con AWS KMSella. Para obtener más información sobre la política de permisos que permite el acceso a tu clave gestionada por el cliente AWS KMS, consulta la sección Política de claves de esta guía.

Primeros pasos AWS AppFabric por seguridad

AWS AppFabric Para empezar por motivos de seguridad, primero debes crear un paquete de aplicaciones y, a continuación, autorizar y conectar las aplicaciones a tu paquete de aplicaciones. Una vez que las autorizaciones de las aplicaciones estén conectadas a las aplicaciones, puede utilizarlas AppFabric para funciones de seguridad, como la ingesta de registros de auditoría y el acceso de los usuarios.

En esta sección se explica cómo empezar a utilizar AppFabric en. AWS Management Console

Temas

- Requisitos previos
- Paso 1: crear agrupación de aplicaciones
- Paso 2: autorizar aplicaciones
- Paso 3: configurar ingestas de registros de auditoría
- Paso 4: utilizar la herramienta de acceso de usuario

- Paso 5: Conéctese AppFabric para obtener datos de seguridad en herramientas de seguridad y otros destinos

Requisitos previos

Antes de empezar, primero debe crear un usuario administrativo Cuenta de AWS y uno. Para obtener más información, consulte Inscríbase en una Cuenta de AWS y Creación de un usuario con acceso administrativo.

Paso 1: crear agrupación de aplicaciones

Un paquete de aplicaciones almacena todas sus autorizaciones e incorporaciones de aplicaciones AppFabric por motivos de seguridad. Para crear una agrupación de aplicaciones, configure una clave de cifrado para proteger de forma segura los datos de la aplicación autorizada.

1. Abre la AppFabric consola en https://console.aws.amazon.com/appfabric/.
2. En el selector Seleccione una región en la esquina superior derecha de la página, seleccione una. Región de AWS AppFabric está disponible únicamente en las regiones de EE. UU. Este (Virginia del Norte), Europa (Irlanda) y Asia Pacífico (Tokio).
3. Elija Empezar.
4. En la página de Introducción, para el Paso 1. Crear agrupación de aplicaciones, seleccione Crear agrupación de aplicaciones.
5. En la sección de Cifrado, configure una clave de cifrado para proteger sus datos de forma segura de todas las aplicaciones autorizadas. Esta clave se utiliza para cifrar sus datos dentro del servicio AppFabric de seguridad.

   AppFabric por motivos de seguridad, cifra los datos de forma predeterminada. AppFabric puede usar una clave Clave propiedad de AWS creada y gestionada por usted AppFabric en su nombre o una clave gestionada por el cliente que usted cree y gestione en AWS Key Management Service (AWS KMS).
6. En Clave de AWS KMS , elija Usar Clave propiedad de AWS o Clave administrada por el cliente.

   Si decide utilizar una clave administrada por el cliente, introduzca el Nombre de recurso de Amazon (ARN) o la ID de clave de la clave existente que desee utilizar, o bien elija Crear una clave de AWS KMS .

   Ten en cuenta lo siguiente al elegir una clave gestionada por el cliente Clave propiedad de AWS o una clave gestionada por el cliente:

- Claves propiedad de AWSson un conjunto de claves AWS Key Management Service (AWS KMS) que una Servicio de AWS posee y administra para su uso en varios Cuentas de AWS. Aunque no Claves propiedad de AWS están en tus Cuenta de AWS manos, Servicio de AWS pueden utilizarlas Clave propiedad de AWS para proteger los recursos de tu cuenta. Claves propiedad de AWS no se tienen en cuenta para las AWS KMS cuotas de su cuenta. No es necesario crear ni mantener la clave ni su política de claves. La rotación Claves propiedad de AWS varía según los servicios. Para obtener información sobre la rotación de una forma Clave propiedad de AWS AppFabric, consulte Cifrado en reposo.
- Las claves administradas por el cliente son claves de KMS Cuenta de AWS que usted crea, posee y administra. Usted tiene el control total sobre estas AWS KMS claves. Puede establecer y mantener sus políticas de claves, políticas de AWS Identity and Access Management (IAM) y subvenciones. Puede activarlas y desactivarlas, modificar su material criptográfico, añadir etiquetas, crear alias que hagan referencia a las AWS KMS claves y programar su AWS KMS eliminación. Las claves administradas por el cliente aparecen en la página de claves administradas por el cliente del AWS Management Console formulario. AWS KMS

  Para identificar definitivamente una clave administrada por el cliente, utilice la operación `DescribeKey`. En el caso de las claves administradas por el cliente, el valor del campo `KeyManager` de la respuesta `DescribeKey` es `CUSTOMER`. Puede usar su clave administrada por el cliente en las operaciones criptográficas y auditar el uso en AWS CloudTrail los registros. Con muchas de las Servicios de AWS que se integran AWS KMS, puede especificar una clave gestionada por el cliente para proteger los datos almacenados y gestionados por usted. Las claves gestionadas por el cliente conllevan una cuota mensual y una cuota por el uso superior a la capa AWS gratuita. Las claves gestionadas por el cliente se descontarán de las AWS KMS cuotas de tu cuenta.

Para obtener más información sobre Claves propiedad de AWS las claves administradas por el cliente, consulta las claves y AWS claves del cliente en la Guía para AWS Key Management Service desarrolladores.

> **Note**
>
> Cuando se crea un paquete de aplicaciones, AppFabric por motivos de seguridad, también se crea una función de IAM especial en su interior, Cuenta de AWS denominada función vinculada a servicios (SLR). AppFabric Permite que el servicio envíe métricas

a Amazon CloudWatch. Tras añadir un destino al registro de auditoría, la SLR permite que el servicio AppFabric de seguridad acceda a sus recursos de AWS (depósitos de Amazon S3, transmisiones de entrega de Amazon Data Firehose). Para obtener más información, consulte Uso de roles vinculados a servicios de AppFabric.

7. (Opcional) En el caso de las etiquetas, tiene la opción de agregar etiquetas a la agrupación de aplicaciones. Las etiquetas son pares de valor de clave que asignan metadatos a los recursos que crea. Para obtener más información, consulte Etiquetar sus AWS recursos en la Guía del usuario del editor de AWS etiquetas.
8. Para crear su agrupación de aplicaciones, seleccione Crear agrupación de aplicaciones.

Paso 2: autorizar aplicaciones

Una vez que el paquete de aplicaciones se haya creado correctamente, ahora puede autorizar AppFabric por motivos de seguridad la conexión e interacción con cada una de sus aplicaciones. Las aplicaciones autorizadas se cifran y almacenan en su agrupación de aplicaciones. Para configurar varias autorizaciones de aplicaciones por agrupación de aplicaciones, repita el paso de autorización de aplicaciones según sea necesario para cada aplicación.

Antes de comenzar con los pasos para autorizar las aplicaciones, revise y verifique los requisitos previos de cada aplicación, como el tipo de plan necesario, en Aplicaciones compatibles.

1. En la página de Introducción, para el Paso 2. Autorizar aplicaciones, seleccione Crear autorización de aplicaciones.
2. En la sección de autorización de aplicaciones, selecciona en el menú desplegable de aplicaciones la aplicación a la que deseas conceder permiso de seguridad AppFabric para conectarte. Las aplicaciones que se muestran son las que actualmente son compatibles AppFabric por motivos de seguridad.
3. Al seleccionar una aplicación, aparecen los campos de información obligatorios. Estos campos incluyen la ID y el nombre de inquilino y también pueden incluir la ID de cliente, el secreto de cliente o el token de acceso personal. Los valores de entrada de estos campos varían según la aplicación. Para obtener instrucciones detalladas específicas de la aplicación sobre cómo encontrar estos valores, consulte Aplicaciones compatibles.
4. (Opcional) En el caso de las etiquetas, tiene la opción de agregar etiquetas a la autorización de aplicaciones. Las etiquetas son pares de valor de clave que asignan metadatos a los recursos que crea. Para obtener más información, consulte Etiquetar AWS los recursos en la Guía del usuario del editor de AWS etiquetas.

5. Seleccione Crear autorización de aplicaciones.
6. Si aparece una ventana emergente (en función de la aplicación a la que se esté conectando), seleccione Permitir AppFabric para autorizar por motivos de seguridad la conexión con su aplicación.

   Si la autorización de la aplicación se realizó correctamente, verá un mensaje de confirmación de Autorización de la aplicación conectada en la página de Introducción.
7. Puede comprobar el estado de la autorización de la aplicación en cualquier momento en la página de Autorizaciones de aplicaciones que aparece en el panel de navegación, en el estado de cada aplicación. El estado Conectado significa que tu aplicación ha sido autorizada por motivos de seguridad AppFabric para conectarse a la aplicación y que está completa.
8. En la siguiente tabla, se muestran los posibles estados de autorización de las aplicaciones, incluidos los pasos de solución de problemas que puede seguir para corregir los errores relacionados.

Nombre del estado	Descripción del estado	Pasos para la solución de problemas
Pendiente	El estado Pendiente significa que se ha creado una autorización de aplicación para la aplicación, pero AppFabric por motivos de seguridad aún no está conectada a la aplicación.	Cuando vea este estado, seleccione Conectar en el menú desplegable Acciones de la página de Autorización de aplicaciones para iniciar una conexión. Si el error persiste, compruebe si el bloqueador de ventanas emergentes de su navegador está desactivado. Si aparece algún mensaje de error, como 400 Solicitud errónea en la ventana emergente, compruebe que toda la información, como la ID de inquilino, la ID de cliente y el secreto de cliente, se haya introducido correctam

Nombre del estado	Descripción del estado	Pasos para la solución de problemas
		ente. También es posible que la autorización de la aplicación no se haya creado correctamente. Para obtener más información, consulte Aplicaciones compatibles.
Falló la validación de la conexión	Un estado de validación de conexión fallida significa que, AppFabric por motivos de seguridad, no se puede validar la conexión de la autorización de la aplicación con una aplicación.	Compruebe que toda la información, como la ID de inquilino, la ID de cliente y el secreto de cliente, se haya introducido correctamente para la autorización de la aplicación.
Error en la rotación automática del token	Un estado de rotación automática del token fallida significa que el token de actualización de OAuth ha fallado después de que la autorización de la aplicació n se haya conectado correctamente.	Si el error persiste, compruebe la aplicació n de autenticación de la aplicación. Para obtener más información, consulte Aplicaciones compatibles.

9. Para autorizar aplicaciones adicionales, repita los pasos 1 a 8 según sea necesario.

Paso 3: configurar ingestas de registros de auditoría

Una vez que haya creado al menos una autorización de aplicación en su paquete de aplicaciones, ahora puede configurar una ingesta de registros de auditoría. La ingesta de registros de auditoría consume los registros de auditoría de una aplicación autorizada y los normaliza en el Open Cybersecurity Schema Framework (OCSF). Luego, los entrega a uno o más destinos dentro de AWS. También puede optar por entregar archivos JSON sin procesar a sus destinos.

1. En la página de Introducción, para el Paso 3. Sección de Configurar la ingesta de registros de auditoría, seleccione Configuración rápida de ingestas.

> **Note**
>
> Para una configuración más rápida, use la página de Configuración rápida de ingestas, a la que solo se puede acceder desde la página de Introducción, para crear ingestas para varias autorizaciones de aplicaciones a la vez, con el mismo destino de ingesta. Por ejemplo, el mismo bucket de Amazon S3 o el mismo flujo de datos de Amazon Data Firehose.
>
> También puede crear ingestas desde la página de Ingestas, a la que se puede acceder desde el panel de navegación. En la página de Ingestas, puede configurar una ingesta a la vez para distintos destinos. En la página de Ingestas, también puede crear una etiqueta para cada ingesta. Las siguientes instrucciones son para la página de Configuración rápida de ingestas.

2. En Seleccionar las autorizaciones de aplicaciones, seleccione las autorizaciones de aplicaciones para las que desee crear un registro de auditoría. Los nombres de los inquilinos que aparecen en el menú desplegable de autorizaciones de aplicaciones son los nombres de los inquilinos de las aplicaciones para las que previamente creó una autorización de aplicación por motivos de seguridad. AppFabric
3. En Agregar destino, seleccione un destino para las ingestas de los registros de auditoría de las aplicaciones que seleccionó. Las opciones de destino incluyen Amazon S3 (Existing Bucket), Amazon S3 (New Bucket) o Amazon Data Firehose. Si selecciona varios nombres de inquilinos, el destino que elija se aplicará a cada ingesta de una autorización de aplicación.
4. Al elegir un destino, aparecen campos obligatorios adicionales.

    a. Si elige Amazon S3 (bucket nuevo) como destino, debe introducir el nombre del bucket de S3 que quiere crear. Para obtener más instrucciones sobre cómo crear un bucket de Amazon S3, consulte Crear un destino de salida.

    b. Si elige Amazon S3 (bucket existente) como destino, seleccione el nombre del bucket de Amazon S3 que desea usar.

    c. Si eliges Amazon Data Firehose como destino, selecciona el nombre del flujo de entrega en la lista desplegable de nombres del flujo de entrega de Firehose. Para obtener más instrucciones sobre cómo crear una transmisión de entrega de Amazon Data Firehose,

consulta Crear un destino de salida y ten en cuenta la política de permisos necesaria AppFabric por motivos de seguridad.

5. En el caso de Schema & Format, puede optar por almacenar los registros de auditoría en formato RAW (JSON), OCSF (JSON), OCSF (Parquetpara los buckets de Amazon S3) o en RAW (JSON) o OCSF-JSON (para Firehose).

   El formato de datos sin procesar proporciona los datos del registro de auditoría convertidos a JSON a partir de una cadena de datos. El formato de datos OCSF normaliza los datos del registro de auditoría al esquema OCSF (Open Cybersecurity Schema Framework), AppFabric por motivos de seguridad. Para obtener más información sobre cómo se AppFabric usa OCSF, consulte. Marco de esquema de ciberseguridad abierto Solo puede seleccionar un tipo de datos de esquema y formato a la vez para una ingesta. Si desea agregar un tipo de datos de esquema y formato adicional, puede configurar un destino de ingesta adicional repitiendo el proceso de creación de la ingesta.

6. (Opcional) Si quiere añadir una etiqueta a una ingesta, vaya a la página de Ingestas desde el panel de navegación. Para ir a la página de detalles de la ingesta, seleccione el nombre de inquilino. Para las Etiquetas, tiene la opción de agregar etiquetas a la ingesta. Las etiquetas son pares de valor de clave que asignan metadatos a los recursos que crea. Para obtener más información, consulte Etiquetar AWS los recursos en la Guía del usuario del editor de AWS etiquetas.

7. Seleccione Configurar ingestas.

   Cuando haya configurado correctamente una ingesta, verá un mensaje de confirmación de Ingesta creada en la página de Introducción.

8. También puede comprobar el estado de sus ingestas y el estado de sus destinos de ingesta en cualquier momento en la página de Ingestas del panel de navegación. En esta página, puede ver el nombre del inquilino que se creó al crear la autorización de la aplicación, el destino y el estado de sus ingestas. Un estado Activado para la ingesta significa que la ingesta está habilitada. Si elige el nombre del inquilino de la autorización de una aplicación en esta página, podrá ver una página de detalles de la autorización de esa aplicación, que incluye los detalles y el estado del destino. Un estado Activo para su destino de ingesta significa que el destino está configurado correctamente y está activo. Si la autorización de la aplicación tiene el estado Conectado y el estado del destino de la ingesta es Activo, el registro de auditoría debe procesarse y entregarse. Si el estado de autorización de la aplicación o el estado del destino de la ingesta es alguno de los estados fallidos, el registro de auditoría no se procesará ni

entregará aunque el estado de ingesta esté activado. Para corregir un error de autorización de una aplicación, consulte el Paso 2. Autorizar aplicaciones.

9. En la siguiente tabla, se muestran los posibles estados de ingesta y destino de la ingesta, con los pasos de solución de problemas que puede seguir para corregir cualquier estado de error.

Nombre del estado o la provincia	Descripción	Pasos para la solución de problemas
Deshabilitada	Un estado de Desactivado para la ingesta significa que la ingesta está desactivada.	Para habilitar la ingesta, seleccione Activar en el menú desplegable Acciones de la página de Ingestas.
Con error	Un estado Error en el destino de la ingesta significa que el destino de la ingesta no acepta el registro de auditoría. Por ejemplo, este estado puede deberse a que la ubicación de almacenam iento está llena.	Para solucionar estos problemas, vaya a las consolas Amazon S3 o Firehose.

Paso 4: utilizar la herramienta de acceso de usuario

Con la herramienta de acceso de usuarios de AppFabric For Security, los equipos de administración de seguridad y TI pueden ver rápidamente quién tiene acceso a aplicaciones específicas realizando una búsqueda sencilla con la dirección de correo electrónico corporativa del empleado. Este enfoque puede resultar útil para reducir el tiempo dedicado a tareas como el desaprovisionamiento de usuarios, que pueden requerir comprobar o auditar manualmente el acceso de un usuario a todas las aplicaciones de SaaS. Si se encuentra un usuario, AppFabric por motivos de seguridad, proporciona el nombre del usuario en la aplicación y su estado de usuario en la aplicación (por ejemplo, Activo) si la aplicación lo proporciona. AppFabric por motivos de seguridad, busca en todas las aplicaciones autorizadas de un paquete de aplicaciones para obtener una lista de las aplicaciones a las que el usuario tiene acceso.

1. En la página de Introducción, para el Paso 4. Utilice la herramienta de acceso de usuario y seleccione Buscar usuario.
2. En el campo Dirección de correo electrónico, escriba la dirección de correo electrónico de un usuario y seleccione Buscar.
3. En la sección de Resultados de la búsqueda, verá una lista de todas las aplicaciones autorizadas a las que tiene acceso el usuario. Para mostrar el nombre del usuario en la aplicación y su estado (si está disponible), seleccione un resultado de la búsqueda.
4. Si aparece un mensaje de Usuario encontrado en la columna de resultados de la búsqueda, el usuario puede acceder a la aplicación que aparece en la lista. En la siguiente tabla, se muestran los posibles resultados de la búsqueda, los errores y las medidas que puede tomar para solucionarlos.

Resultado de la búsqueda	Descripción
No se encuentra al usuario	No se encuentra ningún usuario con la dirección de correo electrónico utilizada.
No se encontró un token de autorización. Conecte la autorización de la aplicación para la aplicación.	Compruebe que toda la información, como la ID de inquilino, la ID de cliente y el secreto de cliente, se haya introducido correctamente para la autorización de la aplicación.
Se rechazó el token de autorización. Conecte la autorización de la aplicación para la aplicación.	Compruebe que toda la información, como la ID de inquilino, la ID de cliente y el secreto de cliente, se haya introducido correctamente para la autorización de la aplicación.
No hemos podido rotar el token de autorizac ión. Conecte la autorización de la aplicación para la aplicación.	El token de actualización de OAuth falló después de que la autorización de la aplicación se conectara correctamente. Si el error persiste, compruebe la aplicació n de autenticación de la aplicación. Para obtener más información, consulte Aplicacio nes compatibles.

Resultado de la búsqueda	Descripción
No se encontraron los permisos necesarios. Conecte la autorización de la aplicación para la aplicación.	Compruebe que toda la información, como la ID de inquilino, la ID de cliente y el secreto de cliente, se haya introducido correctamente para la autorización de la aplicación.
La autorización de la aplicación no es válida.	Compruebe que toda la información, como la ID de inquilino, la ID de cliente y el secreto de cliente, se haya introducido correctamente para la autorización de la aplicación.
No hemos podido llamar a la API de la aplicación debido a la falta de permisos.	Compruebe que toda la información, como la ID de inquilino, la ID de cliente y el secreto de cliente, se haya introducido correctamente para la autorización de la aplicación.
Se ha superado el límite de solicitudes para la aplicación.	Se trata de un mensaje de error que se recibió de la aplicación. Puede intentar buscar una dirección de correo electrónico más tarde.
La aplicación ha detectado un error interno del servidor	Se trata de un mensaje de error que se recibió de la aplicación. Puede intentar buscar una dirección de correo electrónico más tarde.
La aplicación encontró un error de puerta de enlace incorrecta	Se trata de un mensaje de error que se recibió de la aplicación. Puede intentar buscar una dirección de correo electrónico más tarde.
La aplicación no está preparada para gestionar la solicitud	Se trata de un mensaje de error que se recibió de la aplicación. Puede intentar buscar una dirección de correo electrónico más tarde.

Resultado de la búsqueda	Descripción
La aplicación detectó un error de solicitud incorrecta.	Se trata de un mensaje de error que se recibió de la aplicación. Puede intentar buscar un correo electrónico de vuelta más tarde.
La aplicación detectó un error de servicio no disponible.	Se trata de un mensaje de error que se recibió de la aplicación. Puede intentar buscar un correo electrónico de vuelta más tarde.

Paso 5: Conéctese AppFabric para obtener datos de seguridad en herramientas de seguridad y otros destinos

Los datos de aplicaciones normalizados (o sin procesar) de AppFabric son compatibles con cualquier herramienta que permita la ingesta de datos de Amazon S3 y la integración con Firehose, incluidas las herramientas de seguridad comoBarracuda XDR,,Dynatrace,Logz.io, Netskope NetWitness Rapid7Splunk, y/o su solución de seguridad patentada. Para obtener datos de aplicaciones normalizados (o sin procesar) de una aplicación AppFabric, siga los pasos anteriores del 1 al 3. Para obtener más información sobre cómo configurar herramientas y servicios de seguridad específicos, consulte Herramientas y servicios de seguridad compatibles.

Aplicaciones compatibles

AWS AppFabric por motivos de seguridad, admite la integración con las siguientes aplicaciones. Elija el nombre de una aplicación para obtener más información sobre cómo configurar la seguridad AppFabric para conectarse a ella.

Temas

- 1Password
- Asana
- Azure Monitor
- Atlassian Confluence
- Atlassian Jira suite
- Box

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

1Password

1Passwordes un administrador de contraseñas que te ayuda a crear, almacenar y usar contraseñas seguras para todas tus cuentas en línea. También protege sus datos con cifrado, le alerta sobre las infracciones y le permite compartir contraseñas.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuarios1Password, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para 1Password
- AppFabric Conectarse a tu 1Password cuenta

AppFabric soporte para 1Password

AppFabric admite la recepción de información de usuario y registros de auditoría desde1Password.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría 1Password a los destinos admitidos, debe cumplir los siguientes requisitos:

- Debes tener un plan de suscripción 1Password Business o Enterprise de pago activo. Para obtener más información, consulta 1PasswordEnterprise en el 1Password sitio web.
- Debe tener un rol de administrador o propietario de equipo en la 1Password cuenta. Para obtener más información, consulta Grupos en el sitio web de 1Password soporte.

Consideraciones de límites de velocidad

La API de 1Password AuditLog eventos limita las solicitudes a 600 por minuto y hasta 30 000 por hora. Si se superan estos límites, se produce un error. Para obtener más información, consulta los límites de velocidad de la 1Password API en la referencia de la API de 1Password eventos.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu 1Password cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric con1Password. Para encontrar la información necesaria para realizar 1Password la autorización AppFabric, sigue estos pasos.

Crea un token de 1Password acceso personal

1Passwordadmite tokens de acceso personal para clientes públicos. Complete los siguientes pasos para generar un token de acceso personal.

1. Inicie sesión en su cuenta de 1Password.
2. Seleccione Integraciones en el panel de navegación.
3. Si hay integraciones existentes, elija Directorio. De lo contrario, continúe con el siguiente paso.
4. Elija Otros en Events Reporting Integration.
5. En la página Añadir integración, introduzca el nombre de su sistema de información de seguridad y gestión de eventos (SIEM) (por ejemplo, AppFabric Seguro)
6. Seleccione Añadir integración y, a continuación, complete los siguientes pasos en la página de configuración del token.
    a. Proporcione el nombre del token que se utilizará en el entorno AppFabric seguro.
    b. Le recomendamos que seleccione Nunca en la lista desplegable Expira después. Si se selecciona cualquier otro valor, 1Password revoca el token una vez transcurrido el tiempo de caducidad.
    c. En la sección Eventos para informar, selecciona Intentos de inicio de sesión, Eventos de uso de artículos y Eventos de auditoría.
7. Elige Issue Token para crear el token.
8. Selecciona Guardar en 1Password y sigue los pasos que se indican a continuación.
    a. El título se rellenará automáticamente en función de su sistema y de los nombres de los tokens.
    b. Selecciona Privado en Selecciona una bóveda.
    c. Seleccione Guardar.

Para obtener más información, consulte Cómo empezar a informar sobre 1Password eventos en el 1Password sitio web.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará su identificación de inquilino. El identificador de inquilino AppFabric será su dirección de 1Password inicio de sesión. Complete los siguientes pasos para encontrar su ID de inquilino.

1. Inicie sesión en su cuenta de 1Password.
2. Seleccione Configuración en el panel de navegación.
3. Tu 1Password inicio de sesión aparece en la página. Por ejemplo, example-account.1password.com.

Nombre de inquilino

Introduzca un nombre que identifique a esta organización única. 1Password AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

Token de cuenta de servicio

Debe tener un token de cuenta de servicio de una cuenta de 1Password servicio para poder incluirlo en la autorización de la AppFabric 1Password aplicación. Si no dispone de un token de cuenta de servicio, utilice las siguientes instrucciones:

AppFabric solicitará un token de cuenta de servicio. El token de la cuenta de servicio AppFabric es el token de acceso personal que ha creado. Completa los siguientes pasos en el portal de 1Password para encontrar el token de acceso personal.

1. Elija Dashsboard (Panel).
2. Elige Personas.
3. Elige el nombre del propietario de la cuenta.
4. Seleccione Privado.
5. Selecciona View Vault.
6. Elige el nombre del token.

Autorización del cliente

Cree una autorización de aplicación AppFabric utilizando el ID de inquilino, el nombre del inquilino y el token de la cuenta de servicio. A continuación, elija Connect para activar la autorización.

Asana

Asana es una plataforma de gestión del trabajo que ayuda a las personas, los equipos y las organizaciones a organizar el trabajo, desde las tareas diarias hasta las iniciativas estratégicas multifuncionales. Proporciona un sistema vivo de claridad en el que todos pueden comunicarse, colaborar y coordinar el trabajo. Con Asana, los equipos integran las herramientas empresariales fundamentales en un solo lugar para que el trabajo avance sin importar dónde se lleve a cabo.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosAsana, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Asana
- AppFabric Conectarse a su Asana cuenta

AppFabric soporte para Asana

AppFabric admite la recepción de información de usuario y registros de auditoría desdeAsana.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Asana a destinos compatibles, debe cumplir los siguientes requisitos:

- Debe tener una cuenta Enterprise de Asana. Para obtener más información sobre cómo crear o actualizar a una cuenta Enterprise, de Asana consulte Asana Enterprise en el sitio web de Asana.
- Debe tener un usuario con el rol de Superadministrador en su cuenta de Asana. Para obtener más información sobre los roles, consulte Roles de administrador y superadministrador en Asana, en el sitio web de Asana.

Consideraciones de límites de velocidad

Asana impone límites de velocidad a la API de Asana. Para obtener más información sobre los límites de velocidad para la API de Asana, consulte Límites de velocidad en el sitio web Guía para desarrolladores de Asana. Si la combinación de las aplicaciones existentes AppFabric y Asana las aplicaciones existentes supera el límite, es AppFabric posible que los registros de auditoría que aparezcan se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a su Asana cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conAsana. Para encontrar la información necesaria para realizar Asana la autorización AppFabric, sigue estos pasos.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará su identificación de inquilino. La ID de inquilino AppFabric se denomina ID de dominio inAsana. Para encontrar el ID de dominio, siga las siguientes instrucciones de la pantalla de inicio de Asana:

1. Elija la imagen de perfil de su cuenta y seleccione Consola de administrador.
2. A continuación, seleccione Configuración.
3. Desplácese hasta Configuración del dominio.
4. Introduzca el ID de dominio de esta sección en la configuración del ID de AppFabric inquilino.

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de Asana. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

Token de cuenta de servicio

Debe tener un token de cuenta de servicio de una cuenta de Asana servicio para poder incluirlo en la autorización de la AppFabric Asana aplicación. Si no dispone de un token de cuenta de servicio, utilice las siguientes instrucciones:

1. Para crear una cuenta de servicio, siga las instrucciones de Cuentas de servicio en el sitio web de Guía de Asana.
2. Copie y guarde el token de la parte inferior de la página Agregar cuenta de servicio la primera vez que vea la página Agregar cuenta de servicio.
3. Si cierra la página Agregar cuenta de servicio antes de guardar el token, debe editar su cuenta de servicio, generar un nuevo token y guardarlo.

Azure Monitor

Azure Monitores una solución de monitoreo integral para recopilar, analizar y responder a los datos de monitoreo de sus entornos locales y en la nube. Puede utilizarla Azure Monitor para maximizar la disponibilidad y el rendimiento de sus aplicaciones y servicios. Le ayuda a comprender el rendimiento de sus aplicaciones y le permite responder manual y programáticamente a los eventos del sistema.

Azure Monitorrecopila y agrega los datos de cada capa y componente de su sistema en varias suscripciones y arrendatarios de Azure y de otros fabricantes. Los almacena en una plataforma de datos común para que los consuma un conjunto común de herramientas que pueden correlacionar, analizar, visualizar o responder a los datos. También puede integrar otras herramientas de Microsoft y de terceros. El registro de Azure Monitor actividad es un registro de la plataforma que proporciona información sobre los eventos a nivel de suscripción. El registro de actividades incluye información como cuándo se modifica un recurso o se inicia una máquina virtual.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosAzure Monitor, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Azure Monitor
- Conectarse AppFabric a tu cuenta Azure Monitor

AppFabric soporte para Azure Monitor

AppFabric es capaz de recibir información de usuario y registros de auditoría de los siguientes Azure Monitor servicios:

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

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Azure Monitor a destinos compatibles, debes cumplir los siguientes requisitos:

- Debe tener una Microsoft Azure cuenta con una versión de prueba gratuita o una pay-as-you-go suscripción.
- Se requiere al menos una suscripción para acceder a los eventos incluidos en esa suscripción.

Consideraciones de límites de velocidad

Azure Monitorimpone límites de tarifas al responsable de seguridad (usuario o aplicación) que realiza las solicitudes y al identificador de suscripción o al identificador de inquilino. Para obtener más información sobre los límites de frecuencia de la Azure Monitor API, consulta Cómo se limitan las solicitudes en el Azure Resource ManagerAzure Monitor sitio web para desarrolladores.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

Conectarse AppFabric a tu cuenta Azure Monitor

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conAzure Monitor. Para encontrar la información necesaria para realizar Azure Monitor la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Azure Monitor uso de OAuth2. Complete los siguientes pasos para crear una aplicación OAuth2 en: Azure Monitor

1. Navegue hasta el Microsoft Azureportal e inicie sesión.
2. Navega hasta Microsoft EntraID.
3. Selecciona Registros de aplicaciones.
4. Elija Nuevo registro.
5. Introduzca un nombre para el cliente, como Azure Monitor OAuth Client. Será el nombre de la aplicación registrada.
6. Compruebe que los tipos de cuentas compatibles estén configurados como Arrendatario único.
7. Para el URI de redireccionamiento, selecciona Web como plataforma y agrega un URI de redireccionamiento. Usa el siguiente formato para el URI de redireccionamiento:

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

   En esa dirección, *<region>* está el código Región de AWS en el que configuraste el paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

   La respuesta de autenticación se enviará a la URI proporcionada después de autenticar correctamente al usuario. Proporcionarlo ahora es opcional y se puede cambiar más adelante, pero se requiere un valor para la mayoría de los escenarios de autenticación.
8. Elija Registro.
9. En la aplicación registrada, selecciona Certificados y secretos y, a continuación, Nuevo secreto de cliente.
10. Agrega una descripción para el secreto.
11. Selecciona la duración de caducidad del secreto. Puede seleccionar cualquier duración preestablecida en el menú desplegable o establecer una duración personalizada.
12. Elija Añadir. Los valores secretos del cliente solo se pueden ver inmediatamente después de su creación. Asegúrese de guardar el secreto en un lugar seguro antes de salir de la página.

Permisos necesarios

Debe añadir los siguientes permisos a su aplicación de OAuth. Para añadir permisos, sigue las instrucciones de la sección Añadir permisos para acceder a tu API web de la Guía para Microsoft Entra desarrolladores.

- Microsoft GraphAPI de acceso de usuario > User.Read.All (seleccione el tipo delegado)
- Microsoft GraphAPI de acceso de usuario > offline_access (seleccione el tipo delegado)
- AzureAPI de registro de auditoría de gestión de servicios > user_impersonation (seleccione el tipo delegado)

Después de añadir los permisos, para conceder el consentimiento del administrador a los permisos, sigue las instrucciones de la sección sobre el botón de consentimiento del administrador de la Guía para desarrolladores. Microsoft Entra

Autorizaciones de la aplicación

AppFabric permite recibir información de usuario y registros de auditoría de tu Azure Monitor cuenta. Para recibir tanto los registros de auditoría como los datos de los usuariosAzure Monitor, debe crear dos autorizaciones de aplicaciones, una que aparezca Azure Monitoren la lista desplegable de autorizaciones de aplicaciones y otra que se llame Registros de Azure Monitor auditoría en la lista desplegable de autorizaciones de aplicaciones. Puede usar una misma ID de inquilino, ID de cliente y clave secreta de cliente para ambas autorizaciones de aplicaciones. Para recibir los registros de auditoría, Azure Monitor necesita tanto la autorización de la aplicación Audit Logs como la Azure Monitorde la aplicación Azure MonitorAudit Logs. Para usar solo la herramienta de acceso de usuario, solo se requiere la autorización de la Azure Monitoraplicación.

ID de inquilino

AppFabric solicitará su identificación de inquilino. Complete los siguientes pasos para encontrar su ID de cliente en Azure Monitor:

1. Navegue hasta el Microsoft Azureportal.
2. Navegue hasta Azure Active Directory.
3. En la sección Registros de aplicaciones, elija la aplicación que se creó anteriormente.
4. En la sección Descripción general, copia el ID de inquilino del campo ID del directorio (inquilino).

Nombre de inquilino

Introduzca un nombre que identifique esta Azure Monitor suscripción única. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

> **Note**
>
> El nombre del inquilino debe tener un máximo de 2.048 caracteres y estar compuesto por números, letras minúsculas/mayúsculas y los siguientes caracteres especiales: punto (.), guión bajo (_), guión (-) y espacios vacíos.

ID de cliente

AppFabric solicitará un ID de cliente. Complete el siguiente procedimiento para encontrar su ID de cliente enAzure Monitor:

1. Navegue hasta el Microsoft Azureportal.
2. Navegue hasta Azure Active Directory.
3. En la sección Registros de aplicaciones, elija la aplicación que se creó anteriormente.
4. En la sección Descripción general, copie el ID de cliente del campo ID de la aplicación (cliente).

Secreto del cliente

AppFabric solicitará un secreto de cliente. El secreto de cliente de la app OAuth registrada es el que generaste en el paso 11 de la sección de creación de la aplicación OAuth. Si pierdes el secreto de cliente generado durante la creación de la aplicación OAuth, repite los pasos 8 a 11 de la sección de creación de la aplicación OAuth para volver a generar uno nuevo.

Autorización de la aplicación

Tras crear la autorización de la aplicación AppFabric, recibirás una ventana emergente en la que podrás aprobarla. Microsoft Azure Inicia sesión en tu cuenta desde la ventana y aprueba la AppFabric autorización seleccionando Permitir.

Atlassian Confluence

Cree, colabore y organice todo su trabajo en un solo lugar. Confluence es un espacio de trabajo en equipo donde se cruzan el conocimiento con la colaboración. Las páginas dinámicas le ofrecen a su

equipo un lugar donde crear, capturar y colaborar en cualquier proyecto o idea. Los espacios ayudan a su equipo a estructurar, organizar y compartir el trabajo, de modo que cada miembro del equipo tenga visibilidad del conocimiento institucional y acceso a la información que necesita para hacer su trabajo de la mejor manera. Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosConfluence, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Atlassian Confluence
- AppFabric Conectarse a tu Atlassian Confluence cuenta

AppFabric soporte para Atlassian Confluence

AppFabric admite la recepción de registros de auditoría deAtlassian Confluence.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Atlassian Confluence a destinos compatibles, debe cumplir los siguientes requisitos:

- Para acceder a los registros de auditoría, necesita tener una cuenta estándar, prémium o empresarial. Para obtener más información sobre cómo crear o actualizar al tipo de plan de Confluence correspondiente, consulte los Precios de Confluence en el sitio web de Atlassian.
- Para acceder a los registros de auditoría, debe tener los permisos de administrador de su cuenta. Para obtener más información sobre los roles, consulte Otorgar permisos de administrador a usuarios en el sitio web de Asistencia de Atlassian.

Consideraciones de límites de velocidad

Confluence impone límites de velocidad a la API de Atlassian Confluence. Si la combinación de las aplicaciones de Atlassian Confluence API existentes AppFabric y las aplicaciones existentes supera los límites, Atlassian Confluence es AppFabric posible que los registros de auditoría que aparezcan se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría,

así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Atlassian Confluence cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conAtlassian Confluence. Para encontrar la información necesaria para realizar Atlassian Confluence la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Atlassian Confluence uso de OAuth. Para crear una aplicación OAuth en Atlassian Confluence, siga los pasos siguientes:

1. Desplácese hasta la Consola de desarrollador de Atlassian.
2. Elija el icono de su perfil en la esquina superior derecha y seleccione Consola para desarrolladores.
3. Junto a Mis aplicaciones, seleccione Crear, Integración con OAuth 2.0.
4. Seleccione Permisos en el panel de navegación izquierdo y seleccione Agregar junto a la API de Confluence.
5. En Ámbitos clásicos, seleccione Usuario de lectura (`read:confluence-user`).
6. En Ámbitos detallados, seleccione Ver registros de auditoría (`read:audit-log:confluence`).
7. Seleccione Autorización en el panel de navegación izquierdo y seleccione Agregar junto a OAuth 2.0 (3LO).
8. Utilice una URL de redireccionamiento con el siguiente formato en el cuadro de texto URL de devolución de llamada y seleccione Guardar cambios.

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

   En esta URL, <region>se encuentra el código del paquete de aplicaciones Región de AWS en el que configuraste tu paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Ámbitos obligatorios

Debe agregar los siguientes alcances a su aplicación OAuth de Atlassian Confluence. Para obtener más información sobre los ámbitos, consulte Ámbitos de las aplicaciones OAuth 2.0 (3LO) y aplicaciones Forge en el sitio web para desarrolladores de Atlassian. Utilice el ámbito clásico cuando esté disponible.

- Ámbitos clásicos:
  - `read:confluence-user`
- Ámbitos detallados:
  - `read:audit-log:confluence`

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará tu ID de inquilino. El ID de inquilino AppFabric es el subdominio de tu Atlassian Confluence instancia. Puede encontrar el subdominio de su instancia de Atlassian Confluence en la barra de direcciones del navegador, entre https:// y .atlassian.net.

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de Atlassian Confluence. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente en Atlassian Confluence:

1. Desplácese hasta la Consola de desarrollador de Atlassian.
2. Elija el icono de su perfil en la esquina superior derecha y seleccione Consola para desarrolladores, Mis aplicaciones.
3. Selecciona la aplicación OAuth que utilizas para conectarte. AppFabric
4. Introduce el ID de cliente de la página de configuración en el campo ID de cliente de. AppFabric

Secreto del cliente

AppFabric solicitará un secreto de cliente. Siga los pasos siguientes para encontrar su secreto de cliente en Atlassian Confluence:

1. Desplácese hasta la Consola de desarrollador de Atlassian.
2. Elija el icono de su perfil en la esquina superior derecha y seleccione Consola para desarrolladores, Mis aplicaciones.
3. Selecciona la aplicación OAuth que utilizas para conectarte. AppFabric
4. Introduce el secreto de la página de configuración en el campo Secreto del cliente de. AppFabric

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, aparecerá una ventana emergente en la Atlassian Confluence que podrás aprobarla. Para aprobar la AppFabric autorización, selecciona permitir.

Atlassian Jira suite

Atlassian libera el potencial de cada equipo. Su ágil software de gestión de servicios de TI y gestión del trabajo ayuda a los equipos a organizar, debatir y completar el trabajo compartido. DevOps La mayoría de las empresas incluidas en la lista Fortune 500 y más de 240 000 empresas de todos los tamaños en todo el mundo —entre los que se encuentran la NASA, Kiva, Deutsche Bank y Salesforce— confían en las soluciones de Atlassian para ayudar a sus equipos a trabajar mejor juntos y a ofrecer resultados de calidad a tiempo. Obtenga más información sobre los productos Atlassian, incluidos Jira Software, Confluence, Jira Service Management, Trello, Bitbucket y Jira Align en Atlassian.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuarios de Jira suite (distintosJira Align), normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para el Jira suite
- AppFabric Conectarse a tu Jira cuenta

AppFabric soporte para el Jira suite

AppFabric admite la recepción de información de usuario y registros de auditoría desdeJira suite, con la excepción deJira Align.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría de los destinos Jira suite a los que se admiten, debe cumplir los siguientes requisitos:

- Debe tener un plan estándar de Jira o superior. Para obtener más información sobre las capacidades de los planes de Jira, consulte las páginas de precios de Software Jira, Gestión de servicios de Jira, Gestión del trabajo de Jira y Product Discovery de Jira.
- Debe tener un usuario con el rol de Administrador de la organización en su cuenta de Jira. Para obtener más información sobre los roles, consulte Otorgar permisos de administrador a usuarios en el sitio web de Asistencia de Atlassian.

Consideraciones de límites de velocidad

El paquete de Jira impone límites de velocidad a la API de Jira. Para obtener más información sobre los límites de velocidad para la API de Jira suite, consulte Límites de velocidad en el sitio web Guía para desarrolladores de Atlassian. Si la combinación de las aplicaciones de Jira API existentes AppFabric y las aplicaciones de API existentes supera el límite, es AppFabric posible que los registros de auditoría que aparezcan se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Jira cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conJira. Para encontrar la información necesaria para realizar Jira la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Jira suite uso de OAuth. Para crear una aplicación OAuth en Jira, siga los pasos siguientes:

1. Desplácese hasta la Consola de desarrollador de Atlassian.
2. Junto a Mis aplicaciones, seleccione Crear, Integración con OAuth 2.0.
3. Asigne un nombre a su aplicación y elija Crear.
4. Vaya a la sección Autorización y seleccione Agregar junto a OAuth 2.0.
5. Use una URL con el siguiente formato en el campo URL de devolución de llamada y seleccione Guardar cambios.

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

   En esta URL, <region>está el código Región de AWS en el que configuraste tu paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
6. Ve a la sección Configuración, copia tu ID de cliente y tu secreto de cliente y guárdalos para usarlos en la autorización de la AppFabric aplicación.

Ámbitos obligatorios

Debe agregar los siguientes ámbitos a la página Permisos de su aplicación OAuth de Jira:

- En los ámbitos clásicos:
  - API de Jira > `read:jira-user`
- En los ámbitos granulares:
  - API de Jira > `read:audit-log:jira`
  - API de Jira > `read:user:jira`

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará tu ID de inquilino. El ID de inquilino AppFabric es el subdominio de tu Jira instancia. Puede encontrar el subdominio de su instancia de Jira en la barra de direcciones del navegador, entre https:// y .atlassian.net.

Nombre de inquilino

Introduce un nombre que identifique este Jira servidor único. AppFabricusa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará tu ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente en Jira:

1. Desplácese hasta la Consola de desarrollador de Atlassian.
2. Selecciona la aplicación OAuth que utilizas para conectarte. AppFabric
3. Introduce el ID de cliente de la página de configuración en el campo ID de cliente de. AppFabric

Secreto del cliente

AppFabric solicitará su secreto de cliente. El secreto del cliente AppFabric es el secreto deJira. Para encontrar su secreto en Jira, siga los pasos siguientes:

1. Desplácese hasta la Consola de desarrollador de Atlassian.
2. Selecciona la aplicación OAuth que utilizas para conectarte. AppFabric
3. Introduce el secreto de la página de configuración en el campo Secreto del cliente de. AppFabric

Cómo aprobar la autorización

Después de crear la autorización de la aplicación, AppFabric recibirá una ventana emergente Jira para aprobar la autorización. Para aprobar la AppFabric autorización, selecciona Permitir.

Box

Boxes la nube de contenido líder, una plataforma única que permite a las organizaciones gestionar todo el ciclo de vida del contenido, trabajar de forma segura desde cualquier lugar e integrar todas best-of-breed las aplicaciones.

Puede utilizarlos AWS AppFabric para recibir registros de auditoría y datos de usuariosBox, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Box
- AppFabric Conectarse a su Box cuenta

AppFabric soporte para Box

AppFabric admite la recepción de información de usuario y registros de auditoría desdeBox.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Box a los destinos admitidos, debe cumplir los siguientes requisitos:

- Para acceder a los registros de auditoría, debes tener una suscripción de pago activa a los planes Business, Business Plus, Enterprise o Enterprise Plus.
- Debe tener un usuario con privilegios de administrador.
- Debe tener habilitada la autenticación de dos factores en su Box cuenta para ver y copiar el secreto de cliente de la aplicación desde la pestaña de configuración.

Consideraciones de límites de velocidad

Box impone límites de velocidad a la API de Box. Para obtener más información sobre los límites de velocidad de la Box API, consulta los límites de velocidad en el sitio web de la Guía para Box desarrolladores. Si la combinación de las aplicaciones existentes AppFabric y Box las aplicaciones existentes supera el límite, es AppFabric posible que los registros de auditoría que aparezcan se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos en un evento de auditoría hasta que se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto se puede personalizar a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a su Box cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, tendrás que autorizarlo AppFabric conBox. Para encontrar la información necesaria para realizar Box la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Box uso de OAuth. Siga los siguientes pasos para crear una aplicación OAuth en. Para obtener más informaciónBox, consulte Creación de una aplicación OAuth en el sitio web. Box

1. Inicia sesión en la consola de Box desarrolladores y ve a ella.
2. Elija Crear nueva aplicación.
3. Selecciona Aplicación personalizada en la lista de tipos de aplicaciones. Aparecerá un modal para solicitar una selección para el siguiente paso.
4. Introduce un nombre y una descripción de la aplicación.
5. Elija Integración en la lista desplegable Propósito.
    a. Seleccione Seguridad y conformidad en la lista desplegable de categorías.
    b. Introduzca AWS AppFabric Secureel campo ¿Con qué sistema externo se está integrando? cuadro de texto.
6. Elija la autenticación del servidor (concesión de credenciales de cliente) si desea verificar la identidad de la aplicación con un ID de cliente y un secreto de cliente.
7. Seleccione Crear una aplicación.
8. Elija la pestaña Configuración.
9. En la sección Nivel de acceso a la aplicación de la página, elija App + Enterprise Access.
10. En la sección Ámbitos de la aplicación de la página, seleccione Administrar usuarios y Administrar propiedades empresariales.
11. Seleccione Guardar cambios.

El Box administrador debe autorizar la aplicación en la Consola de Box administración para poder utilizarla. Complete los siguientes pasos para solicitar una autorización.

a. Seleccione la pestaña Autorización de su aplicación en la Consola de desarrolladores.
b. Selecciona Revisar y enviar para enviar un correo electrónico al administrador de tu Box empresa para su aprobación. Para obtener más información, consulta la sección Autorización en la Boxguía.

> **Note**
>
> Debes volver a enviar tu aplicación si se realiza algún cambio después del envío.

Ámbitos obligatorios

Se requieren los siguientes ámbitos de solicitud. Para obtener más información sobre los ámbitos, consulte Ámbitos en el sitio web de documentación de Box.

- Gestione las propiedades empresariales () `manage_enterprise_properties`
- Administrar usuarios (`manage_managed_users`)

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará una identificación de inquilino. El ID de inquilino AppFabric es el Box Enterprise ID. El Box Enterprise ID se encuentra en la consola de administración, en Cuenta y facturación > Información de la cuenta > Enterprise ID. Para obtener más información, consulta el Enterprise ID en el sitio web de documentación de Box.

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de Box. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID y clave secreta de cliente

1. Inicia sesión en la Box Consola para desarrolladores y ve a ella.

2. Selecciona Mis aplicaciones en el menú de navegación.
3. Elige la aplicación OAuth que utilizas para conectarte. AppFabric
4. Elija la pestaña Configuración.
5. Ve a la sección Credenciales de OAuth 2.0 de la página.
6. Introduce el ID de cliente de tu ID de cliente de OAuth en el campo ID de cliente de. AppFabric
7. Selecciona Fetch Client Secret.
8. Introduce el secreto de cliente de tu secreto de cliente de OAuth en el campo Secreto de cliente de. AppFabric

Cisco Duo

Cisco Duoprotege contra las infracciones con un paquete de gestión de acceso líder que proporciona sólidas defensas de varios niveles y capacidades innovadoras que permiten la entrada de los usuarios legítimos y mantienen alejados a los malos actores. Para cualquier organización preocupada por la posibilidad de sufrir una violación de seguridad y que necesite una solución rápida, Cisco Duo rápida, que ofrezca una seguridad sólida y, al mismo tiempo, mejore la productividad de los usuarios. Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosCisco Duo, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Cisco Duo
- Conéctate AppFabric a tu Cisco Duo cuenta

AppFabric soporte para Cisco Duo

AppFabric admite la recepción de información de usuario y registros de auditoría desdeCisco Duo.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Cisco Duo a destinos compatibles, debe cumplir los siguientes requisitos:

- Para acceder a los registros de auditoría, debe tener una suscripción activa a las ediciones Duo Essentials, Duo Advantage o Duo Premier. Como alternativa, también pueden acceder los nuevos

clientes con una versión de prueba Advantage o Premier. Para obtener más información sobre Cisco Duo las ediciones, consulta Ediciones y precios.

- Debe ser administrador con función de propietario para crear o modificar la API de administrador.
- Debes añadir permisos de «conceder recursos de lectura y registro» para acceder a los registros de auditoría en la API de administración.

Consideraciones de límites de velocidad

Cisco Duo impone límites de velocidad a la API de Cisco Duo. Para obtener más información sobre los límites de velocidad de la Cisco Duo API, consulta los límites de velocidad en los registros de autenticación. Si la combinación de las aplicaciones de Cisco Duo API existentes AppFabric y las aplicaciones existentes superan los límites, Cisco Duo es AppFabric posible que los registros de auditoría se retrasen. Póngase en contacto con Cisco Duo si necesita aumentar el límite de velocidad.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

Conéctate AppFabric a tu Cisco Duo cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conCisco Duo. Para encontrar la información necesaria para realizar Cisco Duo la autorización AppFabric, sigue estos pasos.

Crea una aplicación Cisco Duo de API de administración

AppFabric se integra con Cisco Duo el uso de un token de servicio de API. Para crear una aplicación enCisco Duo, sigue estos pasos.

- Para crear una aplicación de API de Cisco Duo administración, sigue las instrucciones de los primeros pasos de la API de Cisco Duo administración.

Permisos necesarios

Debes añadir los siguientes ámbitos a tu Cisco Duo aplicación:

- Otorgue el registro de lectura
- Grant lee el recurso

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará una identificación de inquilino. Puedes encontrar el ID de inquilino en el Cisco Duo nombre del servidor. Para encontrar el nombre de hostCisco Duo, sigue estos pasos.

1. Ve a la página de inicio Cisco Duo de sesión del administrador e inicia sesión.
2. Ve a Aplicaciones y, a continuación, selecciona Proteger una aplicación.
3. Busque la entrada API de administración en la lista de aplicaciones y, a continuación, elija Proteger en el extremo derecho para configurar la aplicación y obtener el nombre de host de la API.
4. El nombre de host de la API tiene el formato siguiente: el `api-<tenant-id>.duosecurity.com` ID del *<tenant-id>* inquilino.

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de Cisco Duo. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

Token de servicio

AppFabric solicitará un token de servicio. El token de servicio es una clave de integración y una clave secreta separadas por dos puntos con el siguiente formato.

```
integrationkey:secretkey
```

Para encontrar la clave de integración y la clave secretaCisco Duo, sigue estos pasos.

1. Ve a la página de inicio de sesión del Cisco Duo administrador e inicia sesión.
2. Ve a Aplicaciones y, a continuación, selecciona Proteger una aplicación.
3. «Haga clic en Proteger una aplicación y busque la entrada correspondiente a la API de administración en la lista de aplicaciones. Haga clic en Proteger en el extremo derecho para

configurar la aplicación. Desplácese hacia abajo hasta la sección de ámbitos y añada **`Grant read log`** y. **`Grant read resource`**

Dropbox

Dropbox ayuda a su organización a trabajar mejor y más rápido al reunir a sus empleados, sin importar en qué estén trabajando, dónde estén trabajando o qué tipo de herramientas utilicen. Permite a los usuarios acelerar la innovación y la eficiencia al proporcionar una forma sencilla y segura de compartir contenido. Dropbox es un lugar para mantener la vida organizada y el trabajo en movimiento. Con más de 700 millones de usuarios registrados en 180 países, Dropbox tiene la misión de diseñar una forma más inteligente de trabajar.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosDropbox, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Dropbox
- AppFabric Conectarse a tu Dropbox cuenta

AppFabric soporte para Dropbox

AppFabric admite la recepción de información de usuario y registros de auditoría desdeDropbox.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Dropbox a destinos compatibles, debe cumplir los siguientes requisitos:

- Debe tener una cuenta Dropbox Business. Para obtener más información sobre cómo crear o actualizar a una cuenta de Dropbox Business, consulte Dropbox Business en el sitio web de Dropbox.
- Debe tener un usuario con el rol de Admin. de equipo en su cuenta de Dropbox. Para obtener más información sobre los roles, consulte Cómo cambiar los derechos de administrador de su equipo de Dropbox en el sitio web del Dropbox Centro de ayuda de .

Consideraciones de límites de velocidad

Dropbox impone límites de velocidad a la API de Dropbox. Para obtener más información sobre los límites de velocidad para la API de Dropbox, consulte Límites de velocidad en la Guía de rendimiento de Dropbox. Si la combinación de las aplicaciones de Dropbox API existentes AppFabric y las aplicaciones de API existentes supera el límite, es AppFabric posible que los registros de auditoría se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Dropbox cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conDropbox. Para encontrar la información necesaria para realizar Dropbox la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Dropbox uso de OAuth. Para crear una aplicación OAuth en Dropbox, siga los pasos siguientes:

1. Seleccione Crear aplicación en la consola de aplicaciones de Dropbox en https://www.dropbox.com/developers/apps.
2. En la página de configuración de la nueva aplicación, seleccione Acceso limitado para la API.
3. A continuación, seleccione Completo Dropbox para establecer el tipo de acceso.
4. Asigne un nombre a su aplicación OAuth y, a continuación, elija Crear aplicación para finalizar la configuración inicial de la aplicación OAuth.
5. En la página de información de la aplicación, agregue una URL de redireccionamiento con el siguiente formato en el campo URI de redireccionamiento de OAuth2.

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

   En esta URL, *<region>* está el código Región de AWS en el que configuraste tu paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de

Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

6. Elija Añadir.
7. Copia y guarda la clave y el secreto de la aplicación para usarlos en la autorización de la AppFabric aplicación.
8. Puede dejar los valores predeterminados en todos los demás campos de la pestaña Configuración.

Ámbitos obligatorios

Debe agregar los siguientes ámbitos a su aplicación de Dropbox mediante la pestaña Permisos en la pantalla de información de la aplicación:

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

Seleccione Enviar cuando haya terminado.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará su identificación de inquilino. Introduzca cualquier valor que identifique de forma exclusiva su cuenta de Dropbox, como el nombre del equipo.

Nombre de inquilino

Introduzca un nombre que identifique esta Dropbox cuenta única. AppFabricusa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. El ID de cliente que aparece AppFabric es Dropbox la clave de tu aplicación. Para encontrar la clave de aplicación de Dropbox, siga los pasos siguientes:

1. Vaya a la consola de aplicaciones Dropbox en https://www.dropbox.com/developers/apps.
2. Busca la aplicación que utilizas para conectarte AppFabric.
3. Busque la clave de la aplicación en la sección Estado de la página de información de la aplicación.
4. Introduce la clave de la Dropbox aplicación en el campo ID de cliente de AppFabric.

Secreto del cliente

AppFabric solicitará un secreto de cliente. El secreto de cliente AppFabric es el secreto de tu Dropbox aplicación. Para encontrar el secreto de su aplicación de Dropbox, siga los pasos siguientes:

1. Vaya a la consola de aplicaciones Dropbox en https://www.dropbox.com/developers/apps.
2. Busca la aplicación que utilizas para conectarte AppFabric.
3. Busque el secreto de la aplicación en la sección Estado de la página de información de la aplicación.
4. Introduce el secreto de la Dropbox aplicación en el campo Secreto del cliente de AppFabric.

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, recibirás una ventana emergente en la Dropbox que podrás aprobarla. Para aprobar la AppFabric autorización, selecciona Permitir.

Genesys Cloud

Genesys Cloudcrea conversaciones fluidas a través de canales digitales y de voz en una all-in-one interfaz sencilla. Esto permite a las empresas ofrecer experiencias excepcionales a empleados y clientes, y aprovechar las ventajas de una implementación rápida, menos compleja y una administración sencilla. Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosGenesys Cloud, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Genesys Cloud
- AppFabric Conectarse a tu Genesys Cloud cuenta

AppFabric soporte para Genesys Cloud

AppFabric admite la recepción de información de usuario y registros de auditoría desdeGenesys Cloud.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Genesys Cloud a los destinos admitidos, debe cumplir los siguientes requisitos:

- Debe tener una cuenta de Genesys Cloud.
- Debe tener un usuario con el rol de administrador en su cuenta de Genesys Cloud.

Consideraciones de límites de velocidad

Genesys Cloud impone límites de velocidad a la API de Genesys Cloud. Para obtener más información sobre los límites de tasa para la API de Genesys Cloud, consulte Límites de tasa en el sitio web de Genesys Cloud Developer.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Genesys Cloud cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conGenesys Cloud. Para encontrar la información necesaria para realizar Genesys Cloud la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Genesys Cloud uso de OAuth. Para crear una aplicación OAuth en Genesys Cloud, siga los pasos siguientes:

1. Siga las instrucciones de Crear un cliente OAuth en el sitio web del Centro de recursos de Genesys Cloud.

En Tipos de concesiones, seleccione Autorización del código.

2. Use una URL de redireccionamiento con el siguiente formato como el URI de redireccionamiento autorizado.

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

En esta URL, <region>se encuentra el código del paquete de aplicaciones Región de AWS en el que configuraste tu paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

3. Seleccione la casilla Ámbito para mostrar una lista de los ámbitos disponibles para su aplicación. Selecciona el alcance `audits:readonly` y`users:readonly`. Para obtener información sobre los ámbitos, consulte Ámbitos de OAuth en el Centro para desarrolladores de Genesys Cloud.
4. Seleccione Guardar. Genesys Cloud crea un ID de cliente y un secreto de cliente (token).

Ámbitos obligatorios

Debe añadir los siguientes ámbitos a su aplicación OAuth de Genesys Cloud:

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

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará su identificación de inquilino. El ID de inquilino AppFabric es el nombre de su Genesys Cloud instancia. Puede encontrar su ID de inquilino en la barra de dirección del navegador. Por ejemplo, `usw2.pure.cloud` es el ID de inquilino en la siguiente URL `https://login.usw2.pure.cloud`.

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de Genesys Cloud. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente en Genesys Cloud:

1. Elija Administrador.
2. En Integraciones, seleccione OAuth.
3. Elija el cliente de OAuth para obtener el ID de cliente.

Secreto del cliente

AppFabric solicitará un secreto de cliente. Siga los pasos siguientes para encontrar su secreto de cliente en Genesys Cloud:

1. Elija Administrador.
2. En Integraciones, seleccione OAuth.
3. Elija el cliente de OAuth para obtener el secreto del cliente.

GitHub

GitHub es una plataforma y un servicio basado en la nube para el desarrollo de software y el control de versiones mediante Git, que permite a los desarrolladores almacenar y administrar su código. Proporciona el control de versiones distribuido de Git más control de acceso, seguimiento de errores, solicitudes de características de software, administración de tareas, integración continua y wikis para cada proyecto. Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosGitHub, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para GitHub
- AppFabric Conectarse a su GitHub cuenta

AppFabric soporte para GitHub

AppFabric admite la recepción de información de usuario y registros de auditoría desdeGitHub.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría GitHub a destinos compatibles, debe cumplir los siguientes requisitos:

- Para acceder a los registros de auditoría, debe tener una cuenta empresarial.
- Para acceder a los registros de auditoría empresarial, debe tener el rol de administrador de su cuenta empresarial.
- Para obtener los registros de auditoría de la organización, debe ser el propietario de la organización.

Consideraciones de límites de velocidad

GitHub impone límites de velocidad a la API de GitHub. Para obtener más información sobre los límites de velocidad para la API de GitHub, consulte Límites y asignaciones de solicitudes de API en el sitio web de GitHub. Si la combinación de las aplicaciones de GitHub API existentes AppFabric y las aplicaciones de API existentes supera los GitHub's límites, es AppFabric posible que se retrase la publicación de los registros de auditoría.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a su GitHub cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conGitHub. Para encontrar la información necesaria para realizar GitHub la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el GitHub uso de OAuth. Siga estos pasos para crear una aplicación OAuth en GitHub. Para obtener más información, consulte Creación de GitHubs aplicaciones en el GitHub sitio web.

1. Elija la foto de perfil que se encuentra en la esquina superior derecha de la página y elija Configuración.

2. En el panel de navegación izquierdo, elija Configuración del desarrollador.
3. En el panel de navegación izquierdo, elija Aplicaciones de OAuth.
4. Seleccione Nueva aplicación OAuth.

> **Note**
>
> Este botón tendrá la etiqueta Registrar una nueva aplicación si no ha creado previamente una aplicación OAuth.

5. Ingrese el nombre de la aplicación en Nombre de la aplicación.
6. Introduzca la URL completa de la instancia de la aplicación en el cuadro de texto URL de la página de inicio.
7. (Opcional) Ingrese una descripción de la aplicación en el cuadro de texto Descripción de la aplicación. Los usuarios verán esta descripción.
8. Introduzca una URL con el siguiente formato en el cuadro de texto URL de devolución de llamada de autorización.

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

   En esta URL, <region>se encuentra el código Región de AWS en el que configuraste el paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
9. Elija Activar el flujo de dispositivos si su aplicación OAuth utilizará el flujo de dispositivos para identificar y autorizar a los usuarios. Para obtener más información sobre el flujo de dispositivos, consulte Autorizar aplicaciones OAuth en el sitio web de GitHub.
10. Seleccione Registrar aplicación.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará tu ID de inquilino. El ID del inquilino se debe proporcionar en uno de los siguientes formatos:

Registro de auditoría empresarial:

Utilice el registro de auditoría de la empresa si desea conocer las acciones combinadas de todas las organizaciones que son propiedad de su cuenta empresarial.

Para usar el registro de auditoría empresarial, el ID de inquilino es el ID empresarial de su cuenta. Puede encontrar su ID empresarial en la barra de direcciones del navegador. Por ejemplo, *exampleenterprise* es el ID empresarial en la siguiente URL: `https://github.com/settings/enterprises/`*examplenterprise*.

Al especificar el ID de inquilino para el registro de auditoría empresarial, debe añadirle el prefijo `enterprise:`. Por lo tanto, especifique el ejemplo anterior como `enterprise:examplenterprise`.

Registro de auditoría de la organización:

Utilice el registro de auditoría de la organización como administrador de la organización si desea conocer las acciones realizadas por los miembros de su organización. Incluye detalles como quién realizó la acción, en qué consistió y cuándo se realizó.

Para usar el registro de auditoría de la organización, el ID de inquilino es el ID de su organización. Puede encontrar el ID de su organización en la barra de direcciones del navegador. Por ejemplo, *exampleorganization* es el ID de la organización en la siguiente URL: `https://github.com/settings/organizations/`*exampleorganization*.

Cuando especifique el ID de inquilino para el registro de auditoría de la organización, debe anteponerle el prefijo `organization:`. Por lo tanto, especifique el ejemplo anterior como `organization:exampleorganization`.

Nombre de inquilino

Introduzca un nombre que identifique a esta GitHub empresa u organización única. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente en GitHub:

1. Elija la foto de perfil que se encuentra en la esquina superior derecha de la página y elija Configuración.

2. En el panel de navegación izquierdo, elija Configuración del desarrollador.
3. En el panel de navegación izquierdo, elija Aplicaciones de OAuth.
4. Elija la aplicación OAuth específica y, a continuación, busque el valor del ID de cliente.

Secreto del cliente

AppFabric solicitará un secreto de cliente. Siga los pasos siguientes para encontrar su secreto de cliente en GitHub.

1. Elija la foto de perfil que se encuentra en la esquina superior derecha de la página y elija Configuración.
2. En el panel de navegación izquierdo, elija Configuración del desarrollador.
3. En el panel de navegación izquierdo, elija Aplicaciones de OAuth.
4. Elija la aplicación OAuth específica y, a continuación, busque el valor del Secreto de cliente. Si no puede encontrar un secreto de cliente existente, es posible que tenga que generar uno nuevo.

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, recibirás una ventana emergente GitHub para aprobarla. Para aprobar la AppFabric autorización, selecciona Permitir.

Asegúrese de que sus organizaciones hayan concedido el acceso a la aplicación OAuth, si las restricciones de acceso a la aplicación OAuth están habilitadas.

Google Analytics

Google Analyticses un servicio de análisis web que proporciona estadísticas y herramientas analíticas básicas para la optimización de motores de búsqueda (SEO) y con fines de marketing. Google Analyticsse utiliza para realizar un seguimiento del rendimiento del sitio web y recopilar información sobre los visitantes. Puede ayudar a las organizaciones a determinar las principales fuentes de tráfico de usuarios, evaluar el éxito de sus actividades y campañas de marketing, realizar un seguimiento del cumplimiento de los objetivos (como las compras o la adición de productos a los carritos), descubrir patrones y tendencias en la participación de los usuarios y obtener otra información sobre los visitantes, como la demografía. Los sitios web minoristas pequeños y medianos suelen utilizar Google Analytics para obtener y analizar diversos análisis del

comportamiento de los clientes, que se pueden utilizar para mejorar las campañas de marketing, impulsar el tráfico del sitio web y retener mejor a los visitantes.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosAzure Monitor, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Google Analytics
- AppFabric Conectarse a tu Google Analytics cuenta

AppFabric soporte para Google Analytics

AppFabric admite la recepción de registros de auditoría deGoogle Analytics.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Google Analytics a destinos compatibles, debe cumplir los siguientes requisitos:

- Debe ser el administrador de la Google Analytics cuenta.
- AppFabric Para poder entregar los registros, debes habilitar la API de Google Analytics administración en tu Google Cloud proyecto. Asegúrate de usar un proyecto nuevo al configurar la aplicación Google Analytics OAuth.

Consideraciones de límites de velocidad

Google Analytics impone límites de velocidad a la API de Google Analytics. Para obtener más información sobre los límites de velocidad de las Google Analytics API, consulta Límites y cuotas en el sitio web de Google Analytics. Si la combinación de las aplicaciones de la API de Google Analytics AppFabric y las existentes supera el límite, es AppFabric posible que los registros de auditoría que aparezcan se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría,

así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Google Analytics cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conGoogle Analytics. Sigue los siguientes pasos para encontrar la información necesaria para realizar la autorización Google Analytics AppFabric.

Cómo crear una aplicación OAuth

AppFabric se integra con el Google Analytics uso de OAuth. Complete los siguientes pasos para crear una aplicación OAuth en: Google Analytics

1. Para configurar la pantalla de consentimiento de OAuth, sigue las instrucciones de la sección Configurar la pantalla de consentimiento de OAuth de la Guía para desarrolladores de Google en el sitio web de Google.
2. Selecciona Externo como tipo de usuario
3. Para configurar las credenciales de OAuth AppFabric, sigue las instrucciones de la sección Credenciales del ID de cliente de OAuth de la página Crear credenciales de acceso de la Guía para desarrolladores de Google.
4. Utilice una URL de redireccionamiento con el siguiente formato.

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

   En esa dirección, *<region>* está el código Región de AWS en el que configuraste el paquete de aplicaciones. AppFabric Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Ámbitos obligatorios

Debes añadir el siguiente ámbito a tu aplicación Google Analytics OAuth:

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

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará una identificación de inquilino. El identificador de inquilino AppFabric es el identificador de su Google Analytics cuenta.

1. Ve a la página de Google Analytics inicio.
2. Selecciona Admin en el panel de navegación.
3. Encontrarás el ID de tu cuenta en Cuenta > Configuración de la cuenta > Detalles de la cuenta > ID de cuenta.

Nombre de inquilino

Introduzca un nombre que identifique a esta Google Analytics organización única. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. Sigue los siguientes pasos para encontrar tu ID de cliente enGoogle Analytics:

1. Ve a la página de credenciales.
2. En la sección ID de cliente de OAuth 2.0, elige el ID de cliente que has creado.
3. El ID de cliente aparece en la sección de información adicional de la página.

Secreto del cliente

AppFabric solicitará un secreto de cliente. Sigue los siguientes pasos para encontrar el secreto de tu cliente enGoogle Analytics:

1. Ve a la página de credenciales.
2. En la sección ID de cliente de OAuth 2.0, elige el nombre del cliente.
3. El secreto del cliente aparece en la sección Secretos del cliente de la página.

Autorización de la aplicación

Tras crear la autorización de la aplicación AppFabric , aparecerá una ventana emergente en la Google Analytics que podrás aprobar la autorización. Para aprobar la AppFabric autorización, selecciona Permitir.

Google Workspace

Google Workspace es un conjunto de herramientas, software y productos de computación en la nube, productividad y colaboración que Google ha desarrollado y comercializa.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosGoogle Workspace, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Google Workspace
- AppFabric Conectarse a su Google Workspace cuenta

AppFabric soporte para Google Workspace

AppFabric admite la recepción de información de usuario y registros de auditoría desdeGoogle Workspace.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Google Workspace a los destinos admitidos, debe cumplir los siguientes requisitos:

- Debe estar suscrito a un plan de Standard de Google Workspace Enterprise. Para obtener más información sobre la creación o actualización al plan Standard de Google Workspace Enterprise, consulte el sitio web de Planes de Google Workspace.
- Debe tener un usuario con el rol de Administrador en su Google Workspace.
- AppFabric Para entregar los registros, debes habilitar la API del SDK de administración de Google en tu proyecto de Google Cloud. Para obtener más información, consulte Cómo habilitar las API de Google Workspace en la Google WorkspaceGuía para desarrolladores.

Consideraciones de límites de velocidad

Google Workspace impone límites de velocidad a la API de Google Workspace. Para obtener más información sobre los límites de velocidad para la API de Google Workspace, consulte Límites y cuotas en la Guía para administradores de Google Workspace en el sitio web de Google Workspace. Si la combinación de las aplicaciones de Google Workspace API existentes AppFabric y las aplicaciones de API existentes supera el límite, es AppFabric posible que los registros de auditoría se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos en la mayoría de los eventos de auditoría y de hasta 4 horas en el caso de que algunos eventos de auditoría se entreguen a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Para obtener más información, consulta el artículo sobre retención de datos y tiempos de espera en el sitio web de ayuda para WorkSpace administradores de Google. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a su Google Workspace cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conGoogle Workspace. Para encontrar la información necesaria para realizar Google Workspace la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Google Workspace uso de OAuth. Para crear una aplicación OAuth en Google Workspace, siga los pasos siguientes:

1. Para configurar la pantalla de consentimiento de OAuth, siga las instrucciones de la sección Configurar la pantalla de consentimiento de OAuth en la Guía para desarrolladores de Google Workspace en el sitio web de Google Workspace.

   Seleccione Interno como Tipo de usuario.
2. Para configurar las credenciales de OAuth AppFabric, sigue las instrucciones de la sección Credenciales de ID de cliente de OAuth de la página Crear credenciales de acceso de la Guía para desarrolladores. Google Workspace
3. Utilice una URL de redireccionamiento con el siguiente formato.

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

En esta URL, *<region>* se encuentra el código Región de AWS en el que configuraste el paquete de aplicaciones. AppFabric Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Ámbitos obligatorios

Debe añadir los siguientes ámbitos a su aplicación OAuth de Google Workspace:

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

Si no ve estos ámbitos, agregue la API de SDK de administración a su Google biblioteca de API de Cloud.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará tu ID de inquilino. El ID de inquilino que aparece AppFabric es el ID de tu Google Workspace proyecto. Para encontrar el ID de su proyecto, consulte Localizar el ID de proyecto en el sitio web de Ayuda para la consola de API de Google.

Nombre de inquilino

Introduzca un nombre que identifique este Google Workspace único. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará tu ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente:

1. Busque su ID de cliente con la información de la sección Ver credenciales de la página Administrar credenciales en la Guía para desarrolladores de Google Workspace.
2. Introduce el ID de cliente de tu cliente de OAuth en el campo ID de cliente de. AppFabric

Secreto del cliente

AppFabric solicitará tu secreto de cliente. Siga los pasos siguientes para encontrar su secreto de cliente:

1. Busque su secreto de cliente con la información de la sección Ver credenciales de la página Administrar credenciales en la Guía para desarrolladores de Google Workspace.
2. Si necesita restablecer su secreto de cliente, siga las instrucciones de la sección Restablecer el secreto de cliente de la página Administrar credenciales en la Guía para desarrolladores de Google Workspace.
3. Introduzca su secreto de cliente en el campo Secreto de cliente de AppFabric.

Cómo aprobar la autorización

Después de crear la autorización de la aplicación, AppFabric recibirá una ventana emergente Google Workspace para aprobar la autorización. Para aprobar la AppFabric autorización, selecciona permitir.

HubSpot

HubSpot es una plataforma para clientes con todo el software, las integraciones y los recursos que necesita para conectar sus servicios de marketing, ventas, administración de contenido y servicio al cliente. La plataforma conectada de HubSpot le permite hacer crecer su negocio más rápido al centrarse en lo que más importa: sus clientes. Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosHubSpot, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para HubSpot
- AppFabric Conectarse a tu HubSpot cuenta

AppFabric soporte para HubSpot

AppFabric admite la recepción de información de usuario y registros de auditoría desdeHubSpot.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría HubSpot a los destinos admitidos, debe cumplir los siguientes requisitos:

- Debe tener una cuenta con la suscripción Enterprise en HubSpot para acceder a los registros de auditoría. Para obtener más información sobre las suscripciones de HubSpot, consulte Administrar la suscripción de HubSpot en la Base de conocimientos de HubSpot.
- Debe tener una cuenta de desarrollador y una aplicación asociadas a la cuenta.
- Debe ser superadministrador para instalar aplicaciones en su cuenta de HubSpot o tener permiso de acceso a App Marketplace más los permisos de usuario para aceptar los ámbitos que solicita la aplicación.

Consideraciones de límites de velocidad

HubSpot impone límites de velocidad a la API de HubSpot. Para obtener más información sobre los límites de tasa de la API HubSpot, incluidos los límites para las aplicaciones que utilizan OAuth, consulta Límites de tasa en el sitio web de HubSpot. Si la combinación de las aplicaciones de HubSpot API existentes AppFabric y las aplicaciones existentes supera los límites, HubSpot es AppFabric posible que los registros de auditoría que aparezcan se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu HubSpot cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conHubSpot. Para encontrar la información necesaria para realizar HubSpot la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el HubSpot uso de OAuth. Para crear una aplicación OAuth en HubSpot, siga los pasos siguientes:

1. Siga las instrucciones de la sección Crear una aplicación pública de la guía de HubSpot del sitio web de HubSpot.
2. En la pestaña Autorización, agregue los tres ámbitos que aparecen en Ámbitos obligatorios.
3. Utilice una URL de redireccionamiento con el siguiente formato en URL de redireccionamiento.

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

En esta URL, <region>se encuentra el código del paquete de aplicaciones Región de AWS en el que configuraste tu paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

4. Seleccione Crear una aplicación.

Ámbitos obligatorios

Debe añadir los siguientes ámbitos a su aplicación OAuth de HubSpot:

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

Autorizaciones de la aplicación

ID de inquilino

Introduzca un ID que identifique esta organización de HubSpot única. Por ejemplo, introduzca su ID de cuenta de HubSpot.

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de HubSpot. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente en HubSpot:

1. Vaya a la página de inicio de sesión de HubSpot e inicie sesión con las credenciales de su cuenta de desarrollador.

2. En el menú Aplicaciones, seleccione su aplicación.
3. En la pestaña Autorización, busque el valor del ID de cliente.

Secreto del cliente

AppFabric solicitará un secreto de cliente. Siga los pasos siguientes para encontrar su secreto de cliente en HubSpot:

1. Vaya a la página de inicio de sesión de HubSpot e inicie sesión con las credenciales de su cuenta de desarrollador.
2. En el menú Aplicaciones, seleccione su aplicación.
3. En la pestaña Autorización, busque el valor del Secreto de cliente.

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, recibirás una ventana emergente desde la HubSpot que podrás aprobarla. Inicia sesión en tu cuenta con las credenciales de tu cuenta empresarial (no de tu cuenta de desarrollador) para aprobar la AppFabric autorización. Elija Permitir.

IBM Security® Verify

La IBM Security® Verify familia ofrece funciones automatizadas, basadas en la nube y locales para administrar la gobernanza de la identidad, gestionar la identidad y el acceso de los empleados y los consumidores, y controlar las cuentas privilegiadas. Ya sea que necesite implementar una solución en la nube o local, le IBM Security® Verify ayuda a establecer confianza y a protegerse contra las amenazas internas tanto para sus empleados como para los consumidores.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosIBM Security® Verify, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para IBM Security® Verify
- AppFabric Conectarse a tu IBM Security® Verify cuenta

AppFabric soporte para IBM Security® Verify

AppFabric admite la recepción de información de usuario y registros de auditoría desdeIBM Security® Verify.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría IBM Security® Verify a los destinos admitidos, debe cumplir los siguientes requisitos:

- Para acceder a los registros de auditoría, debe tener una cuenta IBM Security® VerifySaaS.
- Para acceder a los registros de auditoría, debe tener un rol de administrador en su cuenta IBM Security® Verify SaaS.

Consideraciones de límites de velocidad

IBM Security® Verify impone límites de velocidad a la API de IBM Security® Verify. Para obtener más información sobre los límites de velocidad de las IBM Security® Verify API, consulte las condiciones de IBM. Si la combinación de las aplicaciones de IBM Security® Verify API existentes AppFabric y las aplicaciones de API existentes supera IBM Security® Verify los límites, es AppFabric posible que los registros de auditoría se retrasen.

Consideraciones sobre el retraso de datos

Es posible que veas un retraso de hasta 30 minutos en un evento de auditoría para que te entreguen a tu destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto se puede personalizar a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu IBM Security® Verify cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conIBM Security® Verify. Para encontrar la información necesaria para realizar IBM Security® Verify la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el IBM Security® Verify uso de OAuth. Para crear una aplicación OAuth enIBM Security® Verify, consulte Crear un cliente de API en el sitio web de documentación de IBM.

1. Para iniciar sesión por primera vez, utilice la URL de inicio de sesión y las credenciales que se enviaron a su dirección de correo electrónico registrada.
2. Acceda a la consola de administración en`https://<hostname>.verify.ibm.com/ui/admin/`. Para obtener más información, consulte Acceso a IBM Security® Verify.
3. En la consola de administración, en Seguridad < Acceso a la API < Cliente de la API, seleccione Agregar.
4. Seleccione las siguientes opciones. Son necesarias para leer el registro de auditoría y los detalles del usuario.
   - Lea los informes
   - Leer usuarios y grupos
5. Mantenga la opción predeterminada en el método de autenticación del cliente.

   No edite el campo Ámbitos personalizados.
6. Elija Siguiente.
7. No edite el campo del filtro IP.
8. Elija Siguiente.
9. No edite el campo Propiedades adicionales.
10. Elija Siguiente.
11. Especifique un nombre y una descripción. La descripción es opcional.
12. Elija Crear cliente de API.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará su ID de inquilino. Puedes encontrar el ID de inquilino en la URL IBM Security® Verify estándar. Por ejemplo, en la `https://hostname.verify.ibm.com/` URL, el ID de inquilino es el *`nombre de host`* que se puede encontrar antes `.verify.ibm.com` (o antes `ice.ibmcloud.com` si está utilizando un nombre de host anterior). Si utilizas una URL personalizada, ponte en contacto con tu equipo de IBM Security® Verify soporte para obtener tu URL estándar.

Nombre de inquilino

Introduzca un nombre que identifique a este IBM Security® Verify arrendatario único. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente en IBM Security® Verify:

1. Para iniciar sesión por primera vez, utilice la URL de inicio de sesión y las credenciales que se enviaron a la dirección de correo electrónico registrada.
2. Acceda a la consola de administración en`https://<hostname>.verify.ibm.com/ui/admin/`. Para obtener más información, consulte Acceso a IBM Security® Verify.
3. En la consola de administración, en Seguridad < Acceso a la API < Cliente de la API, selecciona los puntos suspensivos (⊙) situados junto a la aplicación OAuth específica.
4. Selecciona Detalles de conexión.
5. Busque el ID de cliente en las credenciales de la API.

Secreto del cliente

AppFabric solicitará un secreto de cliente. Siga los pasos siguientes para encontrar su secreto de cliente en IBM Security® Verify:

1. Para iniciar sesión por primera vez, utilice la URL de inicio de sesión y las credenciales que se enviaron a la dirección de correo electrónico registrada.
2. Acceda a la consola de administración en`https://<hostname>.verify.ibm.com/ui/admin/`. Para obtener más información, consulte Acceso a IBM Security® Verify.
3. En la consola de administración, en Seguridad < Acceso a la API < Cliente de la API, selecciona los puntos suspensivos (⊙) situados junto a la aplicación OAuth específica.
4. Selecciona Detalles de conexión.
5. Busque el secreto del cliente en las credenciales de la API.

JumpCloud

JumpCloud Inc. es una empresa estadounidense de software empresarial que ofrece una plataforma de directorios basada en la nube para la gestión de identidades. Centraliza y simplifica la gestión de identidades, lo que permite a los usuarios acceder de forma segura a sus sistemas, aplicaciones, redes y servidores de archivos con un único conjunto de credenciales, independientemente de la plataforma, el protocolo, el proveedor o la ubicación.

Puede usar AWS AppFabric para recibir registros de auditoría y datos de usuarios JumpCloud, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Kinesis Data Firehose.

Temas

- AppFabric soporte para JumpCloud
- AppFabric Conectarse a su JumpCloud cuenta

AppFabric soporte para JumpCloud

AppFabric admite la recepción de información de usuario y registros de auditoría desdeJumpCloud.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría JumpCloud a los destinos admitidos, debe cumplir los siguientes requisitos:

- Debes tener un plan de JumpCloud suscripción de pago activo. Para obtener más información, consulte el Select a package that's right for yousitio JumpCloud web.
- Debe tener el rol de «Administradores con facturación».

Consideraciones de límites de velocidad

JumpCloud no publica los límites de tasa. Debe crear un caso de soporte o ponerse en contacto con su equipo de JumpCloud atención al cliente. Si la combinación de las aplicaciones de JumpCloud API existentes AppFabric y las aplicaciones de API existentes supera los JumpCloud's límites, es AppFabric posible que se retrase la publicación de los registros de auditoría.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe a los retrasos en los eventos de auditoría puestos a disposición por la aplicación y a las precauciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a su JumpCloud cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conJumpCloud. Para encontrar la información necesaria para realizar la autorización JumpCloud AppFabric, sigue los pasos de la siguiente sección.

Crea un token de organización a partir de la JumpCloud cuenta

AppFabric utiliza una clave de API para integrarse con JumpCloud Para crear una clave de API en JumpCloud, sigue estos pasos:.

1. Inicie sesión en su JumpCloud cuenta como administrador.
2. En el Portal de administración, elige las iniciales de tu cuenta, ubicadas en la parte superior derecha, y selecciona Mi clave de API en el menú.
3. Selecciona Generar nueva clave de API o selecciona una clave existente.

> **Note**
>
> JumpCloudsolo permite una clave de API activa. Al generar una nueva clave de API, se revocará el acceso a la clave de API actual. Esto hará que no se pueda acceder a todas las llamadas que utilicen la clave de API anterior. Deberás actualizar cualquier integración existente que utilice la clave de API anterior con el nuevo valor de clave.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará tu ID de inquilino. Aquí, el «ID de la organización» será el ID del inquilino. Para encontrar el «ID de la organización», sigue estos pasos.

1. Inicie sesión en su cuenta de JumpCloud.

2. En el panel de navegación, selecciona Configuración, Perfil de la organización y, por último, General.
3. Selecciona el icono del «ojo» para eliminar la vista oculta.
4. Selecciona el icono de «doble página» para copiar la identificación.

Nombre de inquilino

Introduzca un nombre que identifique a esta JumpCloud organización única. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

Token de cuenta de servicio

AppFabric solicitará el token de tu cuenta de servicio. En AppFabric, este es el token de API de la organización en el que creasteCrea un token de organización a partir de la JumpCloud cuenta, anteriormente en este tema.

Microsoft365

Microsoft 365 es una familia de productos de Microsoft compuesta por software de productividad, colaboración y servicios en la nube.

Puede usarlo como medida de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuarios de Microsoft 365, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para 365 Microsoft
- AppFabric Conectarse a tu cuenta de Microsoft 365

AppFabric soporte para 365 Microsoft

AppFabric admite la recepción de información de usuario y registros de auditoría de Microsoft 365.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría de Microsoft 365 a los destinos compatibles, debes cumplir los siguientes requisitos:

- Debe estar suscrito a un plan de Microsoft 365 Enterprise. Para obtener más información sobre cómo crear o actualizar a un plan de Microsoft 365 Enterprise, consulte Planes de Microsoft 365 Enterprise en el sitio web de Microsoft.
- Su cuenta de Microsoft 365 debe tener un usuario con permisos de Administrador.
- Debe activar el registro de auditoría en su organización. Para obtener más información, consulte Activar o desactivar la auditoría en el sitio web de Microsoft.

Consideraciones de límites de velocidad

Microsoft 365 impone límites de tasa a la API de Microsoft 365. Para obtener más información sobre los límites de tasa de la API de Microsoft 365, consulte Limitación específica de servicio Microsoft Graph en la documentación de Microsoft Graph que encontrará en el sitio web de Microsoft. Si la combinación de las aplicaciones de la API de Microsoft 365 AppFabric y las existentes supera el límite, es AppFabric posible que los registros de auditoría que aparezcan se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu cuenta de Microsoft 365

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric con Microsoft 365. Para encontrar la información necesaria para autorizar Microsoft 365 AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con Microsoft 365 mediante OAuth. Para crear una aplicación OAuth en Microsoft 365, siga los pasos siguientes:

1. Siga las instrucciones de la sección Registrar una aplicación en la Guía del desarrollador de Azure Active Directory que encontrará en el sitio web de Microsoft.

   Seleccione Solo cuentas de este directorio organizativo en la configuración de Tipos de cuentas compatibles.

2. Siga las instrucciones de la sección Agregar una URL de redireccionamiento en la Guía del desarrollador de Azure Active Directory.

   Elija la plataforma web.

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

   En esta URL, *<region>* está el código Región de AWS en el que configuraste tu paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

   Puede omitir el resto de campos de entrada de la plataforma web.

3. Siga las instrucciones de la sección Agregar un secreto de cliente en la Guía para desarrolladores de Azure Active Directory.

Permisos necesarios

Debe añadir los siguientes permisos a su aplicación de OAuth. Para añadir permisos, sigue las instrucciones de la sección Añadir permisos para acceder a su API web de la Guía del desarrollador de Azure Active Directory.

- `Microsoft Graph API` > `User.Read` (se agrega automáticamente)
- `Office 365 Management APIs` > `ActivityFeed.Read` (Seleccione el tipo delegado)
- `Office 365 Management APIs` > `ActivityFeed.ReadDlp` (Seleccione el tipo delegado)
- `Office 365 Management APIs` > `ServiceHealth.Read` (Seleccione el tipo delegado)

Tras haber agregado los permisos, otorgue el consentimiento del administrador para los permisos siguiendo las instrucciones de la sección Botón de consentimiento del administrador en la Guía del desarrollador de Azure Active Directory.

Autorizaciones de la aplicación

AppFabric permite recibir información de usuario y registros de auditoría de tu cuenta de Microsoft 365. Para recibir tanto los registros de auditoría como los datos de usuario de Microsoft 365, debe crear dos autorizaciones de aplicaciones; una, denominada Microsoft 365, en la lista desplegable de autorizaciones de aplicaciones, y otra, denominada Microsoft 365 Audit Log, en la lista desplegable

de autorizaciones de aplicaciones. Puede usar una misma ID de inquilino, ID de cliente y clave secreta de cliente para ambas autorizaciones de aplicaciones. Para recibir los registros de auditoría de Microsoft 365, necesitará las autorizaciones de las aplicaciones Microsoft 365 y Microsoft 365 Audit Log. Si desea usar únicamente la herramienta de acceso de usuario, solo necesitará la autorización de la aplicación Microsoft 365.

ID de inquilino

AppFabric solicitará su identificación de inquilino. El ID de inquilino que AppFabric aparece es su ID de inquilino de Azure Active Directory. Para encontrar su ID de inquilino de Azure Active Directory, consulte Cómo encontrar su ID de inquilino de Azure Active Directory en la Documentación de producto de Azure que encontrará en el sitio web de Microsoft.

Nombre de inquilino

Introduzca un nombre que identifique esta cuenta única de Microsoft 365. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará tu ID de cliente. El ID de cliente que aparece AppFabric es el ID de la aplicación (cliente) de Microsoft 365. Para encontrar su ID de aplicación (cliente) de Microsoft 365, siga los pasos siguientes:

1. Abre la página de información general de la aplicación OAuth con la que utilices. AppFabric
2. Podrá ver el ID de aplicación (cliente) en el apartado Aspectos básicos.
3. Introduce el ID de la aplicación (cliente) de tu cliente OAuth en el campo ID de cliente de. AppFabric

Secreto del cliente

AppFabric solicitará el secreto de tu cliente. Microsoft365 proporciona este valor solo cuando creas inicialmente el secreto de cliente para tu aplicación OAuth. Si no tiene la clave secreta de cliente, siga los pasos siguientes para generarla:

1. Para crear una clave secreta de cliente, siga las instrucciones de la sección Agregar un secreto de cliente en la Guía para desarrolladores de Azure Active Directory.
2. Introduce el contenido del campo Valor en el campo Secreto del cliente de. AppFabric

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, Microsoft 365 abrirá una ventana emergente para aprobarla. Para aprobar la AppFabric autorización, selecciona permitir.

Miro

Miro es un espacio de trabajo en línea para la innovación que permite a los equipos distribuidos de cualquier tamaño crear la próxima gran innovación. El lienzo infinito de la plataforma permite a los equipos organizar talleres y reuniones interesantes, diseñar productos, intercambiar ideas y mucho más. Miro, con sede conjunta en San Francisco y Ámsterdam, atiende a más de 50 millones de usuarios en todo el mundo, incluido el 99 % de las empresas de la lista Fortune 100. Miro se fundó en 2011 y actualmente cuenta con más de 1500 empleados en 12 centros de todo el mundo. Para obtener más información, consulte Miro.

Miro incluye un conjunto completo de capacidades de colaboración diseñadas para la innovación, como la creación de diagramas, la creación de esquemas, la visualización de datos en tiempo real, la facilitación de talleres y el soporte integrado para prácticas ágiles, talleres y presentaciones interactivas. Miro anunció recientemente la IA de Miro, que amplía las capacidades de Miro, con la creación de mapas y diagramas basados en la IA, la agrupación y el resumen y la generación de contenido. Miro permite a las organizaciones reducir la cantidad de herramientas independientes, lo que reduce la fragmentación y el costo de la información.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosMiro, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Miro
- AppFabric Conectarse a tu Miro cuenta

AppFabric soporte para Miro

AppFabric admite la recepción de información de usuario y registros de auditoría desdeMiro.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Miro a los destinos admitidos, debe cumplir los siguientes requisitos:

- Debe tener un plan Enterprise de Miro. Para obtener más información sobre los tipos de planes de Miro, consulte la página de precios de Miro en el sitio web de Miro.
- Debe tener un usuario con el rol de administrador de la empresa en su cuenta de Miro. Para obtener más información sobre los roles, consulte la sección Roles de Miro a nivel empresarial en el sitio web del centro de ayuda de Miro.
- Debe tener un equipo de desarrolladores empresariales en su cuenta de Miro. Para obtener información sobre la creación de equipos de desarrolladores, consulte los equipos de desarrolladores empresariales en el sitio web del centro de ayuda de Miro.

Consideraciones de límites de velocidad

Miro impone límites de velocidad a la API de Miro. Para obtener más información sobre los límites de tasa de la API de Miro, consulte la sección sobre los límites de tasa en la Guía para desarrolladores de Miro en el sitio web de Miro. Si la combinación de las aplicaciones de Miro API existentes AppFabric y las aplicaciones de API existentes supera el límite, es AppFabric posible que los registros de auditoría se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Miro cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conMiro. Para encontrar la información necesaria para realizar Miro la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Miro uso de OAuth. Para crear una aplicación OAuth en Miro, siga los pasos siguientes:

1. Para crear una aplicación OAuth, siga las instrucciones de la sección Creación e instalación de aplicaciones del artículo sobre los equipos de desarrolladores empresariales del sitio web del centro de ayuda de Miro.

2. En el cuadro de diálogo de creación de la aplicación, seleccione la casilla Vencimiento del token de autorización de usuario después de seleccionar un equipo de desarrolladores de la organización empresarial.

   > **Note**
   >
   > Debe hacerlo antes de crear la aplicación, ya que no puede cambiar esta opción después de crearla.

3. En la página de la aplicación, introduzca una URL con el siguiente formato en la sección URI de redireccionamiento para OAuth 2.0.

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

   En esta URL, <region>se encuentra el código del paquete de aplicaciones Región de AWS en el que configuraste tu paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

4. Copia y guarda tu ID de cliente y tu secreto de cliente para usarlos en la autorización de la AppFabric aplicación.

Ámbitos obligatorios

Debe añadir los siguientes ámbitos en la sección de `Permissions` de la página de su aplicación OAuth de Miro:

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

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará su identificación de inquilino. El ID de inquilino AppFabric que aparece es tu ID de Miro equipo. Para obtener información sobre cómo encontrar su ID de equipo de Miro, consulte la sección de Preguntas frecuentes de Soy un nuevo administrador de Miro. ¿Por dónde empezar? en el sitio web del centro de ayuda de Miro.

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de Miro. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará tu ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente de :

1. Vaya a la configuración de su perfil de Miro.
2. Seleccione la pestaña Sus aplicaciones.
3. Selecciona la aplicación con la que te conectas AppFabric.
4. Introduzca el ID de cliente de la sección Credenciales de la aplicación en el campo ID de cliente de AppFabric.

Secreto del cliente

AppFabric solicitará el secreto de su cliente. Siga los pasos siguientes para encontrar su secreto de cliente:

1. Vaya a la configuración de su perfil de Miro.
2. Seleccione la pestaña Sus aplicaciones.
3. Selecciona la aplicación con la que te conectas AppFabric.
4. Introduzca el secreto del cliente de la sección Credenciales de la aplicación en el campo Secreto del cliente de AppFabric.

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, aparecerá una ventana emergente en la que podrás Miro aprobar la autorización. Para aprobar la AppFabric autorización, selecciona Permitir.

Okta

Okta es la mejor empresa de administración de identidad del mundo. Como principal socio independiente de Identity, Okta permite a todo el mundo utilizar de forma segura cualquier tecnología, en cualquier lugar, en cualquier dispositivo o aplicación. Las marcas más confiables

confían en Okta para permitir el acceso seguro, la autenticación y la automatización. Con la flexibilidad y neutralidad en el núcleo de las nubes de identidad de la fuerza de trabajo y la identidad del cliente de Okta, los líderes empresariales y los desarrolladores pueden centrarse en la innovación y acelerar la transformación digital, gracias a soluciones personalizables y más de 7000 integraciones prediseñadas. Okta está construyendo un mundo en el que la identidad le pertenece a usted. Puede obtener más información en okta.com.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosOkta, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Okta
- AppFabric Conectarse a tu Okta cuenta

AppFabric soporte para Okta

AppFabric admite la recepción de información de usuario y registros de auditoría desdeOkta.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Okta a los destinos admitidos, debe cumplir los siguientes requisitos:

- Se puede usar AppFabric con cualquier tipo de Okta plan.
- Debe tener un usuario con el rol de Superadministrador en su cuenta de Okta.
- El usuario que aprueba la autorización de la aplicación también AppFabric debe tener el rol de superadministrador en tu Okta cuenta.

Consideraciones de límites de velocidad

Okta impone límites de velocidad a la API de Okta. Para obtener más información sobre los límites de tasa de la API de Okta, consulte los límites de tasa en la Guía para desarrolladores de Okta del sitio web de Okta. Si la combinación de las aplicaciones de Okta API existentes AppFabric y las aplicaciones existentes supera los límites, Okta es AppFabric posible que los registros de auditoría se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Okta cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conOkta. Para encontrar la información necesaria para realizar Okta la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Okta uso de OAuth. Para crear una aplicación de OAuth con la que conectarse AppFabric, siga las instrucciones de la sección Crear integraciones de aplicaciones OIDC en el sitio web del Centro de ayuda. Okta A continuación se indican las consideraciones de configuración para: AppFabric

1. Para Tipo de aplicación, elija Aplicación web.
2. Para el tipo de concesión, seleccione Código de autorización y Actualizar token.
3. Use una URL de redireccionamiento con el siguiente formato como URI de redireccionamiento de inicio de sesión y URI de redireccionamiento de cierre de sesión.

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

   En esta URL, <region>se encuentra el código del paquete de aplicaciones Región de AWS en el que configuró su paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
4. Puede omitir la configuración de Trusted Origins.
5. Conceda acceso a todos los miembros de su organización Okta en la configuración de acceso controlado.

> **Note**
>
> Si omite este paso durante la creación inicial de la aplicación OAuth, puede asignar a todos los miembros de su organización como un grupo mediante la pestaña Asignaciones de la página de configuración de la aplicación.

6. Puede dejar todas las demás opciones con sus valores predeterminados.

Ámbitos obligatorios

Debe añadir los siguientes ámbitos a su aplicación OAuth de Okta:

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

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará un ID de inquilino. El ID de inquilino AppFabric es tu Okta dominio. Para obtener más información sobre cómo encontrar su dominio de Okta, consulte Buscar su dominio de Okta en la Guía para desarrolladores de Okta del sitio web de Okta.

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de Okta. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente en Okta:

1. Desplácese hasta la consola de desarrollador de Okta.
2. Elija la pestaña Aplicaciones.
3. Elija su aplicación y, a continuación, seleccione la pestaña General.

4. Desplácese hasta la sección Credenciales de cliente.
5. Introduce el ID de cliente de tu cliente de OAuth en el campo ID de cliente de. AppFabric

Secreto del cliente

AppFabric solicitará un secreto de cliente. Siga los pasos siguientes para encontrar su secreto de cliente en Okta:

1. Desplácese hasta la consola de desarrollador de Okta.
2. Elija la pestaña Aplicaciones.
3. Elija su aplicación y, a continuación, seleccione la pestaña General.
4. Desplácese hasta la sección Credenciales de cliente.
5. Introduce el secreto de cliente de tu aplicación OAuth en el campo Secreto de cliente de. AppFabric

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, recibirás una ventana emergente en la que podrás Okta aprobar la autorización. Para aprobar la AppFabric autorización, selecciona permitir. El usuario que aprueba la autorización de Okta debe tener permiso de superadministrador en Okta.

OneLogin by One Identity

OneLogin by One Identity es una solución moderna de gestión de acceso basada en la nube que administra de forma sencilla todas las identidades digitales para su personal, clientes y socios. OneLogin ofrece inicio de sesión único (SSO) seguro, autenticación multifactor (MFA), autenticación adaptativa, MFA a nivel de escritorio, integración de directorios con AD, LDAP, G Suite y otros directorios externos, gestión del ciclo de vida de la identidad y mucho más. Con élOneLogin, puede proteger a su organización de los ataques más comunes, lo que se traduce en una mayor seguridad, experiencias de usuario sencillas y el cumplimiento de los requisitos reglamentarios. Puede utilizar como medida de seguridad AWS AppFabric para recibir registros de auditoría y datos de los usuariosOneLogin, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un depósito de Amazon Simple Storage Service (Amazon S3) (Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric Soporte para OneLogin by One Identity
- AppFabric Conectarse a tu OneLogin by One Identity cuenta

AppFabric Soporte para OneLogin by One Identity

AppFabric admite la recepción de información de usuario y registros de auditoría desdeOneLogin by One Identity.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría OneLogin by One Identity a destinos compatibles, debe cumplir los siguientes requisitos:

- Debe tener una cuenta de OneLogin nivel Advanced o Professional.
- Debe tener un usuario con los privilegios de administrador o administrador delegado.

Consideraciones de límites de velocidad

OneLogin by One Identity impone límites de velocidad a la API de OneLogin. Para obtener más información sobre los límites de tasa de la API de OneLogin, consulte la sección Obtener límites de tasa en la Referencia de la API de OneLogin. Si la combinación de las aplicaciones de OneLogin API existentes AppFabric y las aplicaciones existentes supera los límites, OneLogin es AppFabric posible que los registros de auditoría que aparezcan se retrasen. Sin embargo, el límite de tasa de OneLogin puede aumentar. Para obtener ayuda, póngase en contacto con su OneLogin by One Identity o contacte con One Identity.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu OneLogin by One Identity cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conOneLogin by One Identity. Para encontrar la información necesaria para realizar OneLogin la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el OneLogin by One Identity uso de OAuth. Para crear una aplicación OAuth en OneLogin, siga los pasos siguientes:

1. Acceda a la pagina de registro de OneLogin e inicie sesión.
2. En el menú Desarrolladores, seleccione Credenciales de API.
3. Elija Credenciales nuevas, introduzca un nombre para la nueva credencial y, a continuación, elija Leer todo.
4. Seleccione Guardar. OneLogin crea un ID de cliente y un secreto de cliente.

Ámbitos obligatorios

Debe añadir los siguientes ámbitos a su aplicación OAuth de OneLogin by One Identity:

- Lea todo. Para obtener más información sobre los ámbitos y las credenciales de los clientes, consulte Trabajar con credenciales de API en la Referencia de la API de OneLogin.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará una identificación de inquilino. El ID de inquilino AppFabric es el subdominio de tu instancia. Puede encontrar su ID de inquilino en la barra de dirección del navegador. Por ejemplo, `subdomain` es el ID de inquilino en la siguiente URL `https://subdomain.onelogin.com`.

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de OneLogin by One Identity. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente en OneLogin by One Identity:

1. Acceda a la pagina de registro de OneLogin e inicie sesión.
2. En el menú Desarrolladores, seleccione Credenciales de API.

3. Elija la credencial de la API para obtener el ID de cliente.

Secreto del cliente

AppFabric solicitará un secreto de cliente. Siga los pasos siguientes para encontrar su secreto de cliente en OneLogin by One Identity:

1. Acceda a la pagina de registro de OneLogin e inicie sesión.
2. En el menú Desarrolladores, seleccione Credenciales de API.
3. Elija la credencial de la API para obtener el secreto del cliente.

Autorización de la aplicación del cliente

En AppFabric, cree una autorización de aplicación con su ID y nombre de inquilino y su ID y nombre de cliente. Elija conectar para activar la autorización.

PagerDuty

PagerDuty es una plataforma de gestión de operaciones digitales que ayuda a los equipos a mitigar los problemas que afectan a los clientes al convertir cualquier señal en acción para que puedan resolver los problemas más rápido y operar de manera más eficiente. Se integra con CloudWatch, GuardDuty, CloudTrail y Personal Health Dashboard. Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosPagerDuty, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para PagerDuty
- AppFabric Conectarse a tu PagerDuty cuenta

AppFabric soporte para PagerDuty

AppFabric admite la recepción de información de usuario y registros de auditoría desdePagerDuty.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría PagerDuty a los destinos admitidos, debe cumplir los siguientes requisitos:

- Para acceder a los registros de auditoría, debe tener un plan de PagerDuty empresarial o digital.
- Debe ser el administrador global o el propietario de la cuenta de PagerDuty.

Consideraciones de límites de velocidad

PagerDuty impone límites de velocidad a la API de PagerDuty. Para obtener más información sobre los límites de tasa de la API de PagerDuty, consulte Límites de tasa de la API de REST en la Plataforma para desarrolladores de PagerDuty. Si la combinación de las aplicaciones de PagerDuty API existentes AppFabric y las aplicaciones existentes supera los límites, PagerDuty es AppFabric posible que los registros de auditoría que aparezcan se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu PagerDuty cuenta

La plataforma de PagerDuty admite claves de acceso a la API. Para generar una clave de acceso a la API, siga los siguientes pasos.

Crear una clave de acceso a la API

AppFabric se integra con PagerDuty el uso de una clave de acceso API para clientes públicos. Para crear una clave de acceso a la API en PagerDuty, siga estos pasos:

1. Acceda a la pagina de registro de PagerDuty e inicie sesión.
2. Elija Integraciones, Claves de acceso a la API.
3. Elija Crear nueva clave de la API.
4. Introduzca una descripción y, a continuación, seleccione Clave de la API de solo lectura.
5. Elija Create Key (Crear clave).
6. Copie y guarde la clave de la API. Lo necesitarás más adelante AppFabric. Si cierra la página antes de guardar la clave de la API, debe generar una nueva clave y guardarla. Esta clave debe estar dedicada AppFabric a evitar compartir el límite de velocidad de la PagerDuty API con tus otras integraciones.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará tu ID de inquilino. El ID de inquilino de su cuenta de PagerDuty es la URL base de su cuenta. Para localizar esto, inicie sesión en PagerDuty y copie la información desde la barra de direcciones de su navegador web. El ID del inquilino debe seguir uno de los siguientes formatos:

- Para las cuentas de EE. UU., *subdomain*`.pagerduty.com`
- Para las cuentas de la UE, *subdomain*`.eu.pagerduty.com`

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de PagerDuty. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

Token de cuenta de servicio

AppFabric solicitará el token de tu cuenta de servicio. El token de la cuenta de servicio AppFabric es la clave de acceso a la API en la que creasteCrear una clave de acceso a la API.

Ping Identity

En Ping Identity, creemos en hacer que las experiencias digitales sean seguras y sencillas para todos los usuarios, sin concesiones. Por eso, más de la mitad de las empresas de la lista Fortune 100 optan por Ping Identity para proteger las interacciones digitales de sus usuarios y, al mismo tiempo, crear experiencias sin interrupciones. El 23 de agosto de 2023, Ping Identity y ForgeRock se unieron para ofrecer más opciones, una experiencia más profunda y una solución de identidad más completa para clientes y socios. Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosPing Identity, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Ping Identity
- AppFabric Conectarse a tu Ping Identity cuenta

AppFabric soporte para Ping Identity

AppFabric admite la recepción de información de usuario y registros de auditoría desdePing Identity.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Ping Identity a destinos compatibles, debe cumplir los siguientes requisitos:

- Debe tener una cuenta de Ping Identity Essential, Plus o Premium. Para obtener más información sobre cómo crear o actualizar al tipo de plan de Ping Identity correspondiente, consulte los precios de todas las funciones de Ping Identity en el sitio web de Ping Identity.
- Debe tener el rol de solo lectura de datos de identidad en su cuenta de Ping Identity. Puede agregar roles a su cuenta al asignar roles a su aplicación. Para obtener más información sobre los roles, consulte Roles en el sitio web de soporte de Ping Identity.

Consideraciones de límites de velocidad

Ping Identity no publica los límites de tasa. Debe crear un caso de soporte o ponerse en contacto con su equipo de Éxito del cliente de Ping Identity. Si la combinación de las aplicaciones de Ping Identity API existentes AppFabric y las aplicaciones existentes supera los límites, Ping Identity es AppFabric posible que los registros de auditoría que aparezcan se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Ping Identity cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conPing Identity. Para encontrar la información necesaria para realizar Ping Identity la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Ping Identity uso de OAuth. Para crear una aplicación OAuth en Ping Identity, siga los pasos siguientes:

1. Siga las instrucciones de la sección Crear una conexión a una aplicación de la guía para desarrolladores de PingOne en el sitio web de Ping Identity.
2. Tras crear la aplicación, personalice los tipos de concesiones.
   a. Cuando haya iniciado sesión en la aplicación, seleccione la pestaña Configuración y haga clic en el icono del lápiz para realizar cambios en la configuración existente.
   b. En Tipo de concesión, seleccione Código de autorización. Mantenga la aplicación de la PKCE como OPCIONAL.
   c. Seleccione Actualizar token y elija las duraciones de actualización.
3. Use una URL de redireccionamiento con el siguiente formato en Redireccionar URL/Devolución de URL.

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

   En esta URL, <region>se encuentra el código del paquete de aplicaciones Región de AWS en el que configuraste tu paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará tu ID de inquilino. El ID de inquilino AppFabric es el nombre de su Ping Identity instancia. Puede encontrar su ID de inquilino en la barra de dirección del navegador. Por ejemplo, *API_PATH*`/v1/environments/`*environmentID*. Donde *API_PATH* representa el dominio regional del servidor PingOne, así como `api.pingone.com`, y *environmentID* representa su ID de entorno indicado en las propiedades del entorno de la aplicación. Para obtener más información sobre las propiedades del entorno, consulte Propiedades del entorno en el sitio web de Ping Identity.

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de Ping Identity. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente en Ping Identity:

1. Inicie sesión en la consola de administración de PingOne y seleccione Aplicaciones.
2. Elija su aplicación en la lista.
3. Seleccione la pestaña Descripción general y, a continuación, busque el valor del ID de cliente.

Secreto del cliente

AppFabric solicitará un secreto de cliente. Siga los pasos siguientes para encontrar su secreto de cliente en Ping Identity:

1. Inicie sesión en la consola de administración de PingOne y seleccione Aplicaciones.
2. Elija su aplicación en la lista.
3. Seleccione la pestaña Descripción general y, a continuación, busque el valor de secreto de cliente.

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, recibirás una ventana emergente Ping Identity para aprobarla. Para aprobar la AppFabric autorización, selecciona permitir.

Salesforce

Salesforcefabrica software basado en la nube diseñado para ayudar a las empresas a encontrar más clientes potenciales, cerrar más negocios y sorprender a los clientes con un servicio increíble. Salesforce’s Customer 360 ofrece un conjunto completo de productos, une a los equipos de ventas, servicio, marketing, comercio y TI con una visión única y compartida de la información del cliente, lo que ayuda a las organizaciones a desarrollar relaciones tanto con los clientes como con los empleados. Puede utilizarlos AWS AppFabric para recibir registros de auditoría y datos de usuariosSalesforce, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Salesforce
- AppFabric Conectarse a tu Salesforce cuenta

AppFabric soporte para Salesforce

AppFabric admite la recepción de información de usuario y registros de auditoría desdeSalesforce.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Salesforce a los destinos admitidos, debe cumplir los siguientes requisitos:

- Debe tener una edición Performance, Enterprise o Unlimited deSalesforce. Póngase en contacto con nosotros Salesforce para actualizar a una de estas ediciones.
- Si desea AppFabric transferir archivos de registro de eventos por hora con un conjunto completo de eventos de registro deSalesforce, debe suscribirse a Event Monitoring como parte de las funciones de Shield deSalesforce. De lo contrario, AppFabric transferirá los eventos limitados (es decir, los eventos de inicio de sesión InsecureExternalAssets, cierre de sesión, uso total de la API, infracción de CORS y eventos de HostnameRedirects ELF) del archivo de registro diario Salesforce's estándar. Para comprobar si tu Salesforce cuenta ya está suscrita a Shield Features, ve a Configuración > Gestor de eventos. Si ves 19 o más eventos en la lista, tu cuenta está suscrita al Event Monitoring. Si no tienes Event Monitoring, puedes comprar una suscripción a este complemento contactando con Salesforce nosotros.
- Debes habilitar la generación del archivo de registro de eventos en la Salesforce configuración.
- Deberías usar el perfil de administrador del sistema para crear una aplicación OAuth e iniciar sesión con las mismas credenciales para. AppFabric

> **Note**
>
> El uso total de la API, el registro de infracciones del CORS, los redireccionamientos de nombres de host, los activos externos inseguros y los eventos de inicio y cierre de sesión están disponibles sin coste adicional en las ediciones compatibles de. Salesforce Póngase en contacto con nosotros Salesforce para adquirir los tipos de eventos restantes. Para obtener más información sobre los tipos de Salesforce eventos, consulta los tipos de eventos EventLogFile compatibles en el Salesforce sitio web.
>
> AppFabric puede admitir hasta 100 000 eventos por tipo de evento y por instancia de archivo de registro (por día u hora, según la suscripción al complemento Event Monitoring). Si un

archivo de registro supera el umbral, es posible que se excluya todo el archivo de registro de la ingesta.

Consideraciones de límites de velocidad

Salesforce impone límites de velocidad a la API de Salesforce. Para obtener más información sobre los límites de velocidad de la Salesforce API, consulta los límites y las asignaciones de las solicitudes de API en el Salesforce sitio web. Si la combinación de las aplicaciones de Salesforce API existentes AppFabric y las aplicaciones de API existentes supera los Salesforce's límites, es AppFabric posible que los registros de auditoría se retrasen.

Consideraciones sobre el retraso de datos

Es posible que veas un retraso de hasta 6 horas en el archivo de registro diario o de hasta 29 horas en el archivo de registro por hora para que un evento de auditoría se entregue a tu destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Salesforce cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conSalesforce. Para encontrar la información necesaria para realizar Salesforce la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Salesforce uso de OAuth. Para crear una aplicación OAuth en Salesforce, siga los pasos siguientes:

1. Inicie sesión en su Salesforce cuenta.
2. Vaya a la página de configuración tal y como se describe en la Salesforcedocumentación.
3. Busque App Manager en la búsqueda rápida.
4. Elige Nueva aplicación conectada.
5. Introduzca la información requerida en los campos del formulario.
6. Selecciona Activar la configuración de OAuth.
7. Asegúrate de desactivar las siguientes opciones:

- Solicite la extensión Proof Key for Code Exchange (PKCE) para los flujos de autorización compatibles
- Se requiere un secreto para el flujo del servidor web
- Se requiere un secreto para actualizar el flujo del token

8. Introduzca una URL con el siguiente formato en el cuadro de texto URL de devolución de llamada y seleccione Guardar cambios.

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

En esta URL, <region>se encuentra el código Región de AWS en el que configuraste el paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

9. Rellene los ámbitos según sea necesario (se describe en la siguiente Ámbitos obligatorios sección). Todos los demás campos se pueden dejar con sus valores predeterminados.
10. Seleccione Guardar.
11. Complete los siguientes pasos para verificar la política de token de actualización de la nueva aplicación OAuth:

    a. En la página de configuración, introduce Aplicaciones conectadas en el cuadro de texto Búsqueda rápida y, a continuación, selecciona Administrar aplicaciones conectadas.

    b. Selecciona Editar junto a la aplicación recién creada.

    c. Asegúrese de que el token de actualización sea válido hasta que se seleccione la opción de revocación.

    d. Guarde los cambios.

12. Complete los siguientes pasos para comprobar que se están generando los registros de auditoría:

    a. En la página de configuración, introduzca el archivo de registro de eventos en el cuadro de texto Búsqueda rápida y, a continuación, seleccione el explorador de archivos de registro de eventos.

    b. Confirme que los registros de eventos estén listados en el explorador de archivos de registro de eventos.

13. Navega hasta la aplicación creada y selecciona Ver en el menú desplegable.

14. Elija Manage Consumer Details.

    Se te redirigirá a una nueva pestaña en la que tendrás que verificar tu identidad. En esa pestaña, anota los valores Consumer Key y Consumer Secret. Los necesitarás más adelante para iniciar sesión.

Ámbitos obligatorios

Debe añadir los siguientes ámbitos a su aplicación OAuth de Salesforce:

- Administre los datos de los usuarios a través de las API (`API`).
- Realice la solicitud en cualquier momento (`refresh_tokenyoffline_access`).

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará su identificación de inquilino. El ID de inquilino AppFabric es el subdominio de Salesforce Mi dominio. Puedes encontrar tu subdominio de Mi dominio en la barra de direcciones de tu navegador entre y`https://`. `.my.salesforce.com`

Para encontrar tu Salesforce dominio, sigue las siguientes instrucciones de la pantalla de Salesforce inicio.

1. Ve a la página de configuración tal y como se describe en la Salesforcedocumentación.
2. Busque la configuración de la empresa en la búsqueda rápida y elija Mi dominio en los resultados.

Nombre de inquilino

Introduzca un nombre que identifique a esta Salesforce organización única. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente en Salesforce:

1. Navegue a la página de configuración.
2. Selecciona Configuración y, a continuación, selecciona Administrador de aplicaciones.
3. Elige la aplicación creada y selecciona Ver en el menú desplegable.
4. Elija Manage Consumer Details. Se te redirigirá a una nueva pestaña.
5. Verifica tu identidad y, a continuación, busca el valor de la clave de consumidor.
6. Introduzca la clave de consumidor en el campo de ID de cliente de AppFabric.

Secreto del cliente

AppFabric solicitará su secreto de cliente. El secreto del cliente AppFabric es el secreto del consumidor enSalesforce. Para encontrar tu secretoSalesforce, sigue los siguientes pasos:

1. Ve a la página de configuración.
2. Selecciona Configuración y, a continuación, selecciona Administrador de aplicaciones.
3. Elige la aplicación creada y selecciona Ver en el menú desplegable.
4. Elija Manage Consumer Details. Se te redirigirá a una nueva pestaña.
5. Verifica tu identidad y, a continuación, busca el valor de secreto del consumidor.
6. Introduzca el secreto del consumidor en el campo secreto del cliente de AppFabric.

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, aparecerá una ventana emergente en la que podrás Salesforce aprobar la autorización. En la página de aprobación, asegúrese de utilizar el rol de administrador del Salesforce sistema o un Salesforce usuario que tenga permisos de usuario para ver los archivos de registro de eventos y habilitados para la API durante la autorización. Seleccione Permitir para aprobar la AppFabric autorización.

ServiceNow

ServiceNowes un proveedor líder de servicios basados en la nube que automatizan las operaciones de TI empresariales. ServiceNowde ITOM ofrece a las empresas una visibilidad y un control totales de todo su entorno de TI, incluida la infraestructura virtualizada y en la nube. Simplifica el mapeo, la prestación y la garantía de los servicios porque consolida los datos de infraestructura y servicios de TI en un único sistema de registro. También automatiza y agiliza los procesos clave, incluida la gestión de eventos, incidentes, problemas, configuraciones y cambios. Puede utilizarlos por motivos

de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosServiceNow, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para ServiceNow
- Consideraciones sobre el retraso de datos
- AppFabric Conectarse a su ServiceNow cuenta

AppFabric soporte para ServiceNow

AppFabric admite la recepción de información de usuario y registros de auditoría desdeServiceNow.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría ServiceNow a los destinos admitidos, debe cumplir los siguientes requisitos:

- Se puede usar AppFabric con cualquier tipo de ServiceNow plan.
- Debe tener un usuario con el rol de administrador en su cuenta de ServiceNow.
- Debe tener una instancia de ServiceNow.

Consideraciones de límites de velocidad

ServiceNow impone límites de velocidad a la API de ServiceNow. Para obtener más información sobre los límites de velocidad para la API de ServiceNow, consulte Límites de velocidad de API de REST de entrada en el sitio web de ServiceNow. Si la combinación de las aplicaciones de ServiceNow API existentes AppFabric y las aplicaciones de API existentes supera los límites, es AppFabric posible que se retrase la publicación de los registros de auditoría.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a su ServiceNow cuenta

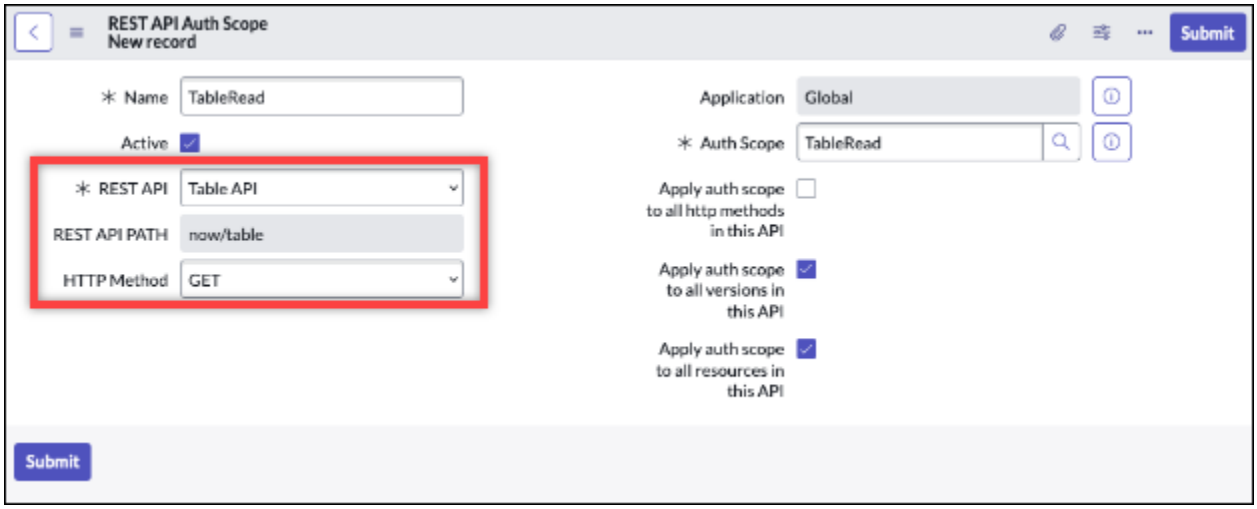
Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conServiceNow. Sigue los siguientes pasos para encontrar la información necesaria para realizar la autorización ServiceNow AppFabric.

Cómo crear una aplicación OAuth

Now Platform es compatible con OAuth 2.0, un tipo de concesión de autorización para que los clientes públicos generen un token de acceso.

1. Registre su aplicación OAuth. Esto requiere que dé los tres pasos siguientes. Para obtener más información sobre cómo completar estos pasos, consulte la sección Registre su solicitud con ServiceNow en el sitio web de ServiceNow.

   a. Registre la aplicación y asegúrese de que Ámbito de aut. tenga acceso a la Tabla API, con un RUTA de API de REST de now/table y un método HTTP de GET, como se muestra en el siguiente ejemplo.



   b. Genere un código de autorización.

   c. Genere un token al portador utilizando el código de autorización.

2. Utilice una URL de redireccionamiento con el siguiente formato.

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

   En esta URL, <region>se encuentra el código Región de AWS en el que configuraste el paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de

Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará un ID de inquilino. El ID de inquilino AppFabric es el nombre de su instancia. Puede encontrar su ID de inquilino en la barra de dirección del navegador. Por ejemplo, *example* es el ID de inquilino en la siguiente URL `https://example.service-now.com`.

Nombre de inquilino

Introduce un nombre que identifique a esta ServiceNow organización única. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente en ServiceNow.

1. Vaya a la consola de ServiceNow.
2. Seleccione OAuth de sistema y, a continuación, seleccione la pestaña Registro de aplicaciones.
3. Elija su aplicación.
4. Introduce el ID de cliente de tu cliente de OAuth en el campo ID de cliente de. AppFabric

Secreto del cliente

AppFabric solicitará un secreto de cliente. Siga los pasos siguientes para encontrar su secreto de cliente en ServiceNow.

1. Vaya a la consola de ServiceNow.
2. Seleccione OAuth de sistema y, a continuación, seleccione la pestaña Registro de aplicaciones.
3. Elija su aplicación.
4. Introduce el secreto de cliente de tu aplicación OAuth en el campo Secreto de cliente de. AppFabric

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, recibirás una ventana emergente en la que podrás ServiceNow aprobar la autorización. Selecciona Permitir para aprobar la AppFabric autorización.

Singularity Cloud

La Singularity Cloud plataforma protege a su empresa de las amenazas de todas las categorías y en todas las etapas. Su inteligencia artificial patentada amplía la seguridad desde las firmas y patrones conocidos hasta los ataques más sofisticados, como los ataques de día cero y el ransomware.

Puede utilizarlos AWS AppFabric para recibir registros de auditoría y datos de usuariosSingularity Cloud, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

> **Note**
>
> Singularity CloudSolo podrá acceder a la documentación después de iniciar sesión en su Singularity Cloud cuenta. Por lo tanto, no podemos vincular directamente a la Singularity Cloud documentación de este documento.

Temas

- AppFabric soporte para Singularity Cloud
- AppFabric Conectarse a tu Singularity Cloud cuenta

AppFabric soporte para Singularity Cloud

AppFabric admite la recepción de información de usuario y registros de auditoría desdeSingularity Cloud.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Singularity Cloud a destinos compatibles, debe tener un rol de administrador en su Singularity Cloud cuenta. Para obtener más información sobre los límites de velocidad de la Singularity Cloud API, inicie sesión en su cuenta de Singularity Cloud, consulte la sección de documentación y busque los roles.

Consideraciones de límites de velocidad

Singularity Cloud impone límites de velocidad a la API de Singularity Cloud. Para obtener más información sobre los límites de velocidad de las Singularity Cloud API, inicie sesión en su cuenta de Singularity Cloud, consulte la sección de documentación y busque los límites de velocidad de las API.

Consideraciones sobre el retraso de datos

Es posible que vea un retraso de hasta 30 minutos en la entrega de un evento de auditoría a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Singularity Cloud cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conSingularity Cloud. Para encontrar la información necesaria para realizar Singularity Cloud la autorización AppFabric, sigue estos pasos.

Cree un token de API para Singularity Cloud

Complete el siguiente procedimiento para crear un token de API asociado a un usuario del servicio. El token de API no se vinculará a un usuario de consola ni a una dirección de correo electrónico específicos.

> **Note**
>
> Cree un nuevo usuario o copie el usuario del servicio para obtener un nuevo token de API antes o después de que caduque el token de API de un usuario de servicio.

1. Inicie sesión en su cuenta de Singularity Cloud.
2. En la barra de herramientas de configuración, selecciona Usuarios y, a continuación, selecciona Usuarios del servicio.
3. Elija Acciones y, a continuación, seleccione Crear nuevo usuario de servicio.
4. En la página Crear un nuevo usuario del servicio, introduzca un nombre, una descripción y una fecha de caducidad para el usuario del servicio.
5. Elija Siguiente.

6. En la sección Seleccione el ámbito de acceso, seleccione el ámbito.
   - Seleccione Cuenta para el nivel de acceso.
   - Seleccione la cuenta para la que desea obtener los registros de auditoría.
7. Elija Crear usuario.

   Se genera el token de la API. Se abre una ventana en la que se muestra la cadena del token con un mensaje que indica que es la última vez que se puede ver el token.
8. (Opcional) Selecciona Copiar el token de API y guárdalo en un lugar seguro.
9. Elija Close.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará su identificación de inquilino. El identificador de inquilino AppFabric será el subdominio de la dirección del Sentinel One sitio web en el que inicie sesión en el servicio. Por ejemplo, si inicias sesión en tu Singularity Cloud cuenta en la `example-company-1.sentinelone.net` dirección, tu ID de inquilino es`example-company-1`.

Nombre de inquilino

Introduce un nombre que identifique a esta Singularity Cloud organización única. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

Token de cuenta de servicio

Usa el token que generaste siguiendo los pasos de la Cree un token de API para Singularity Cloud sección de esta guía. Si pierdes el token o no lo encuentras, puedes generar uno nuevo siguiendo de nuevo los mismos pasos.

> **Note**
>
> Si se genera un nuevo token de API en la consola de Singularity Cloud mientras AppFabric se ingieren los registros de auditoría, las ingestas se detendrán. Si esto ocurre, tendrá que actualizar la autorización de la aplicación con un nuevo token de API para reanudar la ingesta de registros de auditoría.

Slack

Slack tiene la misión de hacer que la vida laboral de las personas sea más sencilla, agradable y productiva. Es la plataforma de productividad para empresas clientes que mejora el rendimiento al capacitar a todos con la automatización sin código, haciendo que la búsqueda y el intercambio de conocimientos sean fluidos manteniendo a los equipos conectados y comprometidos a medida que avanzan juntos en el trabajo. Como parte de Salesforce, Slack está profundamente integrada en Salesforce Customer 360, lo que potencia la productividad de los equipos de ventas, servicio y marketing. Para obtener más información y empezar a usar Slack de forma gratuita, visite slack.com.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosSlack, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Slack
- AppFabric Conectarse a tu Slack cuenta

AppFabric soporte para Slack

AppFabric admite la recepción de información de usuario y registros de auditoría desdeSlack.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Slack a los destinos admitidos, debe cumplir los siguientes requisitos:

- Debe tener un plan Enterprise Grid con Slack. Para obtener más información, consulte la Introducción a Enterprise Grid con Slack en el sitio web de Slack.
- Debe tener un usuario con el rol de propietario de la organización en su cuenta de Slack. Para obtener más información sobre las funciones, consulte Tipos de funciones en Slack en el Centro de ayuda de Slack del sitio web de Slack.

Consideraciones de límites de velocidad

Slack impone límites de velocidad a la API de Slack. Para obtener más información sobre los límites de tasa de la API de Slack, consulte los límites de tasa en la Guía de uso de la API de Slack del

sitio web de Slack. Si la combinación de las aplicaciones de Slack API existentes AppFabric y las aplicaciones de API existentes supera el límite, es AppFabric posible que los registros de auditoría se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Slack cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conSlack. Para encontrar la información necesaria para realizar Slack la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Slack uso de OAuth. Hay dos formas de crear una aplicación OAuth: mediante un manifiesto de aplicación o desde cero. Para crear una aplicación OAuth en Slack, siga los pasos siguientes:

Using an app manifest

1. Navegue hasta la interfaz de usuario de administración de aplicaciones de Slack en su navegador.
2. Elija Crear nueva aplicación.
3. Elija Desde el manifiesto de una aplicación.
4. Elige el espacio de trabajo para el que quieres autorizar. AppFabric
5. En el cuadro Introduzca el manifiesto de la aplicación a continuación, elija JSON y sustituya el JSON existente por el siguiente. <region>Sustitúyalo por el apropiado Región de AWS (por ejemplo, *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. Copie y guarde la ID y el secreto del cliente de la página de información básica.
7. Para conocer el alcance de `auditLogs:read`, debe habilitar la distribución pública de su aplicación. Para obtener más información, consulte Habilitar la distribución pública en el sitio web de Slack.

From scratch

1. Seleccione Desde cero en la pantalla Crear una aplicación.
2. Póngale un nombre a su aplicación y elija un espacio de trabajo.
3. Copie y guarde la ID y el secreto del cliente de la página de información básica.
4. En la página OAuth y permisos, seleccione la opción avanzada de seguridad de los tokens mediante la rotación de los mismos.
5. Añada una URL con el siguiente formato en la sección URL de redireccionamiento de la página OAuth y permisos.

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

   En esta URL, *<region>* se encuentra el código Región de AWS en el que configuraste el paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

6. Para conocer el alcance de `auditLogs:read`, debe habilitar la distribución pública de su aplicación. Para obtener más información, consulte Habilitar la distribución pública en el sitio web de Slack.

Ámbitos obligatorios

> **Note**
>
> Esta sección solo es aplicable si ha decidido crear la app OAuth desde cero. Omita esta sección si elige usar el manifiesto de la aplicación para crear una autorización de aplicación.

Debe añadir los siguientes ámbitos de token de usuario en la página OAuth y permisos de su aplicación OAuth de Slack:

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

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará tu ID de inquilino. El ID de inquilino AppFabric es el ID de tu Slack espacio de trabajo. Para obtener su ID de inquilino, siga las instrucciones de Busque su URL de Slack en el Centro de ayuda de Slack del sitio web de Slack. La URL de su espacio de trabajo de Slack tiene un formato similar a `examplecorp.slack.com` o `examplecorp.enterprise.slack.com`. La ID de inquilino que necesita es `examplecorp` sin `.slack.com` ni `.enterprise.slack.com`.

Nombre de inquilino

Introduce un nombre que identifique el ID de tu Slack espacio de trabajo. AppFabricusa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación

ID de cliente

AppFabric solicitará el ID de cliente desde tu aplicación Slack OAuth. Siga los pasos siguientes para encontrar la ID de cliente:

1. Navegue hasta la interfaz de usuario de administración de aplicaciones de Slack en su navegador.
2. Elige la aplicación de OAuth con la que vas a utilizar. AppFabric
3. Introduce el ID de cliente de la página de información básica en el campo ID de cliente de. AppFabric

Secreto del cliente

AppFabric solicitará el secreto del cliente desde tu aplicación Slack OAuth. Siga los pasos siguientes para encontrar su secreto de cliente:

1. Navegue hasta la interfaz de usuario de administración de aplicaciones de Slack en su navegador.
2. Elige la aplicación de OAuth con la que utilices. AppFabric
3. Introduce el secreto del cliente de la página de información básica en el campo secreto del cliente de. AppFabric

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, aparecerá una ventana emergente en la que podrás Slack aprobar la autorización. Para aprobar la AppFabric autorización, selecciona permitir.

Smartsheet

Smartsheet es una plataforma de gestión del trabajo que le ayuda a alinear el trabajo, las personas y la tecnología en toda su empresa. Smartsheet ofrece un sólido conjunto de capacidades de nivel empresarial que permiten a todos gestionar proyectos, automatizar los flujos de trabajo y diseñar rápidamente soluciones a escala, creando así un entorno propicio para la innovación y, al mismo tiempo, manteniendo la seguridad y la conformidad.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosSmartsheet, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Smartsheet

- AppFabric Conectarse a tu Smartsheet cuenta

AppFabric soporte para Smartsheet

AppFabric admite la recepción de información de usuario y registros de auditoría desdeSmartsheet.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Smartsheet a destinos compatibles, debe cumplir los siguientes requisitos:

- Debe tener una cuenta Smartsheet Business, Enterprise o Advance. Para obtener más información sobre cómo crear o actualizar su cuenta de Smartsheet, consulte Precios de Smartsheet o Smartsheet Advance en el sitio web de Smartsheet.
- Debe completar el proceso de Registro de desarrollador de Smartsheet.

Consideraciones de límites de velocidad

Smartsheet impone límites de velocidad a la API de Smartsheet. Para obtener más información sobre los límites de tasa de la API de Smartsheet, consulte la sección Límites de tasa en la Referencia sobre la API de Smartsheet disponible en el sitio web de Smartsheet.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Smartsheet cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conSmartsheet. Para encontrar la información necesaria para realizar Smartsheet la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Smartsheet uso de OAuth. Para crear una aplicación OAuth en Smartsheet, siga los pasos siguientes:

1. En su cuenta de Smartsheet, acceda a las herramientas para desarrolladores.
2. En la pantalla de herramientas para desarrolladores, seleccione Crear nueva aplicación.
3. Rellene todos los campos de entrada de la pantalla Crear nueva aplicación.
4. Use cualquier valor único en los campos URL de la aplicación y Contacto/soporte de la aplicación.
5. Use una URL de redireccionamiento con el siguiente formato como URL de redireccionamiento de la aplicación.

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

   En esta URL, *<region>* se encuentra el código del paquete de aplicaciones Región de AWS en el que configuraste tu paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
6. Seleccione Guardar.
7. Copie y guarde el ID de cliente de la aplicación y la clave secreta de la aplicación.

Ámbitos obligatorios

Smartsheetno requiere que añadas ámbitos de forma explícita a tu configuración de OAuth. AppFabric solicitará los siguientes ámbitos en la solicitud de autorización a tu cuenta: Smartsheet

- `READ_EVENTS`
- `READ_USERS`

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará su identificación de inquilino. El identificador de inquilino AppFabric es el identificador de su Smartsheet cuenta.

Nombre de inquilino

AppFabric solicitará su identificación de inquilino. Introduzca cualquier valor que identifique su cuenta de Smartsheet de manera única.

ID de cliente

AppFabric solicitará su ID de cliente. El ID de cliente que aparece AppFabric es el ID de cliente de la Smartsheet aplicación. Para encontrar su ID de aplicación (cliente) de Smartsheet, siga los pasos siguientes:

1. En su cuenta de Smartsheet, acceda a las herramientas para desarrolladores.
2. Selecciona la aplicación OAuth con la que te conectas. AppFabric
3. Introduce el ID de cliente de la aplicación desde la pantalla de perfil de la aplicación en el campo ID de cliente de. AppFabric

Secreto del cliente

AppFabric solicitará el secreto de su cliente. El secreto de cliente AppFabric es el secreto de tu Smartsheet aplicación. Para encontrar la clave secreta en Smartsheet, siga los pasos siguientes:

1. En su cuenta de Smartsheet, acceda a las herramientas para desarrolladores.
2. Selecciona la aplicación OAuth con la que te conectas. AppFabric
3. Introduce el secreto de la aplicación desde la pantalla de perfil de la aplicación en el campo Secreto del cliente. AppFabric

Cómo aprobar la autorización

Después de crear la autorización de la aplicación AppFabric, recibirás una ventana emergente en la que podrás Smartsheet aprobar la autorización. Para aprobar la AppFabric autorización, selecciona Permitir.

Terraform Cloud

HashiCorp Terraform Cloudes el producto de aprovisionamiento multinube más utilizado del mundo. El Terraform ecosistema cuenta con más de 3000 proveedores, 14 000 módulos y 250 millones de descargas. Terraform Cloudes la forma más rápida de adoptarloTerraform, ya que proporciona todo lo que los profesionales, los equipos y las empresas globales necesitan para crear infraestructuras y colaborar en el ámbito de la infraestructura y gestionar los riesgos relacionados con la seguridad, el cumplimiento y las limitaciones operativas. Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosTerraform Cloud, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Terraform Cloud
- AppFabric Conectarse a tu Terraform Cloud cuenta

AppFabric soporte para Terraform Cloud

AppFabric admite la recepción de información de usuario y registros de auditoría desdeTerraform Cloud.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Terraform Cloud a destinos compatibles, debe cumplir los siguientes requisitos:

- Para acceder a los registros de auditoría, debe tener un plan Terraform Cloud Plus Edition y ser el propietario de la organización. Para obtener más información sobre Terraform Cloud los planes, consulta Terraformlos precios en el HashiCorp Terraform sitio web.
- Los registros de auditoría por determinar están disponibles para las organizaciones que se pueden crear a partir de la Terraform Cloud cuenta.

Consideraciones de límites de velocidad

Terraform Cloud impone límites de velocidad a la API de Terraform Cloud. Para obtener más información sobre los límites de velocidad de las Terraform Cloud API, consulta la sección sobre la limitación de la velocidad de las API en la configuración general de administración de Terraform Cloud desarrolladores del sitio Terraform Cloud web. Si la combinación de las aplicaciones de Terraform Cloud API existentes AppFabric y las aplicaciones Terraform Cloud de API existentes supera los límites, es AppFabric posible que los registros de auditoría se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Terraform Cloud cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conTerraform Cloud. Para encontrar la información necesaria para realizar Terraform Cloud la autorización AppFabric, sigue estos pasos.

Crea un token de API de la organización

AppFabric se integra con Terraform Cloud el uso de un token de API de la organización. Para obtener más información sobre los tokens de API de la Terraform Cloud organización, consulta los tokens de API de la organización. Para crear una organización, siga las instrucciones de Creating Organizations. Para crear un token de API de una organizaciónTerraform Cloud, sigue estos pasos.

1. Ve a la Terraform Cloud página de inicio de sesión e inicia sesión.
2. Selecciona Organización, Configuración en el panel de la izquierda y, a continuación, elige los tokens de API.
3. En Tokens de organización, selecciona Crear un token de organización y, a continuación, selecciona Generar token.
4. (Opcional) Introduce la fecha u hora de caducidad del token o crea un token que nunca caduque.
5. Copia y guarda el token. Lo necesitarás más adelante AppFabric. Si cierras la página antes de guardar el token, debes revocar el token anterior y crear uno nuevo.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará una identificación de inquilino. El ID de inquilino de tu Terraform Cloud cuenta es la URL de la organización actual de tu cuenta. Para encontrarlo, inicia sesión en tu Terraform Cloud organización y copia la URL de la organización actual. El ID del inquilino debe seguir uno de los siguientes formatos:

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

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de Terraform Cloud. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

Token de cuenta de servicio

AppFabric solicitará el token de tu cuenta de servicio. El token de la cuenta de servicio AppFabric es el token de la API de la organización en el que creasteCrea un token de API de la organización.

Webex by Cisco

Cisco es líder mundial en la tecnología que impulsa Internet. Cisco inspira nuevas posibilidades al reimaginar sus aplicaciones, proteger sus datos, transformar su infraestructura y capacitar a sus equipos para un futuro global e inclusivo.

Sobre Webex by Cisco

Webex es un proveedor líder de soluciones de colaboración basadas en la nube, que incluyen videoconferencias, llamadas, mensajería, eventos, soluciones de experiencia del cliente, como centros de atención al cliente y dispositivos de colaboración diseñados específicamente. El enfoque de Webex en ofrecer experiencias de colaboración inclusivas impulsa la innovación, que aprovecha la IA y el machine learning para eliminar las barreras de la geografía, el idioma, la personalidad y la familiaridad con la tecnología. Sus soluciones se basan en la seguridad y la privacidad desde su diseño. Webex funciona con las aplicaciones empresariales y de productividad líderes del mundo y se entrega a través de una sola aplicación e interfaz. Encontrará más información en webex.com.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosWebex, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Webex
- AppFabric Conectarse a tu Webex cuenta

AppFabric soporte para Webex

AppFabric admite la recepción de información de usuario y registros de auditoría desdeWebex.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Webex a destinos compatibles, debe cumplir los siguientes requisitos:

- Debe tener un plan Collaboration Flex, un plan Meet, un plan de llamadas u otro plan superior. Para obtener más información sobre cómo crear o actualizar al tipo de plan de Webex correspondiente, consulte los precios de todas las funciones de Webex en el sitio web de Webex.
- Su cuenta debe tener la licencia Pro Pack para acceder a los eventos de auditoría de seguridad proporcionados por una de las AuditLog API de Cisco.
- Debe tener un usuario con el rol Administrador de la organización > Administrador total.
- La configuración de Roles de administrador para su Administrador total debe tener habilitada la opción de Responsable de cumplimiento.

Consideraciones de límites de velocidad

Webex impone límites de velocidad a la API de Webex. Para obtener más información sobre los límites de velocidad para la API de Webex, consulte Límites de velocidad en la Guía para desarrolladores de Webex en el sitio web de Webex. Si la combinación de las aplicaciones de Webex API existentes AppFabric y las aplicaciones de API existentes supera el límite, es AppFabric posible que se retrase la publicación de los registros de auditoría.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Webex cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conWebex. Para encontrar la información necesaria para realizar Webex la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Webex uso de OAuth. Para crear una aplicación OAuth en Webex, siga los pasos siguientes:

1. Siga las instrucciones de la sección Cómo registrar su integración en la página Integraciones y autorizaciones de la Guía para desarrolladores de Webex.
2. Utilice una URL de redireccionamiento con el siguiente formato.

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

En esta URL, *<region>* está el código Región de AWS en el que configuraste tu paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Ámbitos obligatorios

Debe añadir los siguientes ámbitos a su aplicación OAuth de Webex:

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

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará tu ID de inquilino. El identificador de inquilino AppFabric es el identificador de su Webex organización. Para obtener información sobre cómo encontrar el ID de su organización en Webex, consulte Buscar el ID de su organización en el centro de control de CiscoWebex en el Centro de ayuda del sitio web de Webex.

Nombre de inquilino

Introduce un nombre que identifique esta Webex instancia única. AppFabricusa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará tu ID de Webex cliente. Siga los pasos siguientes para encontrar su ID de cliente de Webex:

1. Inicie sesión en su cuenta de Webex en https://developer.webex.com.
2. Elija su avatar en la parte superior derecha.

3. Elija Mis aplicaciones de Webex.
4. Elija la aplicación OAuth2 que utiliza. AppFabric
5. Introduzca el ID de cliente de esta página en el campo ID de cliente de. AppFabric

Secreto del cliente

AppFabric solicitará su secreto de Webex cliente. Webexsolo presenta el secreto de tu cliente una vez cuando creaste tu aplicación OAuth por primera vez. Para generar un nuevo secreto de cliente si no guardó el secreto de cliente inicial, siga los pasos siguientes:

1. Inicie sesión en su cuenta de Webex en https://developer.webex.com.
2. Elija su avatar en la parte superior derecha.
3. Elija Mis aplicaciones de Webex.
4. Elige la aplicación OAuth2 que utilizas. AppFabric
5. En esta página, genere un nuevo secreto de cliente.
6. Introduzca el nuevo secreto de cliente en el campo Secreto de cliente de. AppFabric

Cómo aprobar la autorización

Después de crear la autorización de la aplicación, AppFabric recibirá una ventana emergente Webex para aprobar la autorización. Para aprobar la AppFabric autorización, selecciona aceptar.

Zendesk

Zendesk inició la revolución de la experiencia del cliente en 2007 al hacer posible que cualquier empresa del mundo pudiera ofrecer su servicio de atención al cliente en línea. En la actualidad, Zendesk es el paladín de ofrecer un excelente servicio en todas partes y para todos, y potencia miles de millones de conversaciones, conectando a más de 100 000 marcas con cientos de millones de clientes a través de telefonía, chat, correo electrónico, mensajería, canales sociales, comunidades, sitios de reseñas y centros de ayuda. Los productos de Zendesk se crean con amor para ser amados. La empresa se concibió en Copenhague (Dinamarca), se construyó y desarrolló en California y, en la actualidad, emplea a más de 6000 personas en todo el mundo.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosZendesk, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Zendesk
- AppFabric Conectarse a tu Zendesk cuenta

AppFabric soporte para Zendesk

AppFabric admite la recepción de información de usuario y registros de auditoría desdeZendesk.

Requisitos previos

Para poder AppFabric transferir los registros de auditoría Zendesk a destinos compatibles, debe cumplir los siguientes requisitos:

- Debe tener una cuenta Suite Enterprise o Enterprise Plus de Zendesk o una cuenta Support Enterprise de Zendesk. Para obtener más información sobre cómo crear o actualizar a una cuenta de Enterprise de Zendesk , consulte Ver su tipo de plan de Zendesk en el sitio web de Zendesk.
- Debe tener un usuario con el rol de Administrador en su cuenta de Zendesk. Para obtener más información sobre los roles, consulte Entender los roles de usuario de soporte de Zendesk en el sitio web de Zendesk.

Consideraciones de límites de velocidad

Zendesk impone límites de velocidad a la API de Zendesk. Para obtener más información sobre los límites de velocidad para la API de Zendesk, consulte Límites de velocidad en la Guía para desarrolladores de Zendesk en el sitio web de Zendesk. Si la combinación de las aplicaciones de Zendesk API existentes AppFabric y las aplicaciones de API existentes supera el límite, es AppFabric posible que los registros de auditoría se retrasen.

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de hasta 30 minutos para que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos. Sin embargo, esto puede personalizarse a nivel de cuenta. Para obtener ayuda, póngase en contacto con AWS Support.

AppFabric Conectarse a tu Zendesk cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conZendesk. Para encontrar la información necesaria para realizar Zendesk la autorización AppFabric, sigue estos pasos.

Cómo crear una aplicación OAuth

AppFabric se integra con el Zendesk uso de OAuth. En Zendesk, debe crear una aplicación OAuth con la siguiente configuración:

1. Siga las instrucciones de la sección Registrar su aplicación en Zendesk del artículo Cómo usar la autenticación OAuth con su aplicación en el sitio web de Soporte de Zendesk.
2. Utilice una URL de redireccionamiento con el siguiente formato.

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

   En esta URL, *<region>* está el código Región de AWS en el que configuraste tu paquete de AppFabric aplicaciones. Por ejemplo, el código de la región del Este de EE. UU. (Norte de Virginia) es `us-east-1`. Para esa región, la URL de redireccionamiento es `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará tu ID de inquilino. El ID de inquilino AppFabric es tu Zendesk subdominio. Para obtener más información sobre cómo encontrar su subdominio de Zendesk, consulte Dónde puedo encontrar mi subdominio de Zendesk en el sitio web de Soporte de Zendesk.

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de Zendesk. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier ingesta creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará un ID de cliente. El ID de cliente que aparece AppFabric es el identificador único de su Zendesk API. Para encontrar su identificador único de Zendesk, siga los pasos siguientes:

1. Diríjase al Centro de administración de su cuenta de Zendesk.
2. Seleccione Aplicaciones e integraciones.
3. Elija API, API de Zendesk.
4. Seleccione la pestaña Clientes de OAuth.
5. Elige la aplicación OAuth para la que has creado. AppFabric
6. Introduce el identificador único de tu cliente OAuth en el campo ID de cliente de. AppFabric

Secreto del cliente

AppFabric solicitará un secreto de cliente. El identificador secreto del cliente AppFabric es tu token Zendesk secreto. Zendeskpresenta tu token secreto solo una vez cuando creas tu aplicación Zendesk OAuth por primera vez. Para generar un nuevo token secreto si no guardó el token secreto inicial, siga los pasos siguientes:

1. Diríjase al Centro de administración de su cuenta de Zendesk.
2. Seleccione Aplicaciones e integraciones.
3. Elija API, API de Zendesk.
4. Seleccione la pestaña Clientes de OAuth.
5. Elige la aplicación OAuth para la que la has creado. AppFabric
6. Pulse el botón Regenerar situado junto al campo Token secreto.
7. Introduce el nuevo token secreto en el campo Secreto del cliente de. AppFabric

Cómo aprobar la autorización

Tras crear la autorización de la aplicación AppFabric, aparecerá una ventana emergente Zendesk para aprobarla. Para aprobar la AppFabric autorización, selecciona Permitir.

Zoom

Zoomes una plataforma de colaboración all-in-one inteligente que hace que la conexión sea más fácil, inmersiva y dinámica para empresas y particulares. ZoomLa tecnología pone a las personas en el centro de atención, posibilita conexiones significativas, facilita la colaboración moderna e impulsa la innovación humana a través de soluciones como el chat en equipo, el teléfono, las reuniones, el centro de atención omnicanal en la nube, las grabaciones inteligentes, la pizarra y más, todo en una sola oferta.

Puede utilizarlos por motivos de seguridad AWS AppFabric para recibir registros de auditoría y datos de usuariosZoom, normalizar los datos al formato Open Cybersecurity Schema Framework (OCSF) y enviar los datos a un bucket de Amazon Simple Storage Service (Amazon S3) o a una transmisión de Amazon Data Firehose.

Temas

- AppFabric soporte para Zoom
- AppFabric Conectarse a su Zoom cuenta

AppFabric soporte para Zoom

AppFabric admite la recepción de información de usuario y registros de auditoría desdeZoom.

Requisitos previos

AppFabric Para poder transferir los registros de auditoría Zoom a los destinos admitidos, debe cumplir los siguientes requisitos:

- Debe tener un plan Pro, Business, Education o Enterprise de Zoom.
- Tu función Zoom de administrador debe tener permiso para crear aplicaciones de server-to-server OAuth. Para obtener información sobre cómo habilitar las aplicaciones server-to-server OAuth, consulta la sección Habilitar permisos de la página OAuth de servidor a servidor en la Guía para desarrolladores del sitio web. Zoom Zoom
- Su función de administrador de Zoom debe tener permiso para ver los registros de actividad de administrador e iniciar o cerrar sesión en la actividad de auditoría. Para obtener más información sobre cómo habilitar el permiso para ver la actividad de auditoría, consulte Uso de la administración de roles y Uso de registros de actividad de administración en el sitio web de Soporte de Zoom.

Consideraciones de límites de velocidad

Zoom impone límites de velocidad a la API de Zoom. Para obtener más información sobre los límites de velocidad para la API de Zoom, consulte Límites de velocidad en el sitio web Guía para desarrolladores de Zoom. Si la combinación de las aplicaciones existentes AppFabric y las Zoom aplicaciones existentes supera el límite, es posible que los registros de auditoría que aparezcan se retrasen. AppFabric

Consideraciones sobre el retraso de datos

Es posible que se produzca un retraso de aproximadamente 24 horas antes de que un evento de auditoría se entregue a su destino. Esto se debe al retraso con el que la aplicación envía los eventos de auditoría, así como a las protecciones adoptadas para reducir la pérdida de datos.

AppFabric Conectarse a su Zoom cuenta

Después de crear tu paquete de aplicaciones dentro del AppFabric servicio, debes autorizarlo AppFabric conZoom. Para encontrar la información necesaria para realizar Zoom la autorización AppFabric, sigue estos pasos.

Crea una aplicación server-to-server OAuth

AppFabric usa server-to-server OAuth con las credenciales de la aplicación para integrarse. Zoom Para crear una aplicación server-to-server OAuth enZoom, sigue las instrucciones de la Guía para desarrolladores sobre cómo crear una aplicación OAuth de servidor a servidor. Zoom AppFabric no admite Zoom webhooks, por lo que puedes saltarte la sección para añadir suscripciones a webhooks.

Ámbitos obligatorios

Debes añadir los siguientes ámbitos a tu Zoom server-to-server aplicación OAuth:

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

Autorizaciones de la aplicación

ID de inquilino

AppFabric solicitará tu ID de inquilino. El ID de inquilino AppFabric es el ID de la Zoom cuenta. Para encontrar su ID de cuenta de Zoom, siga los pasos siguientes:

1. Vaya al Marketplace de Zoom.
2. Elija Administrar.
3. Elige la aplicación de server-to-server OAuth que utilizas. AppFabric
4. Introduce el ID de cuenta de la página de credenciales de la aplicación en el campo ID de inquilino de. AppFabric

Nombre de inquilino

Introduzca un nombre que identifique esta organización única de Zoom. AppFabric usa el nombre del inquilino para etiquetar las autorizaciones de la aplicación y cualquier incorporación creada a partir de la autorización de la aplicación.

ID de cliente

AppFabric solicitará tu ID de cliente. Siga los pasos siguientes para encontrar su ID de cliente de Zoom:

1. Vaya al Marketplace de Zoom.
2. Elija Administrar.
3. Elige la aplicación de server-to-server OAuth que utilizas. AppFabric
4. Introduce el ID de cliente de la página de credenciales de la aplicación en el campo ID de cliente de. AppFabric

Secreto del cliente

AppFabric solicitará el secreto de su cliente. Siga los pasos siguientes para encontrar su secreto de cliente de Zoom:

1. Vaya al Marketplace de Zoom.
2. Elija Administrar.
3. Elige la aplicación de server-to-server OAuth que utilizas. AppFabric
4. Introduce el secreto del cliente de la página de credenciales de la aplicación en el campo secreto del cliente de. AppFabric

Entrega de registro de auditoría

Zoom pone a disposición los registros de auditoría accediendo a la API cada 24 horas. Al consultar los registros de auditoría AppFabric, los datos que busca Zoom corresponden a las actividades del día anterior.

Herramientas y servicios de seguridad compatibles

AWS AppFabric for security admite la integración con las siguientes herramientas y servicios de seguridad. Elija el nombre de un servicio para obtener más información sobre cómo configurar la seguridad AppFabric para conectarse a él.

Temas

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

Barracuda XDR

Barracuda Networks es un socio de confianza y un proveedor líder de soluciones de seguridad centradas en la nube, que protege el correo electrónico, las redes, los datos y las aplicaciones con soluciones innovadoras que crecen y se adaptan a la trayectoria de las empresas. Barracuda XDR es una solución amplia y abierta de detección y respuesta que combina tecnologías sofisticadas con un equipo de analistas de seguridad en nuestro centro de operaciones de seguridad (SOC). La plataforma Barracuda XDR analiza miles de millones de eventos sin procesar a diario, a partir de más de 40 orígenes de datos integrados y, junto con amplias normas de detección de amenazas que se adaptan al marco MITRE ATT&CK®, puede detectar las amenazas con mayor rapidez y reducir el tiempo de respuesta.

AWS AppFabric consideraciones sobre la ingesta de registros de auditoría

En las siguientes secciones se describe el esquema AppFabric de salida, los formatos de salida y los destinos de salida con Barracuda XDR los que se va a utilizar.

Esquema y formato

Barracuda XDRadmite los siguientes esquemas y formatos de AppFabric salida:

- OCSF - JSON: AppFabric normaliza los datos mediante el Open Cybersecurity Schema Framework (OCSF) y genera los datos en formato JSON.

Ubicaciones de salida

Barracuda XDR admite la recepción de registros de auditoría de Amazon Security Lake. Para enviar datos de a, siga las AppFabric instrucciones que Barracuda XDR se indican a continuación:

1. Enviar datos a Amazon Security Lake: AppFabric configúrelo para enviar datos a Amazon Security Lake a través de una Amazon Data Firehose. Para obtener más información, consulte Amazon Security Lake.
2. Enviar datos a Barracuda XDR: configure Barracuda XDR para recibir registros de auditoría de Amazon Security Lake. Para obtener más información, consulte Configuración y uso de Amazon Security Lake.

Dynatrace

Dynatrace® PlatformCombina una observabilidad amplia y profunda y una seguridad de aplicaciones en tiempo de ejecución continuo con AIOps avanzados para proporcionar respuestas y una automatización inteligente a partir de los datos. Esto permite a los innovadores modernizar y automatizar las operaciones en la nube, ofrecer software de forma más rápida y segura y garantizar experiencias digitales impecables.

AWS AppFabric consideraciones sobre la ingesta de registros de auditoría

En las siguientes secciones se describen el esquema AppFabric de salida, los formatos de salida y los destinos de salida que se van a utilizar con. Dynatrace Platform

Esquema y formato

Dynatrace PlatformEs compatible con los siguientes esquemas y formatos de AppFabric salida:

- OCSF - JSON: AppFabric normaliza los datos mediante el Open Cybersecurity Schema Framework (OCSF) y genera los datos en formato JSON.

Ubicaciones de salida

Dynatrace PlatformAdmite la recepción de registros de auditoría de las siguientes ubicaciones de salida AppFabric .

- Amazon Simple Storage Service (Amazon S3)
  - Para configurar la Dynatrace Platform recepción de datos del bucket de Amazon S3 que contiene sus registros de auditoría, siga las instrucciones del proyecto S3 Log Forwarder de Dynatrace en. GitHub

Logz.io

Logz.io ayuda a las empresas nativas en la nube a supervisar y proteger sus entornos a través de Logz.io Open 360 Platform, transformando la observabilidad y la seguridad de una carga de alto costo y escaso valor en un factor de alto valor y rentable que permite obtener mejores resultados empresariales.

Logz.io Cloud SIEM aborda directamente los principales desafíos de seguridad actuales, desde la sobrecarga de datos hasta la omnipresente brecha de habilidades cibernéticas, mediante consultas rápidas, detección multidimensional y contenido de seguridad profundamente personalizable. Estos contribuyen a monitorear e investigar toda la extensión de su entorno de nube, sin degradación del rendimiento e independientemente de los volúmenes de datos.

La solución Logz.io se diseñó específicamente para ofrecer análisis e investigaciones de amenazas avanzados con una complejidad y un costo menores. Los clientes cuentan con el respaldo de analistas de seguridad especializados, contenido sobre amenazas como servicio y funciones respaldadas por la IA, que están diseñadas específicamente para ayudar a reducir el ruido de los datos y centrarse en la información que permite a su equipo priorizar rápidamente las amenazas del mundo real.

AWS AppFabric consideraciones sobre la ingesta de registros de auditoría

En las siguientes secciones se describe el esquema AppFabric de salida, los formatos de salida y los destinos de salida que se van a Logz.io utilizar.

Esquema y formato

Logz.ioadmite los siguientes esquemas y formatos de AppFabric salida:

- Sin procesar: JSON

  - AppFabric genera datos en el esquema original utilizado por la aplicación de origen en formato JSON.
- OCSF: JSON
  - AppFabric normaliza los datos mediante el Open Cybersecurity Schema Framework (OCSF) y genera los datos en formato JSON.

Ubicaciones de salida

Logz.ioadmite las siguientes ubicaciones de AppFabric salida:

- Amazon Data Firehose
  - Para configurar la transmisión de entrega de Firehose para que envíe datos aLogz.io, sigue las instrucciones de Choose Logz.io for Your Destination en la Guía para desarrolladores de Amazon Data Firehose.
- Amazon Simple Storage Service (Amazon S3)
  - A fin de configurar Logz.io para la recepción de datos del bucket de Amazon S3 que contiene sus registros de auditoría, siga las instrucciones en Configurar un bucket de Amazon S3 en el sitio web de Logz.io.

Netskope

Netskope, líder mundial en ciberseguridad, está redefiniendo la seguridad de la nube, los datos y la red para ayudar a las organizaciones a aplicar el principio de confianza cero en la protección de sus datos. La plataforma Netskope, rápida y fácil de usar, proporciona un acceso optimizado y una seguridad de confianza cero para personas, dispositivos y datos dondequiera que estén. Netskope ayuda a sus clientes a reducir el riesgo, acelerar el rendimiento y conseguir una visibilidad inigualable de cualquier actividad en la nube, la web y las aplicaciones privadas. Miles de clientes, incluidos más de 25 empresas de la lista Fortune 100, confían en Netskope su poderosa NewEdge red para hacer frente a las amenazas en constante evolución, los nuevos riesgos, los cambios tecnológicos, los cambios organizativos y de red y los nuevos requisitos normativos. Descubra cómo Netskope ayuda a sus clientes a estar preparados en cualquier etapa de su proceso SASE visitando netskope.com.

AWS AppFabric consideraciones sobre la ingesta de registros de auditoría

En las siguientes secciones se describe el esquema AppFabric de salida, los formatos de salida y los destinos de salida que se van a Netskope utilizar.

Esquema y formato

Netskopeadmite los siguientes esquemas y formatos de AppFabric salida:

- Sin procesar: JSON
  - AppFabric genera datos en el esquema original utilizado por la aplicación de origen en formato JSON.
- OCSF: JSON
  - AppFabric normaliza los datos mediante el Open Cybersecurity Schema Framework (OCSF) y genera los datos en formato JSON.

Ubicaciones de salida

Netskopeadmite la siguiente ubicación de AppFabric salida:

- Amazon Simple Storage Service (Amazon S3)
  - Para configurar Netskope para la recepción de datos del bucket de Amazon S3 que contiene sus registros de auditoría, siga las instrucciones de Protección de datos para Amazon Web Services S3 que encontrará en el sitio web de Netskope.

NetWitness

NetWitness es uno de los principales desarrolladores de software de detección y respuesta ampliadas (XDR). Su base global de clientes muy preocupados por la seguridad confía en NetWitness XDR para defenderse de adversarios sofisticados y agresivos. Con la plataforma más completa, integrada y avanzada del sector para detectar, investigar y responder a los ataques digitales, NetWitness XDR es la base unificadora de un SOC moderno y eficaz.

Gracias a su arquitectura altamente modular, NetWitness XDR detecta las amenazas dondequiera que se produzcan: en la nube, en las instalaciones, con trabajadores móviles y remotos, o en cualquier punto intermedio. La plataforma NetWitness XDR ofrece una visibilidad completa combinada con inteligencia de amenazas aplicada y análisis del comportamiento de los usuarios para detectar las amenazas, priorizar las actividades, investigar y automatizar la respuesta. Todo esto permite a los analistas de seguridad contar con una eficiencia mejor y más rápida para mantener las operaciones de seguridad muy por delante de las amenazas que afectan a la empresa.

AWS AppFabric consideraciones sobre la ingesta de registros de auditoría

En las siguientes secciones se describe el esquema AppFabric de salida, los formatos de salida y los destinos de salida con NetWitness los que se va a utilizar.

Esquema y formato

NetWitness admite los siguientes esquemas y formatos de AppFabric salida:

- Sin procesar: JSON
  - AppFabric genera datos en el esquema original utilizado por la aplicación de origen en formato JSON.
- OCSF: JSON
  - AppFabric normaliza los datos mediante el Open Cybersecurity Schema Framework (OCSF) y genera los datos en formato JSON.

Ubicaciones de salida

NetWitnessadmite la siguiente ubicación de AppFabric salida:

- Amazon Simple Storage Service (Amazon S3)
  - Para configurar NetWitness para la recepción de datos del bucket de Amazon S3 que contiene sus registros de auditoría, siga las instrucciones de la Guía de configuración del registro de fuentes de eventos de S3 Universal Connector en la página de Integraciones de la plataforma de NetWitness en el sitio web de NetWitness.

Amazon QuickSight

Amazon QuickSight impulsa a las organizaciones basadas en datos con inteligencia empresarial (BI) unificada a hiperescala. De este QuickSight modo, todos los usuarios pueden satisfacer diferentes necesidades analíticas partiendo de la misma fuente de información mediante modernos paneles interactivos, informes paginados, análisis integrados y consultas en lenguaje natural. Para analizar los datos de los registros de AWS AppFabric auditoría QuickSight, elija como fuente el depósito de Amazon Simple Storage Service (Amazon S3), en el que AppFabric se almacenan los registros de seguridad.

AppFabric consideraciones sobre la ingesta de registros de auditoría

En las siguientes secciones se describen el esquema AppFabric de salida, los formatos de salida y los destinos de salida que se van a usar con Amazon QuickSight.

Esquema y formatos

QuickSight admite los siguientes esquemas y formatos de AppFabric salida:

- Sin procesar: JSON
  - AppFabric genera datos en el esquema original utilizado por la aplicación de origen en formato JSON.
- OCSF: JSON
  - AppFabric normaliza los datos mediante el Open Cybersecurity Schema Framework (OCSF) y genera los datos en formato JSON.

Ubicaciones de salida

QuickSight admite las siguientes ubicaciones de AppFabric salida:

- Amazon S3
  - Puede incorporar datos de Amazon S3 directamente a través de la creación QuickSight de un conjunto de datos con archivos de Amazon S3. Para comprobar que tu conjunto de archivos de destino no supera las cuotas de fuentes de QuickSight datos, consulta las cuotas de fuentes de datos en la Guía del QuickSight usuario de Amazon.
  - Si su conjunto de archivos supera QuickSight las cuotas de una fuente de datos de Amazon S3, puede ingerir los datos en Amazon S3 mediante Amazon Athena AWS Glue y tablas. El uso de Athena en su QuickSight conjunto de datos implicará costes adicionales. Para obtener más información acerca de los precios, consulte la página de precios de Athena.

    Para utilizar Athena:

    1. Siga las instrucciones de Uso de AWS Glue para conectarse al origen de datos en Amazon S3 de la Guía del usuario de Athena.
    2. Sigue las instrucciones de Crear un conjunto de datos con datos de Athena en la Guía QuickSight del usuario de Amazon.

Rapid7

Rapid7, Inc. tiene la misión de crear un mundo digital más seguro haciendo que la ciberseguridad sea más simple y accesible. Rapid7permite a los profesionales de la seguridad gestionar una superficie de ataque moderna mediante best-in-class la tecnología, la investigación de vanguardia y una amplia experiencia estratégica. Rapid7nuestras soluciones de seguridad integrales ayudan a más de 10 000 clientes de todo el mundo a unir la gestión de riesgos en la nube y la detección de amenazas para reducir las superficies de ataque y eliminar las amenazas con rapidez y precisión.

AWS AppFabric consideraciones sobre la ingesta de registros de auditoría

En las siguientes secciones se describen el esquema AppFabric de salida, el formato de salida y los destinos de salida con Rapid7 los que se va a utilizar.

Esquema y formato

Rapid7admite los siguientes esquemas y formatos de AppFabric salida:

- Sin procesar: JSON
  - AppFabric genera datos en el esquema original utilizado por la aplicación de origen en formato JSON.
- OCSF: JSON
  - AppFabric normaliza los datos mediante el Open Cybersecurity Schema Framework (OCSF) y genera los datos en formato JSON.

Ubicaciones de salida

Rapid7admite la siguiente ubicación de AppFabric salida:

- Amazon Simple Storage Service (Amazon S3)
  - Para configurar Rapid7 para la recepción de datos del bucket de Amazon S3 que contiene sus registros de auditoría, siga las instrucciones de la publicación del blog Cómo supervisar su actividad en Amazon S3 con InsightIDR que encontrará en el sitio web del blog de Rapid7.

Amazon Security Lake

Amazon Security Lake centraliza automáticamente los datos de seguridad de los AWS entornos, los proveedores de software como servicio (SaaS) y las fuentes locales y en la nube en un lago de datos

diseñado específicamente y almacenado en su interior. Cuenta de AWS Con Security Lake, puede obtener una comprensión más completa de sus datos de seguridad en toda su organización. Security Lake ha adoptado el Open Cybersecurity Schema Framework (OCSF), un esquema de eventos de seguridad de origen abierto. Gracias a la compatibilidad con OCSF, el servicio normaliza y combina los datos de seguridad procedentes de una amplia gama de AWS fuentes de datos de seguridad empresariales.

AppFabric consideraciones sobre la ingesta de registros de auditoría

Puede incluir sus registros de auditoría de SaaS en Amazon Security Lake Cuenta de AWS añadiendo una fuente personalizada a Security Lake. En las siguientes secciones se describen el esquema AppFabric de salida, el formato de salida y los destinos de salida que se van a usar con Security Lake.

Esquema y formato

Security Lake admite el siguiente esquema y formato de AppFabric salida:

- OCSF: JSON
  - AppFabric normaliza los datos mediante el Open Cybersecurity Schema Framework (OCSF) y genera los datos en formato JSON.

Ubicaciones de salida

Security Lake admite AppFabric como fuente personalizada el uso de un flujo de entrega de Amazon Data Firehose como ubicación de salida de la AppFabric ingesta. Para configurar la AWS Glue tabla y el flujo de entrega de Firehose, así como para configurar una fuente personalizada en Security Lake, utilice los siguientes procedimientos.

Cree una tabla AWS Glue

1. Navegue a Amazon Simple Storage Service (Amazon S3) y cree un bucket con un nombre de su elección.
2. Navega hasta la AWS Glue consola.
3. Para el Catálogo de datos, vaya a la sección Tablas y seleccione Añadir tabla.
4. Introduzca el nombre que desee para esta tabla.
5. Elija el bucket de Amazon S3 que ha creado en el paso 1.

6. Para el formato de datos, seleccione JSON y Siguiente.
7. En la página Elegir o definir esquema, seleccione Editar esquema como JSON.
8. Introduzca el siguiente esquema y complete el proceso de creación de la AWS Glue tabla.

```
[
    {
        "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>"
    }
]
```

Cómo crear una fuente personalizada en Security Lake

1. Vaya a la consola de Amazon Security Lake.
2. Seleccione Fuentes personalizadas en el panel de navegación.
3. Seleccione Crear acción personalizada.
4. Ingrese un nombre para la fuente personalizada y seleccione una clase de evento de OCSF correspondiente.

> **Note**
>
> AppFabric utiliza las clases de eventos de cambio de cuenta, autenticación, administración de acceso de usuarios, administración de grupos, actividad de recursos web y actividad de acceso a recursos web.

5. Introduzca su Cuenta de AWS ID tanto para el ID como para el Cuenta de AWS ID externo. A continuación, elija Crear.
6. Guarde la ubicación de Amazon S3 de la fuente personalizada. La usarás para configurar una transmisión de entrega de Amazon Data Firehose.

Crea un flujo de entrega en Firehose

1. Navegue hasta la consola Amazon Data Firehose.
2. Elija Crear un flujo de entrega.
3. En Fuente, seleccione PUT directo.
4. Para Destino: elija S3.
5. En la sección Transformar y convertir registros, elija Habilitar la conversión del formato de registro y elija Apache Parquet como formato de salida.
6. Para la AWS Glue tabla, elija la AWS Glue tabla que creó en el procedimiento anterior y elija la versión más reciente.
7. En la Configuración de destino, elija el bucket de Amazon S3 que creó con la fuente personalizada de Security Lake.
8. Para la Partición dinámica, seleccione Activado.
9. Para el Análisis en línea de JSON, seleccione Activado.
   - Para Nombre de clave, introduzca `eventDayValue`.
   - Para Expresión JQ, introduzca `(.time/1000)|strftime("%Y%m%d")`.
10. Para el Prefijo del bucket S3, introduzca el siguiente valor.

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

    Sustituya <region>y por <account_id>su Cuenta de AWS ID Región de AWS y.
11. Para el prefijo de salida del bucket S3, introduzca el siguiente valor.

    ```
    ext/AppFabric/error/
    ```
12. Para la Duración del reintento, seleccione 300.
13. Para el Tamaño del búfer, seleccione 128 MiB.
14. Para el Intervalo del búfer, seleccione 60s.
15. Completa el proceso de creación del flujo de entrega de Firehose.

Crea ingestas AppFabric

Para enviar datos a Amazon Security Lake, debe crear una ingesta en la AppFabric consola que utilice la transmisión de entrega de Firehose que creó anteriormente como ubicación de salida. Para obtener más información sobre cómo configurar AppFabric las ingestiones para usar Firehose como ubicación de salida, consulta Crear una ubicación de salida.

Singularity Cloud

La Singularity Cloud plataforma protege a su empresa de amenazas de todas las categorías y en todas las etapas. Su IA (inteligencia artificial) patentada amplía la seguridad desde las firmas y patrones conocidos hasta los ataques más sofisticados, como los ataques de día cero y el ransomware.

AWS AppFabric consideraciones sobre la ingesta de registros de auditoría

En las siguientes secciones se describe el esquema AppFabric de salida, los formatos de salida y los destinos de salida que se van a Singularity Cloud utilizar.

Esquema y formato

Singularity Cloudadmite los siguientes esquemas y formatos de AppFabric salida:

OCSF - JSON: AppFabric normaliza los datos mediante el Open Cybersecurity Schema Framework (OCSF) y genera los datos en formato JSON.

Ubicaciones de salida

Singularity Cloudadmite la recepción de registros de auditoría de las siguientes ubicaciones de salida AppFabric .

- Amazon Simple Storage Service (Amazon S3)
  - Singularity CloudPara configurar la recepción de datos del bucket de Amazon S3 que contiene sus registros de auditoría, siga las instrucciones de la Singularity Cloud’s documentación.

Splunk

Splunk ayuda a que las organizaciones sean más resilientes. Las principales organizaciones utilizan la plataforma unificada de seguridad y observabilidad de Splunk para mantener sus sistemas digitales seguros y confiables. Las organizaciones confían en Splunk para evitar que los problemas

de seguridad, infraestructura y aplicaciones se conviertan en incidentes importantes, absorber los impactos de las interrupciones digitales y acelerar la transformación digital.

AWS AppFabric consideraciones sobre la ingesta de registros de auditoría

En las siguientes secciones se describe el esquema AppFabric de salida, los formatos de salida y los destinos de salida con Splunk los que se va a utilizar.

Esquema y formato

Splunk admite los siguientes esquemas y formatos de AppFabric salida:

- Sin procesar: JSON
  - AppFabric genera datos en el esquema original utilizado por la aplicación fuente en formato JSON.
- OCSF: JSON
  - AppFabric normaliza los datos mediante el Open Cybersecurity Schema Framework (OCSF) y genera los datos en formato JSON.
- OCSF: Parquet
  - AppFabric normaliza los datos mediante el Open Cybersecurity Schema Framework (OCSF) y genera los datos en ese formato. Apache Parquet

Ubicaciones de salida

Splunkadmite las siguientes ubicaciones de AppFabric salida:

- Amazon Data Firehose
  - SplunkPara configurar la recepción de registros de auditoría de la transmisión de Firehose que contiene tus registros de auditoría, sigue las instrucciones del Splunkcomplemento para Amazon Data Firehose en el sitio web. Splunk
- Amazon Simple Storage Service (Amazon S3)
  - A fin de configurar Splunk para la recepción de datos del bucket de Amazon S3 que contiene sus registros de auditoría, siga las instrucciones en Configurar entradas S3 basadas en SQL del complemento Splunk para AWS del sitio web de Splunk.

Eliminar AWS AppFabric para recursos de seguridad

Si no quieres seguir utilizándolos AWS AppFabric por motivos de seguridad, asegúrate de eliminar los datos de las ubicaciones de salida que creaste durante la configuración y de tus recursos de seguridad AppFabric para evitar incurrir en cargos adicionales. Para limpiar sus AppFabric recursos, debe eliminar los recursos en el orden inverso al que los creó para cada aplicación de software como servicio (SaaS): Destinos de ingestión > Ingestas > Autorización de aplicaciones > Paquetes de aplicaciones

Una vez que haya eliminado la autorización final de la aplicación, podrá eliminar la agrupación de aplicaciones.

Temas

- Cómo eliminar un destino de ingesta
- Cómo eliminar una ingesta
- Cómo eliminar la autorización de una aplicación
- Cómo eliminar una agrupación de aplicaciones

Cómo eliminar un destino de ingesta

Si selecciona una ubicación de salida al crear una ingesta, AppFabric por motivos de seguridad, crea destinos de ingesta en su nombre. Para eliminar un destino de ingesta, siga los pasos siguientes:

1. Abra la AppFabric consola en https://console.aws.amazon.com/appfabric/.
2. En la página de Introducción, expanda el menú de la izquierda.
3. Elija Ingestas.
4. Elija una autorización de aplicación.
5. Seleccione el botón de opción junto al destino que desee eliminar y seleccione Eliminar.
6. Elija Eliminar en el cuadro de diálogo de destino para confirmar.
7. Repita los pasos anteriores para todos sus destinos.

Cómo eliminar una ingesta

Para eliminar una ingesta, siga los pasos siguientes:

1. En la página de Introducción, expanda el menú de la izquierda.
2. Elija Ingestas.
3. Seleccione el botón de opciones que se encuentra junto a la autorización de su aplicación.
4. Elija el menú desplegable Acciones.
5. Elija Eliminar.
6. Elija Eliminar en el cuadro de diálogo de ingesta para confirmar.

Cómo eliminar la autorización de una aplicación

Para eliminar la autorización de una aplicación, siga los pasos siguientes:

1. En la página de Introducción, expanda el menú de la izquierda.
2. Seleccione Autorizaciones de aplicaciones.
3. Seleccione el botón de opciones que se encuentra junto a la autorización que desea eliminar.
4. Elija el menú desplegable Acciones.
5. Elija Eliminar.
6. Elija Eliminar en el cuadro de diálogo de ingesta para confirmar.

Cómo eliminar una agrupación de aplicaciones

Para eliminar su agrupación de aplicaciones, use los pasos siguientes:

1. En la página de Introducción, expanda el menú de la izquierda.
2. Elija Agrupación de aplicaciones.
3. Elija el botón Eliminar.
4. Escriba `delete` para confirmar y luego elija Eliminar.

¿Qué es AWS AppFabric para la productividad?

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

> **Note**
>
> Desarrollado por Amazon Bedrock: AWS implementa la detección automática de abusos. Dado que AWS AppFabric la productividad se basa en Amazon Bedrock, los usuarios heredan los controles implementados en Amazon Bedrock para garantizar la protección, la seguridad y el uso responsable de la IA.

AWS AppFabric for productivity (versión preliminar) ayuda a reimaginar la productividad de los usuarios finales en aplicaciones de terceros al generar información y acciones contextualizadas a partir de múltiples aplicaciones. Los desarrolladores de aplicaciones valoran el acceso a datos de usuario de otras aplicaciones para mejorar la experiencia, pero buscan evitar la creación y administración de integraciones con cada aplicación individualmente. En cuanto AppFabric a la productividad, los desarrolladores de aplicaciones tienen acceso a API generativas impulsadas por IA que generan información y acciones sobre datos entre aplicaciones para ofrecer experiencias más enriquecedoras a los usuarios finales a través de asistentes de IA generativa nuevos o existentes. AppFabric para mejorar la productividad, integra datos de varias aplicaciones, lo que elimina la necesidad de que los desarrolladores creen o mantengan integraciones. point-to-point Los desarrolladores de aplicaciones pueden incorporarlos directamente AppFabric para aumentar la productividad en la interfaz de usuario de sus aplicaciones, manteniendo una experiencia coherente para sus usuarios finales y, al mismo tiempo, descubriendo el contexto relevante de otras aplicaciones.

AppFabric para aumentar la productividad conecta los datos de las aplicaciones más utilizadasAsana, como,,Atlassian Jira Suite,Google Workspace,,Microsoft 365,Miro,,Slack,Smartsheet, y más. AppFabric for productivity ofrece a los desarrolladores de aplicaciones una forma más sencilla de crear experiencias de aplicaciones más personalizadas que mejoran la adopción, la satisfacción y la fidelidad de los usuarios. Al mismo tiempo, los usuarios finales pueden obtener información de todas sus aplicaciones sin interrumpir su trabajo.

Temas

- Ventajas
- Casos de uso
- Acceso AppFabric para aumentar la productividad
- Introducción a la AppFabric productividad (versión preliminar) para desarrolladores de aplicaciones
- Introducción a la AppFabric productividad (vista previa) para los usuarios finales

- AppFabric API de productividad
- Procesamiento de datos

Ventajas

En cuanto AppFabric a la productividad, los desarrolladores de aplicaciones tienen acceso a las API que generan información y acciones sobre datos entre aplicaciones, de forma que pueden ofrecer experiencias más enriquecedoras a los usuarios finales mediante asistentes de IA generativa nuevos o existentes.

- Fuente única de datos de usuarios entre aplicaciones: AppFabric para aumentar la productividad, integra datos de varias aplicaciones, lo que elimina la necesidad de que los desarrolladores creen o mantengan integraciones. point-to-point Los datos de aplicaciones SaaS se procesan para usarlos en otras aplicaciones, por medio de la adaptación automática de diversos tipos de datos a un formato entendible por cualquier aplicación. Esto permite a los desarrolladores incluir más datos que mejoren la productividad de los usuarios.
- Control total de la experiencia del usuario: los desarrolladores incorporan AppFabric el enfoque de productividad directamente en la interfaz de usuario de sus aplicaciones, lo que les permite mantener el control total de la experiencia del usuario y, al mismo tiempo, ofrecer información personalizada y acciones recomendadas a los usuarios finales con el contexto de todas sus aplicaciones. Esto AppFabric hace que la productividad esté disponible en la aplicación SaaS preferida de los usuarios finales y esté accesible en la aplicación que prefieran para completar sus tareas. Los usuarios finales pasan menos tiempo cambiando de una aplicación a otra y pueden mantenerse al día con su trabajo.
- Acelere el tiempo de comercialización: en una sola llamada a la API, los desarrolladores de aplicaciones pueden recibir información a nivel de usuario sobre los datos de un usuario que se generan sin tener que ajustar un modelo, escribir un mensaje personalizado ni crear integraciones en varias aplicaciones. AppFabric resume esta complejidad para permitir a los desarrolladores de aplicaciones crear, integrar o enriquecer las capacidades generativas de IA con mayor rapidez. Esto permite a los desarrolladores de aplicaciones centrar sus recursos en las tareas más importantes.
- Referencias a artefactos para fomentar la confianza de los usuarios: como parte del resultado, AppFabric para aumentar la productividad, aparecerán artefactos relevantes o archivos fuente que se utilizarán para generar la información necesaria para fomentar la confianza del usuario final en los resultados de LLM.

- Permisos de usuario simplificados: los artefactos de usuario que se utilizan para generar información se basan en los elementos a los que tiene acceso el usuario. AppFabric para la productividad, utiliza los permisos y el control de acceso de un ISV como fuente de información fiable.

Casos de uso

Los desarrolladores de aplicaciones pueden utilizar la productividad AppFabric para reimaginar la productividad dentro de sus aplicaciones. AppFabric for productivity ofrece dos API centradas en los siguientes casos de uso para ayudar a sus usuarios finales a ser más productivos:

- Priorice su día
  - La API de información práctica ayuda a los usuarios a administrar mejor su día al obtener información oportuna de todas sus aplicaciones, incluidos los correos electrónicos, el calendario, los mensajes, las tareas y más. Además, los usuarios pueden ejecutar acciones entre aplicaciones, como crear correos electrónicos, programar reuniones y crear elementos de acción desde la aplicación que prefieran. Por ejemplo, un empleado al que le haya ocurrido un aumento de clientes de la noche a la mañana no solo verá un resumen de las conversaciones de la noche, sino que también podrá ver una acción recomendada para programar una reunión con el gerente de cuentas de clientes. Las acciones están completadas previamente con campos necesarios (como el nombre y el propietario de la tarea, o el remitente o destinatario del correo electrónico), con la posibilidad de editar dicha información antes de ejecutar la acción.
- Prepárese para las próximas reuniones
  - La API de preparación para reuniones ayuda a los usuarios a prepararse mejor para las reuniones al resumir el propósito de la reunión y mostrar artefactos pertinentes entre aplicaciones, como correos electrónicos, mensajes y más. Ahora los usuarios pueden prepararse rápidamente para las reuniones y no perder el tiempo al cambiar de una aplicación a otra para buscar contenido.

Acceso AppFabric para aumentar la productividad

AppFabric for productivity se lanza actualmente como versión preliminar y está disponible en el este de EE. UU. (Virginia del Norte) Región de AWS. Para obtener más información al respecto Regiones de AWS, consulte AWS AppFabric los puntos finales y las cuotas en. Referencia general de AWS

En cada región, puede acceder a AppFabric la productividad de cualquiera de las siguientes maneras:

- Como desarrollador de aplicaciones
  - Introducción a la AppFabric productividad (versión preliminar) para desarrolladores de aplicaciones
- Como usuario final
  - Introducción a la AppFabric productividad (vista previa) para los usuarios finales

Introducción a la AppFabric productividad (versión preliminar) para desarrolladores de aplicaciones

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Esta sección ayuda a los desarrolladores de aplicaciones AWS AppFabric a integrar la productividad (vista previa) en sus aplicaciones. AWS AppFabric for productivity permite a los desarrolladores crear experiencias de aplicaciones más sofisticadas para sus usuarios al generar información y acciones impulsadas por la IA a partir de correos electrónicos, eventos del calendario, tareas, mensajes y más en múltiples aplicaciones. Para ver una lista de las aplicaciones compatibles, consulte Aplicaciones AWS AppFabric compatibles.

AppFabric for productivity ofrece a los desarrolladores de aplicaciones el acceso a crear y experimentar en un entorno seguro y controlado. Al empezar a utilizarla AppFabric para fines de productividad, se crea un único usuario de prueba AppClient y se registra uno. Este enfoque está diseñado para ayudarlo a comprender y probar el flujo de autenticación y comunicación entre su aplicación y AppFabric. Después de realizar la prueba con un solo usuario, puede enviar su solicitud AppFabric para su verificación antes de ampliar el acceso a otros usuarios (consulte Paso 5. Solicitud AppFabric para verificar su solicitud). AppFabric verificará la información de la aplicación antes de permitir una adopción generalizada para ayudar a proteger a los desarrolladores de aplicaciones, a los usuarios finales y sus datos, lo que allanará el camino para ampliar la adopción por parte de los usuarios de manera responsable.

Temas

- Requisitos previos
- Paso 1. Cree una AppFabric para la productividad AppClient

- Paso 2. Autenticación y autorización de su aplicación
- Paso 3. Añada la URL del portal de AppFabric usuario a su aplicación
- Paso 4. AppFabric Úselo para mostrar información y acciones entre aplicaciones
- Paso 5. Solicitud AppFabric para verificar su solicitud
- Administrar AppFabric para aumentar la productividad AppClients
- Resolución de problemas

Requisitos previos

Antes de empezar, necesitas crear un Cuenta de AWS. Para obtener más información, consulte Inscríbase en una Cuenta de AWS. También debe crear al menos un usuario con acceso a la política de `"appfabric:CreateAppClient"` IAM que se indica a continuación, con AppFabric la que el usuario podrá registrar su solicitud. Para obtener más información sobre la concesión de permisos AppFabric para las funciones de productividad, consulteAppFabric para ver ejemplos de políticas de IAM de productividad. Si bien disponer de un usuario administrativo es útil, no es obligatorio para la configuración inicial. Para obtener más información, consulte Creación de un usuario con acceso administrativo.

AppFabric para la productividad solo está disponible en EE. UU. Este (Norte de Virginia) durante la versión preliminar. Asegúrese de estar en esta región antes de iniciar los pasos que se indican a continuación.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Paso 1. Cree una AppFabric para la productividad AppClient

Antes de poder empezar a AppFabric buscar información sobre la productividad de su aplicación, debe crear una AppFabric AppClient. Básicamente, An AppClient es su puerta de entrada a AppFabric la productividad, ya que funciona como un cliente de aplicaciones OAuth seguro que permite una comunicación segura entre su aplicación y. AppFabric Cuando crees una AppClient, recibirás un AppClient ID, un identificador único crucial para asegurarte de que AppFabric funciona con tu aplicación y la tuya. Cuenta de AWS

AppFabric for productivity ofrece a los desarrolladores de aplicaciones el acceso a crear y experimentar en un entorno seguro y controlado. Al empezar a utilizarla AppFabric para fines de productividad, se crea un único usuario de prueba AppClient y se registra uno. Este enfoque está diseñado para ayudarlo a comprender y probar el flujo de autenticación y comunicación entre su aplicación y AppFabric. Después de realizar la prueba con un solo usuario, puede enviar su solicitud AppFabric para su verificación antes de ampliar el acceso a otros usuarios (consultePaso 5. Solicitud AppFabric para verificar su solicitud). AppFabric verificará la información de la aplicación antes de permitir una adopción generalizada para ayudar a proteger a los desarrolladores de aplicaciones, a los usuarios finales y sus datos, lo que allanará el camino para ampliar la adopción por parte de los usuarios de manera responsable.

Para crear una AppClient, utilice la operación de la AWS AppFabric `CreateAppClient` API. Si necesitas actualizar la versión AppClient posterior, puedes usar la operación de `UpdateAppClient` API para cambiar solo las URL de redireccionamiento. Si necesitas cambiar alguno de los demás parámetros asociados a tu aplicación, AppClient como el nombre de la aplicación o la descripción, debes eliminarlo AppClient y crear uno nuevo. Para obtener más información, consulte CreateAppClient.

Puede registrar su aplicación en los AWS servicios mediante la `CreateAppClient` API mediante varios lenguajes de programación, incluidos Python, Node.js, Java, C#, Go y Rust. Para obtener más información, consulte Ejemplos de firma de solicitudes en la Guía del usuario de IAM. Debe utilizar las credenciales de su cuenta de Signature versión 4 para realizar esta operación de la API. Para obtener más información sobre la versión 4 de la firma, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Campos requeridos

- `appName`- El nombre de la aplicación que se mostrará a los usuarios en la página de consentimiento del portal de AppFabric usuarios. La página de consentimiento pide permiso a los usuarios finales para mostrar AppFabric información dentro de la aplicación. Para obtener más

detalles sobre la página de consentimiento, consulte Paso 2. Otorgue su consentimiento para que la aplicación muestre información.

- `description`: una descripción de la aplicación.
- `redirectUrls`: el URI al que se redirige a los usuarios finales después de la autorización. Puede agregar hasta 5 redirectUrls. Por ejemplo, `https://localhost:8080`.
- `starterUserEmails`: una dirección de correo electrónico de usuario a la que se permitirá acceder para recibir información hasta que se verifique la aplicación. Solo se permite una dirección de correo electrónico. Por ejemplo, `anyuser@example.com`
- `customerManagedKeyIdentifier` (opcional): el ARN de la clave administrada por el cliente (generada por KMS) que se utilizará para cifrar los datos. Si no se especifica, se utilizará la clave AWS AppFabric gestionada. Para obtener más información acerca de Claves propiedad de AWS las claves administradas por el cliente, consulte Claves de cliente y claves de AWS en la Guía para desarrolladores de AWS Key Management Service .

Campos de respuesta

- `appClientArn`- El nombre del recurso de Amazon (ARN) que incluye el AppClient ID. Por ejemplo, el AppClient ID es`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `verificationStatus`- El estado AppClient de la verificación.
  - `pending_verification`- La verificación del aún AppClient está en curso AppFabric. Hasta que AppClient se verifique, solo un usuario (especificado en`starterUserEmails`) puede usar el AppClient. El usuario verá una notificación en el portal de AppFabric usuarios, introducida enPaso 3. Añada la URL del portal de AppFabric usuario a su aplicación, que indica que la aplicación no está verificada.
  - `verified`- El proceso de verificación se completó correctamente AppFabric y ahora AppClient está completamente verificado.
  - `rejected`- El proceso de verificación del AppClient fue rechazado por AppFabric. AppClient No lo pueden utilizar otros usuarios hasta que el proceso de verificación se reinicie y se complete correctamente.

```
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 la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

```
{
    "appClientConfigSummary": {
        "appClientArn": "arn:aws:appfabric:<region>:<account>:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "verificationStatus": "pending_verification"
    }
}
```

Paso 2. Autenticación y autorización de su aplicación

Permite que tu aplicación integre AppFabric información de forma segura mediante el establecimiento de un flujo de autorización de OAuth 2.0. En primer lugar, debe crear un código de autorización que verifique la identidad de su aplicación. Para obtener más información, consulte Autorizar. Luego, cambiarás este código de autorización por un token de acceso, que otorga a tu aplicación los permisos necesarios para obtener y mostrar AppFabric información dentro de ella. Para obtener más información, consulte Token.

Para obtener más información sobre cómo conceder permisos para autorizar una aplicación, consulte Permitir el acceso para autorizar aplicaciones.

1. Para crear un código de autorización, usa la operación de AWS AppFabric `oauth2/authorize` API.

   Campos requeridos

   - `app_client_id`(obligatorio): el AppClient ID del Cuenta de AWS creado en el paso 1. Crea un AppClient. Por ejemplo, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
   - `redirect_uri` (obligatorio): el URI al que redirigir a los usuarios finales tras la autorización que utilizó en el Paso 1. Crea un AppClient. Por ejemplo, `https://localhost:8080`.

- `state` (obligatorio): un valor único para mantener el estado entre la solicitud y la devolución de llamada. Por ejemplo, `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. Tras la autenticación, se lo redirigirá al URI especificado y se le devolverá un código de autorización como parámetro de consulta. Por ejemplo, escriba `code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`.

```
https://localhost:8080/?code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-
sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-
oampc&state=a8904edc-890c-1005-1996-29a757272a44
```

3. Cambie este código de autorización por un token de acceso mediante la operación AppFabric `oauth2/token` API.

   Este token se usa para las solicitudes de API e inicialmente es válido `starterUserEmails` hasta que AppClient se verifique. Una vez verificado, este token se puede usar para cualquier usuario. AppClient Debe utilizar las credenciales de su cuenta de Signature versión 4 para realizar esta operación de la API. Para obtener más información sobre la versión 4 de la firma, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

   Campos requeridos

   - `code` (obligatorio): el código de autorización que recibió tras autenticarse en el último paso. Por ejemplo, `mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`.
   - `app_client_id`(obligatorio): el AppClient ID de lo Cuenta de AWS creado en el paso 1. Crea un AppClient. Por ejemplo, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
   - `grant_type` (obligatorio): el valor debe ser `authorization_code`.
   - `redirect_uri` (obligatorio): el URI al que redirigir a los usuarios tras la autorización que utilizó en el Paso 1. Crea un AppClient. Debe ser el mismo URI de redireccionamiento que se utilizó para crear un código de autorización. Por ejemplo, `https://localhost:8080`.

Campos de respuesta

- `expires_in`: cuánto falta para que caduque el token. El tiempo de caducidad predeterminado es de 12 horas.
- `refresh_token`: el token de actualización recibido de la solicitud /token inicial.
- `token`: el token recibido de la solicitud /token inicial.
- `token_type`: el valor será `Bearer`.
- `appfabric_user_id`- El AppFabric seudónimo. Se devuelve solo para las solicitudes que utilizan el tipo de concesión `authorization_code`.

```
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 la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

```
{
    "expires_in": 43200,
    "refresh_token": "apkaeibaerjr2example",
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "<userId>"
}
```

Paso 3. Añada la URL del portal de AppFabric usuario a su aplicación

Los usuarios finales deben autorizarse AppFabric a acceder a los datos de sus aplicaciones que se utilizan para generar información. AppFabric elimina la complejidad que supone para los desarrolladores de aplicaciones la responsabilidad de este proceso mediante la creación de un portal de usuario dedicado (una pantalla emergente) para que los usuarios finales autoricen sus aplicaciones. Cuando los usuarios estén preparados AppFabric para aumentar la productividad, accederán al portal de usuarios que les permitirá conectar y gestionar las aplicaciones que se utilizan para generar información y realizar acciones entre aplicaciones. Al iniciar sesión, los usuarios pueden conectar las aplicaciones AppFabric para aumentar la productividad y, después, volver a la aplicación para explorar los conocimientos y las acciones. Para integrar la aplicación con AppFabric fines de productividad, debe añadir una AppFabric URL específica a la aplicación. Este paso es crucial para permitir a los usuarios acceder al portal de AppFabric usuarios directamente desde la aplicación.

1. Navegue hasta la configuración de su aplicación y busque la sección para agregar las URL de redireccionamiento.
2. Cuando encuentres el área adecuada, añade la siguiente AppFabric URL como URL de redireccionamiento a tu aplicación:

```
https://userportal.appfabric.<region>.amazonaws.com/eup_login
```

Tras añadir la URL, la aplicación se configurará para dirigir a los usuarios al portal AppFabric de usuarios. Aquí, los usuarios pueden iniciar sesión, conectarse y gestionar las aplicaciones que utilizan AppFabric para generar información sobre la productividad.

Paso 4. AppFabric Úselo para mostrar información y acciones entre aplicaciones

Una vez que los usuarios conecten sus aplicaciones, puedes aprovechar la información de tus usuarios para mejorar su productividad y reducir el cambio de contexto y aplicación. AppFabric solo genera información para un usuario en función de lo que el usuario tiene permiso para acceder. AppFabric almacena los datos del usuario en una Cuenta de AWS propiedad de AppFabric. Para obtener información sobre cómo AppFabric utiliza sus datos, consulteProcesamiento de datos.

Puede usar las siguientes API con tecnología de inteligencia artificial para generar y mostrar información y acciones a nivel de usuario en sus aplicaciones:

- `ListActionableInsights`: para obtener más información, consulte la sección Conocimientos prácticos a continuación.
- `ListMeetingInsights`: para obtener más información, consulte la sección de Preparación para la reunión más adelante en esta guía.

Conocimientos prácticos (**`ListActionableInsights`**)

La API `ListActionableInsights` ayuda a los usuarios a administrar mejor su día a día y obtener información útil basada en la actividad de sus aplicaciones, como el correo electrónico, el calendario, los mensajes, las tareas y mucho más. La información devuelta también mostrará enlaces insertados a los artefactos utilizados para generar la información, lo que ayudará a los usuarios a ver rápidamente qué datos se utilizaron para generar la información. Además, la API puede mostrar acciones sugeridas en función de la información y permitir a los usuarios ejecutar acciones entre aplicaciones desde su aplicación. En concreto, la API se integra con plataformas como Asana, Google Workspace, Microsoft 365 y Smartsheet para que los usuarios envíen correos electrónicos, creen eventos de calendario y tareas. Los modelos de lenguaje grande (LLM) pueden completar previamente los detalles de una acción recomendada (como el cuerpo del correo electrónico o el nombre de la tarea), que los usuarios pueden personalizar antes de ejecutarla, lo que simplifica la toma de decisiones y mejora la productividad. Al igual que ocurre con los usuarios finales al autorizar aplicaciones, AppFabric utiliza el mismo portal dedicado para que los usuarios vean, editen y ejecuten acciones entre aplicaciones. Para ejecutar acciones, AppFabric requiere que los ISV redirijan a los usuarios a un portal de AppFabric usuarios donde puedan ver los detalles de las acciones y ejecutarlas. Cada acción generada por AppFabric tiene una URL única. Esta URL está disponible en la respuesta a la respuesta de la API `ListActionableInsights`.

A continuación, se muestra un resumen de las acciones entre aplicaciones compatibles y en qué aplicaciones:

- Enviar correos electrónicos (Google Workspace, Microsoft 365)
- Crear un evento de calendario (Google Workspace, Microsoft 365)
- Crear tarea (Asana, Smartsheet)

Campos requeridos

- `nextToken` (opcional): el token de paginación para obtener el siguiente conjunto de información.

- `includeActionExecutionStatus`: un filtro que acepta una lista de estados de ejecución de acciones. Las acciones se filtran en función de los valores de estado transferidos. Los valores posibles son: `NOT_EXECUTED` | `EXECUTED`

Encabezado de la solicitud

- El encabezado de autorización debe pasarse junto con el valor `Bearer Token` .

Campos de respuesta

- `insightId`: el identificador único de la información generada.
- `insightContent`: esto devuelve un resumen de la información y enlaces integrados a los artefactos utilizados para generar la información. Nota: Se trataría de un contenido HTML que incluye enlaces integrados (**<a>** etiquetas).
- `insightTitle`: el título de la información generada.
- `createdAt`: cuándo se generó la información.
- `actions`: una lista de acciones recomendadas para la información generada. Objeto action:
  - `actionId`: el identificador único de la acción generada.
  - `actionIconUrl`: la URL del icono de la aplicación en la que se sugiere ejecutar la acción.
  - `actionTitle`: el título de la acción generada.
  - `actionUrl`- La URL única para que el usuario final vea y ejecute la acción en el portal AppFabric de usuarios. Nota: para ejecutar acciones, las aplicaciones ISV redirigirán a los usuarios al portal de AppFabric usuarios (pantalla emergente) utilizando esta URL.
  - `actionExecutionStatus`: una enumeración que indica el estado de la acción. Los valores posibles son: `EXECUTED` | `NOT_EXECUTED`
- `nextToken` (opcional): el token de paginación para obtener el siguiente conjunto de información. Es un campo opcional que, si se devuelve nulo, significa que no hay más información que cargar.

Para obtener más información, consulte ActionableInsights.

```
curl -v --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/actionableInsights" \
  --header "Authorization: Bearer <token>"
```

Si la acción se realiza correctamente, el servicio devuelve una respuesta 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
}
```

Preparación para la reunión (**`ListMeetingInsights`**)

La API `ListMeetingInsights` ayuda a los usuarios a prepararse mejor para las próximas reuniones al resumir el propósito de la reunión y mostrar artefactos pertinentes entre aplicaciones, como correos electrónicos, mensajes y más. Ahora los usuarios pueden prepararse rápidamente para las reuniones y no perder el tiempo al cambiar de una aplicación a otra para buscar contenido.

Campos requeridos

- `nextToken` (opcional): el token de paginación para obtener el siguiente conjunto de información.

Encabezado de la solicitud

- El encabezado de autorización debe pasarse junto con el valor `Bearer Token`.

Campos de respuesta

- `insightId`: el identificador único de la información generada.
- `insightContent`: la descripción de la información que destaca los detalles en formato de cadena. Por ejemplo, ¿por qué es importante esta información?
- `insightTitle`: el título de la información generada.
- `createdAt`: cuándo se generó la información.
- `calendarEvent`: el evento o reunión importante del calendario en el que el usuario debe centrarse. Objeto calendarEvent:
  - `startTime`: la hora de inicio del evento.
  - `endTime`: la hora de finalización del evento.
  - `eventUrl`: la URL del evento del calendario en la aplicación ISV.
- `resources`: la lista que contiene los demás recursos relacionados con la generación de información. Objetos de recursos:
  - `appName`: el nombre de la aplicación a la que pertenece el recurso.
  - `resourceTitle`: el título del recurso.
  - `resourceType`: el tipo del recurso. Los valores posibles son: `EMAIL` | `EVENT` | `MESSAGE` | `TASK`

  - `resourceUrl`: la URL del recurso en la aplicación.
  - `appIconUrl`: la URL de la imagen de la aplicación a la que pertenece el recurso.
- `nextToken` (opcional): el token de paginación para obtener el siguiente conjunto de información. Es un campo opcional que, si se devuelve nulo, significa que no hay más información que cargar.

Para obtener más información, consulte MeetingInsights.

```
curl --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/meetingContexts" \
  --header "Authorization: Bearer <token>"
```

Si la acción se realiza correctamente, el servicio devuelve una respuesta 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
}
```

Proporcione comentarios sobre sus información o acciones

Utilice la operación de la AppFabric `PutFeedback` API para proporcionar comentarios sobre la información y las acciones generadas. Puedes integrar esta función en tus aplicaciones para proporcionar una forma de enviar una valoración (del 1 al 5, donde cuanto más alta sea, mejor) para una InsightId o más ActionId.

Campos requeridos

- `id`: el identificador del objeto para el que se envían los comentarios. Puede ser el InsightId o el ActionId.
- `feedbackFor`: el tipo de recurso para el que se envían los comentarios. Valores posibles: `ACTIONABLE_INSIGHT` | `MEETING_INSIGHT` | `ACTION`
- `feedbackRating`: calificación de comentarios de 1 a 5. Cuanto más alta sea la calificación, mejor.

Campos de respuesta

- No hay campos de respuesta.

Para obtener más información, consulte 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 la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201 con un cuerpo HTTP vacío.

Paso 5. Solicitud AppFabric para verificar su solicitud

Hasta este punto, has actualizado la interfaz de usuario de la aplicación para incluir AppFabric información y acciones entre aplicaciones, y has recibido información para un solo usuario. Cuando estés satisfecho con las pruebas y desees extender tu experiencia AppFabric enriquecida a más usuarios, puedes enviar tu solicitud AppFabric para que la revisen y verifiquen. AppFabric verificará la información de la aplicación antes de permitir una adopción generalizada para ayudar a proteger a los desarrolladores de aplicaciones, los usuarios finales y sus datos, lo que allanará el camino para ampliar la adopción por parte de los usuarios de manera responsable.

Inicie el proceso de verificación

Comience el proceso de verificación al enviar un correo electrónico a appfabric-appverification@amazon.com y solicitar que se verifique su aplicación.

En el correo electrónico, incluya los siguientes detalles:

- Tu ID Cuenta de AWS
- El nombre de la aplicación para la que busca la verificación
- Tu AppClient DNI
- Información de contacto

Además, proporcione la siguiente información, si está disponible, para ayudarnos a evaluar la prioridad y el impacto:

- Número estimado de usuarios a los que piensa conceder acceso
- Su fecha de lanzamiento prevista

> **Note**
>
> Si tiene un Cuenta de AWS gerente o gerente de desarrollo de AWS socios, cópielo en su correo electrónico. Incluir estos contactos puede ayudar a agilizar el proceso de verificación.

Criterios de verificación

Antes de iniciar el proceso de verificación, asegúrese de que cumple los siguientes criterios:

- Debe utilizar un código válido Cuenta de AWS AppFabric para aumentar la productividad

Además, cumple al menos uno de estos criterios:

- Su organización es un AWS socio AWS Partner Network con al menos un nivel «AWS Select». Para obtener más información, consulte Niveles de servicios para socios de AWS.
- Su organización debería haber gastado al menos 10 000$ en AppFabric servicios en los últimos tres años.
- Su aplicación debería figurar en el AWS Marketplace. Para obtener más información, consulte AWS Marketplace.

Actualización del estado de verificación en espera

Tras revisar tu solicitud, te responderemos por correo electrónico y el estado de tu solicitud AppClient cambiará de `pending_verification` a `verified`. Si su aplicación es rechazada, tendrá que volver a iniciar el proceso de verificación.

Administrar AppFabric para aumentar la productividad AppClients

> La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Puede gestionar su productividad AppFabric AppClients para garantizar el buen funcionamiento y el mantenimiento de los procesos de autenticación y autorización.

Obtenga detalles de un AppClient

Utilice la operación de la AppFabric `GetAppClient` API para ver los detalles sobre su AppClient, incluida la verificación del AppClient estado. Para obtener más información, consulte GetAppClient.

Para obtener los detalles de una AppClient, debes tener, como mínimo, los permisos de la política de `"appfabric:GetAppClient"` IAM. Para obtener más información, consulte Permita el acceso para obtener detalles de AppClients.

Campos requeridos

- `appClientId`- El AppClient carné.

Campos de respuesta

- `appName`- El nombre de la aplicación que se mostrará a los usuarios en la página de consentimiento del portal de AppFabric usuarios.
- `customerManagedKeyIdentifier` (opcional): el ARN de la clave administrada por el cliente (generada por KMS) que se utilizará para cifrar los datos. Si no se especifica, se utilizará la clave AWS AppFabric gestionada.
- `description`: una descripción de la aplicación.
- `redirectUrls`: el URI al que se redirige a los usuarios finales después de la autorización. Puede agregar hasta 5 redirectUrls. Por ejemplo, `https://localhost:8080`.

- `starterUserEmails`: una dirección de correo electrónico de usuario a la que se permitirá acceder para recibir información hasta que se verifique la aplicación. Solo se permite una dirección de correo electrónico. Por ejemplo, `anyuser@example.com`.
- `verificationStatus`- El estado AppClient de la verificación.
  - `pending_verification`- La verificación del aún AppClient está en curso AppFabric. Hasta que AppClient se verifique, solo un usuario (especificado en`starterUserEmails`) puede usar el AppClient.
  - `verified`- El proceso de verificación se completó correctamente AppFabric y ahora AppClient está completamente verificado.
  - `rejected`- El proceso de verificación del AppClient fue rechazado por AppFabric. AppClient No lo pueden utilizar otros usuarios hasta que el proceso de verificación se reinicie y se complete correctamente.

```
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 la acción se realiza correctamente, el servicio devuelve una respuesta 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"
        }
    }
}
```

Lista AppClients

Usa la operación de la AppFabric `ListAppClients` API para ver una lista de tus AppClients. AppFabric solo permite uno AppClient por Cuenta de AWS. Este límite está sujeto a cambios en el futuro. Para obtener más información, consulte ListAppClients.

Para publicar AppClients, debes tener, como mínimo, los permisos de la política de `"appfabric:ListAppClients"` IAM. Para obtener más información, consulte Permitir el acceso a la lista AppClients.

Campos requeridos

- No hay campos obligatorios.

Campos de respuesta

- `appClientARN`- El nombre del recurso de Amazon (ARN) que incluye el AppClient ID. Por ejemplo, el AppClient ID es`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `verificationStatus`- El estado AppClient de la verificación.
  - `pending_verification`- La verificación del aún AppClient está en curso AppFabric. Hasta que AppClient se verifique, solo un usuario (especificado en`starterUserEmails`) puede usar el AppClient.
  - `verified`- El proceso de verificación se completó correctamente AppFabric y ahora AppClient está completamente verificado.
  - `rejected`- El proceso de verificación del AppClient fue rechazado por AppFabric. AppClient No lo pueden utilizar otros usuarios hasta que el proceso de verificación se reinicie y se complete correctamente.

```
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 la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

```
200 OK

{
    "appClientList": [
        {
            "appClientArn": "arn:aws:appfabric:<region>:111122223333:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "verificationStatus": "pending_verification"
        }
    ]
}
```

Actualice un AppClient

Utilice la operación de AppFabric `UpdateAppClient` API para actualizar las URL de redireccionamiento asignadas a su. AppClient Si necesita cambiar cualquier otro parámetro, por ejemplo, u otro starterUserEmails, debe eliminarlo AppClient y crear uno nuevo. AppName Para obtener más información, consulte UpdateAppClient.

Para actualizar un AppClient, debe tener, como mínimo, los permisos de la política de `"appfabric:UpdateAppClient"` IAM. Para obtener más información, consulte Permitir el acceso a la actualización AppClients.

Campos requeridos

- `appClientId`(obligatorio): el AppClient ID con el que vas a actualizar las URL del redireccionamiento.
- `redirectUrls` (obligatorio): la lista actualizada de las redirectUrls. Puede agregar hasta 5 redirectUrls.

Campos de respuesta

- `appName`- El nombre de la aplicación que se mostrará a los usuarios en la página de consentimiento del portal de usuarios. AppFabric

- `customerManagedKeyIdentifier` (opcional): el ARN de la clave administrada por el cliente (generada por KMS) que se utilizará para cifrar los datos. Si no se especifica, se utilizará la clave AWS AppFabric gestionada.
- `description`: una descripción de la aplicación.
- `redirectUrls`: el URI al que se redirige a los usuarios finales después de la autorización. Por ejemplo, `https://localhost:8080`.
- `starterUserEmails`: una dirección de correo electrónico de usuario a la que se permitirá acceder para recibir información hasta que se verifique la aplicación. Solo se permite una dirección de correo electrónico. Por ejemplo, `anyuser@example.com`.
- `verificationStatus`- El estado AppClient de la verificación.
  - `pending_verification`- La verificación del aún AppClient está en curso AppFabric. Hasta que AppClient se verifique, solo un usuario (especificado en`starterUserEmails`) puede usar el AppClient.
  - `verified`- El proceso de verificación se completó correctamente AppFabric y ahora AppClient está completamente verificado.
  - `rejected`- El proceso de verificación del AppClient fue rechazado por AppFabric. AppClient No lo pueden utilizar otros usuarios hasta que el proceso de verificación se reinicie y se complete correctamente.

```
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 la acción se realiza correctamente, el servicio devuelve una respuesta 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"
        }
    }
}
```

Eliminar un AppClient

Usa la operación de la AppFabric `DeleteAppClient` API para eliminar los que ya no AppClients necesites. Para obtener más información, consulte DeleteAppClient.

Para eliminar una AppClient, debes tener, como mínimo, los permisos de la política de `"appfabric:DeleteAppClient"` IAM. Para obtener más información, consulte Permitir el acceso para eliminar AppClients.

Campos requeridos

- `appClientId`- El AppClient identificador.

Campos de respuesta

- No hay campos de respuesta.

```
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 la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

Actualizar los tokens para los usuarios finales

Los tokens que AppClient adquieras para los usuarios finales se pueden actualizar al caducar. Esto se puede hacer mediante la API Token con el grant_type `refresh_token`. El `refresh_token` que se va a utilizar se devuelve como parte de la respuesta de la API del token cuando el grant_type es `authorization_code`. El máximo de caducidad predeterminado es de 12 horas. Para llamar a la API de actualización, debe tener el permiso de la política de IAM `"appfabric:Token"`. Para obtener más información, consulte Token y Permitir el acceso a la actualización AppClients.

Campos requeridos

- `refresh_token` (obligatorio): el token de actualización recibido de la solicitud inicial del `/token`.
- `app_client_id`(obligatorio): el ID del AppClient recurso creado para. Cuenta de AWS
- `grant_type` (obligatorio): debe ser `refresh_token`.

Campos de respuesta

- `expires_in`: cuánto falta para que caduque el token. El tiempo de caducidad predeterminado es de 12 horas.
- `refresh_token`: el token de actualización recibido de la solicitud /token inicial.
- `token`: el token recibido de la solicitud /token inicial.
- `token_type`: el valor será `Bearer`.
- `appfabric_user_id`- El AppFabric seudónimo. Se devuelve solo para las solicitudes que utilizan el tipo de concesión `authorization_code`.

```
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 la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

```
200 OK

{
    "expires_in": 43200,
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "${UserID}"
}
```

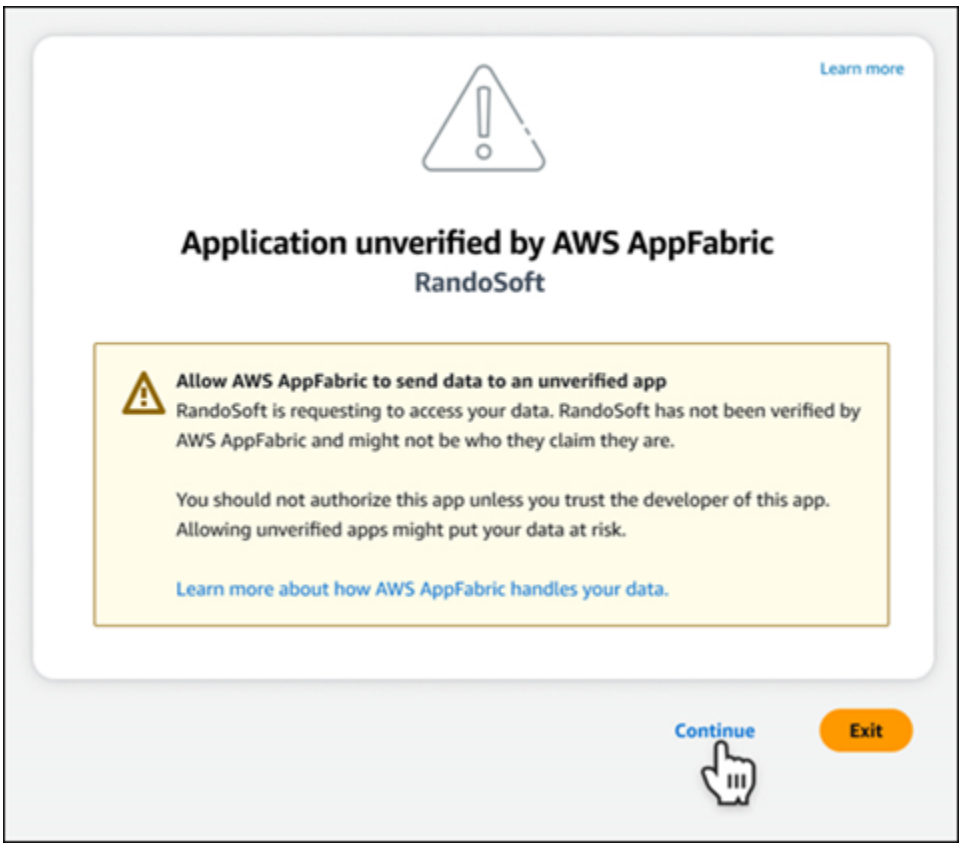
Resolución de problemas

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

En esta sección se describen los errores más comunes y la solución de AppFabric problemas relacionados con la productividad.

Aplicación sin verificar

Los desarrolladores de aplicaciones que utilizan la productividad AppFabric para enriquecer sus experiencias con las aplicaciones pasarán por un proceso de verificación antes de lanzar sus funciones a los usuarios finales. Todas las aplicaciones comienzan como no verificadas y cambian a verificadas solo cuando se completa el proceso de verificación. Esto significa que la que `starterUserEmails` utilizaste al crear una AppClient verá este mensaje.



Errores de **`CreateAppClient`**

ServiceQuotaExceededException

Si recibes la siguiente excepción al crear una AppClient, significa que has superado el número de ellas AppClients que se pueden crear por cada una Cuenta de AWS. El límite es 1. Código de estado 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
```

Errores de **`GetAppClient`**

ResourceNotFoundException

Si recibes la siguiente excepción al obtener los detalles de una AppClient, asegúrate de haber introducido el AppClient identificador correcto. Este error significa que no AppClient se ha encontrado el especificado.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Errores de **`DeleteAppClient`**

ConflictException

Si recibes la siguiente excepción al eliminar una AppClient, significa que hay otra solicitud de eliminación en curso. Espere a que se complete e inténtelo de nuevo. Código de estado HTTP: 409

```
ConflictException
Another delete request is in progress. Wait until it completes then try again.
HTTP Status Code: 409
```

ResourceNotFoundException

Si recibes la siguiente excepción al eliminar una AppClient, asegúrate de haber introducido el AppClient identificador correcto. Este error significa que no AppClient se ha encontrado el especificado.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Errores de **`UpdateAppClient`**

ResourceNotFoundException

Si recibes la siguiente excepción al actualizar una AppClient, asegúrate de haber introducido el AppClient identificador correcto. Este error significa que no se ha encontrado AppClient lo especificado.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Errores de **`Authorize`**

ValidationException

Es posible que reciba la siguiente excepción si alguno de los parámetros de la API no cumple las restricciones definidas en las especificaciones de la API.

```
ValidationException
HTTP Status Code: 400
```

Motivo 1: cuando no se especifica el AppClient ID

Falta `app_client_id` en los parámetros de la solicitud. Crea el AppClient si aún no se ha creado o usa el existente `app_client_id` e inténtalo de nuevo. Para encontrar el AppClient ID, usa la operación ListAppClientde API.

Motivo 2: ¿Cuándo AppFabric no tiene acceso a la clave gestionada por el cliente

```
Message: AppFabric couldn't access the customer managed key configured for AppClient.
```

AppFabric actualmente no puede acceder a las claves gestionadas por el cliente, probablemente debido a cambios recientes en sus permisos. Compruebe que la clave especificada existe y asegúrese de que AppFabric se le concedan los permisos de acceso adecuados.

Motivo 3: la URL de redireccionamiento especificada no es válida

```
Message: Redirect url invalid
```

Asegúrese de que la URL de redireccionamiento de su solicitud sea correcta. Debe coincidir con una de las URL de redireccionamiento especificadas al crear o actualizar la AppClient. Para ver la lista de direcciones URL de redireccionamiento permitidas, utilice la operación de GetAppClientAPI.

Errores de **`Token`**

TokenException

Puede que reciba la siguiente excepción por los siguientes motivos.

```
TokenException
```

```
HTTP Status Code: 400
```

Motivo 1: cuando se especifica un correo electrónico que no es válido

```
Message: Invalid Email used
```

Asegúrese de que la dirección de correo electrónico que utiliza coincide con la que aparece para el `starterUserEmails` atributo cuando creó el AppClient. Si los correos electrónicos no coinciden, cambie a la dirección de correo electrónico coincidente e inténtelo de nuevo. Para ver el correo electrónico utilizado, usa la operación de GetAppClientAPI.

Motivo 2: para grant_type como refresh_token cuando no se especifica el token.

```
Message: refresh_token must be non-null for Refresh Token Grant-type
```

El token de actualización especificado en la solicitud es nulo o está vacío. Especifique un `refresh_token` activo recibido en la respuesta a la llamada a la API Token.

ThrottlingException

Es posible que reciba la siguiente excepción si se llama a la API en una tasa superior a la cuota permitida.

```
ThrottlingException
HTTP Status Code: 429
```

Errores de **`ListActionableInsights`**, **`ListMeetingInsights`** y **`PutFeedback`**

ValidationException

Es posible que reciba la siguiente excepción si alguno de los parámetros de la API no cumple la restricción definida en las especificaciones de la API.

```
ValidationException
HTTP Status Code: 400
```

ThrottlingException

Es posible que reciba la siguiente excepción si se llama a la API en una tasa superior a la cuota permitida.

```
ThrottlingException
HTTP Status Code: 429
```

Introducción a la AppFabric productividad (vista previa) para los usuarios finales

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Esta sección está destinada a los usuarios finales de aplicaciones SaaS que desean habilitar la productividad (vista previa) AWS AppFabric para mejorar la administración de tareas y la eficiencia del flujo de trabajo. Sigue estos pasos para conectar tus aplicaciones y autorizarte AppFabric a obtener información sobre todas las aplicaciones y ayudarte a realizar acciones (como enviar un correo electrónico o programar una reunión) desde tus aplicaciones preferidas. Puede conectar aplicaciones como Asana, Atlassian Jira Suite, Google Workspace, Microsoft 365, Miro, Slack, Smartsheet y más. Una vez que autorices el acceso AppFabric a tu contenido, AppFabric incorpora información y acciones entre aplicaciones directamente a tus aplicaciones preferidas, lo que te ayuda a trabajar de forma más eficiente y a mantenerte dentro de tus flujos de trabajo actuales.

AppFabric para la productividad utiliza IA generativa impulsada por Amazon Bedrock. AppFabric generará información y acciones solo después de recibir su permiso explícito. Autorizas a cada aplicación individual a mantener el control total del contenido que se utiliza. AppFabric no utilizará sus datos para entrenar o mejorar los grandes modelos lingüísticos subyacentes que se utilizan para generar información. Para obtener más información, consulte las preguntas frecuentes de Amazon Bedrock.

Temas

- Requisitos previos
- Paso 1. Inicie sesión en AppFabric
- Paso 2. Otorgue su consentimiento para que la aplicación muestre información
- Paso 3. Conecte sus aplicaciones para generar información y acciones
- Paso 4. Comience a ver información valiosa y ejecute acciones entre aplicaciones en su aplicación
- Atención, administradores de TI y seguridad: administración del acceso a AppFabric las funciones de productividad (versión preliminar)
- Resolución de problemas

Requisitos previos

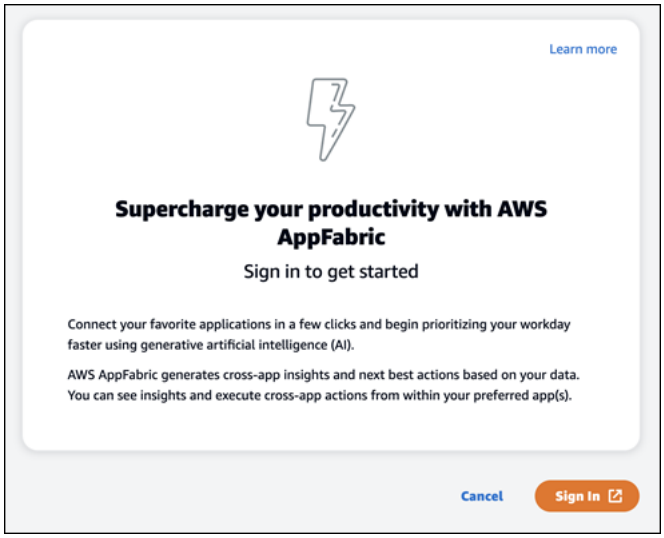
Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Credenciales para iniciar sesión AppFabric: AppFabric para empezar a utilizarlas con fines de productividad, necesitará credenciales de inicio de sesión federadas (nombre de usuario y contraseña) de uno de los siguientes proveedores:Asana, Google WorkspaceMicrosoft 365, o. Slack Iniciar sesión nos AppFabric ayuda a identificarte como usuario en cada aplicación que utilices AppFabric para aumentar tu productividad. Tras iniciar sesión, puede conectar sus aplicaciones para empezar a generar información.
- Credenciales para conectar sus aplicaciones: la información y las acciones entre aplicaciones solo se generan en función de las aplicaciones que usted autorice. Necesitará credenciales de inicio de sesión (nombre de usuario y contraseña) para cada una de las aplicaciones que desee autorizar. Las aplicaciones compatibles incluyen Asana, Atlassian Jira Suite, Google Workspace, Microsoft 365, Miro, Slack y Smartsheet.

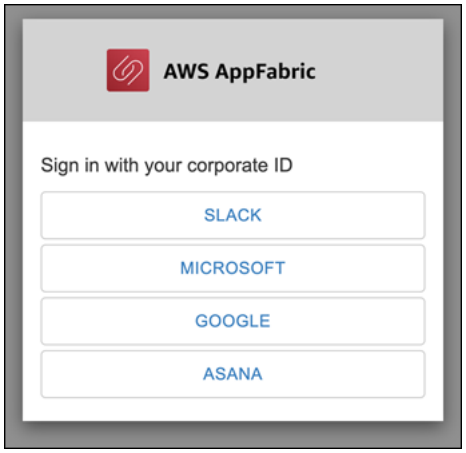
Paso 1. Inicie sesión en AppFabric

Conecte las aplicaciones AppFabric para llevar su contenido e información directamente a sus aplicaciones preferidas.

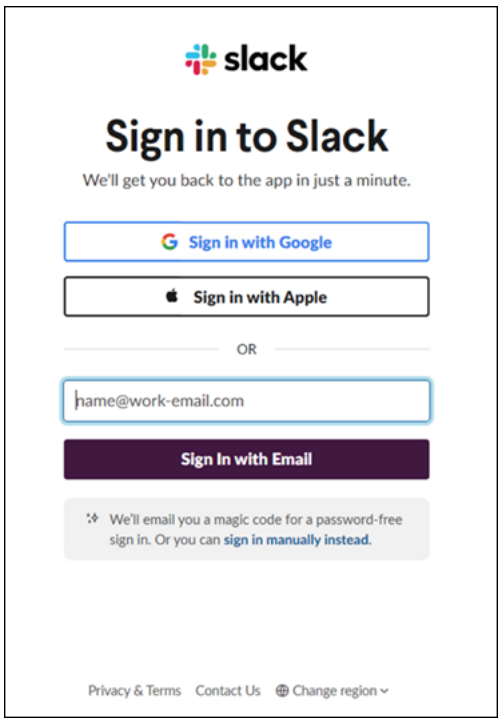
1. Cada aplicación se utilizará AppFabric para aumentar la productividad de diferentes maneras para ofrecerte experiencias de aplicación más enriquecedoras. Debido a esto, cada aplicación tendrá un punto de entrada diferente para acceder a la AppFabric página principal de productividad que aparece a continuación. La página de inicio establece el contexto del proceso que se va a activar AppFabric y, en primer lugar, te pide que inicies sesión. Todas las aplicaciones que desees activar AppFabric llegarán a esta pantalla.

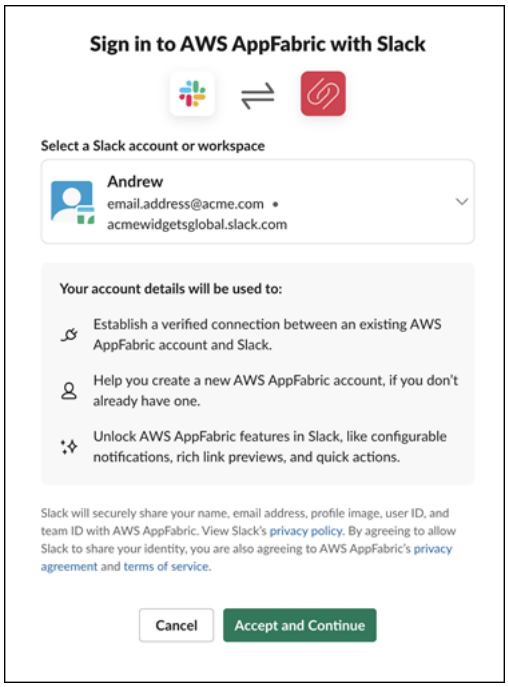


2. Inicie sesión con las credenciales de uno de estos proveedores: Asana, Google Workspace, Microsoft 365, o Slack. Para disfrutar de la mejor experiencia, te recomendamos iniciar sesión con el mismo proveedor para cada aplicación que AppFabric actives. Por ejemplo, si elige las credenciales de Google Workspace en la Aplicación 1, le recomendamos que elija Google Workspace en la Aplicación 2 y cada vez que necesite volver a iniciar sesión. Si inicia sesión con otro proveedor, tendrá que reiniciar el proceso de conexión de las aplicaciones.



3. Si se te solicita, introduce tus credenciales de inicio de sesión y acepta iniciar sesión AppFabric desde este proveedor.

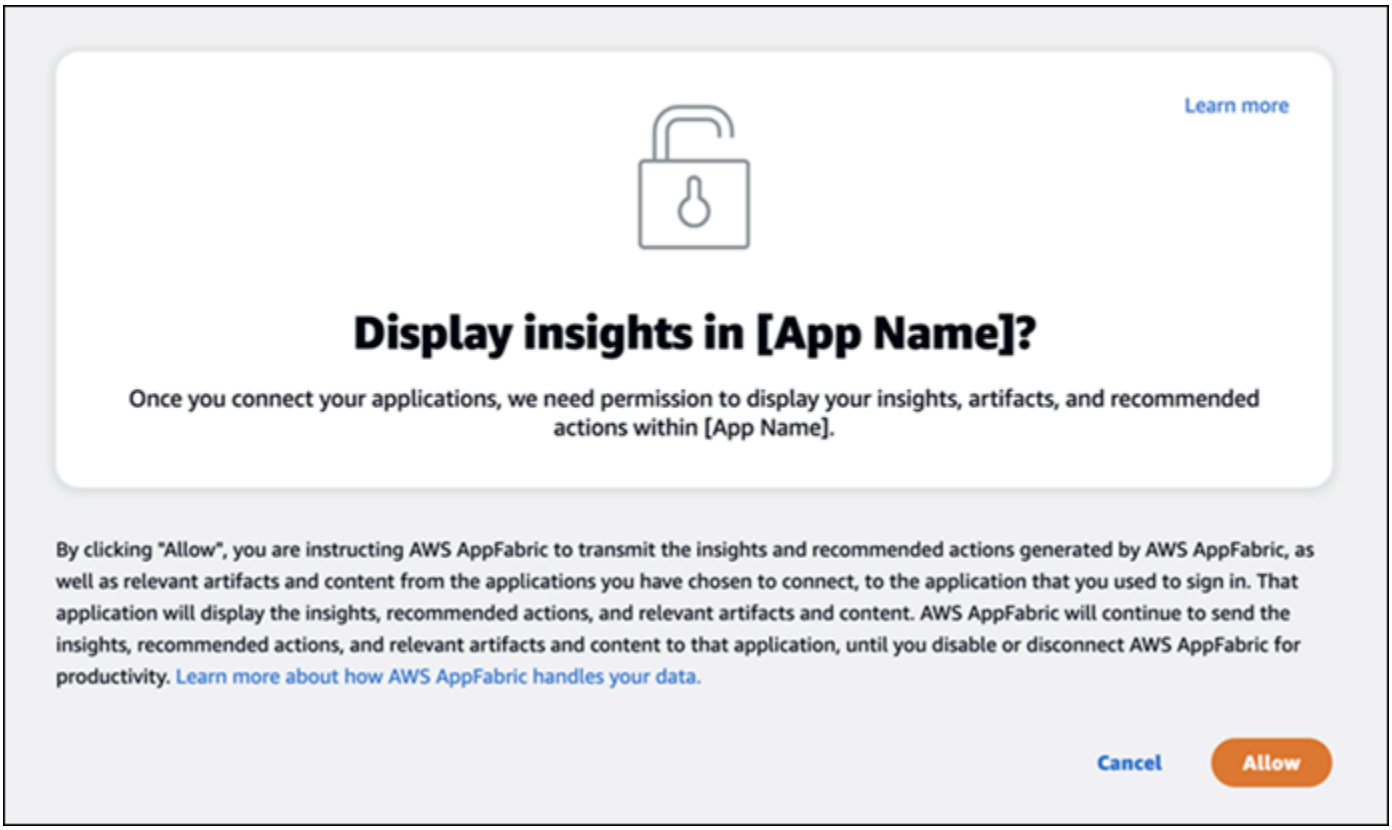




Paso 2. Otorgue su consentimiento para que la aplicación muestre información

Tras iniciar sesión, AppFabric aparecerá una página de consentimiento en la que se te preguntará si permites AppFabric mostrar información y acciones entre aplicaciones dentro de la aplicación en la que estás fomentando la productividad. AppFabric Por ejemplo, ¿permites AppFabric tomar tus

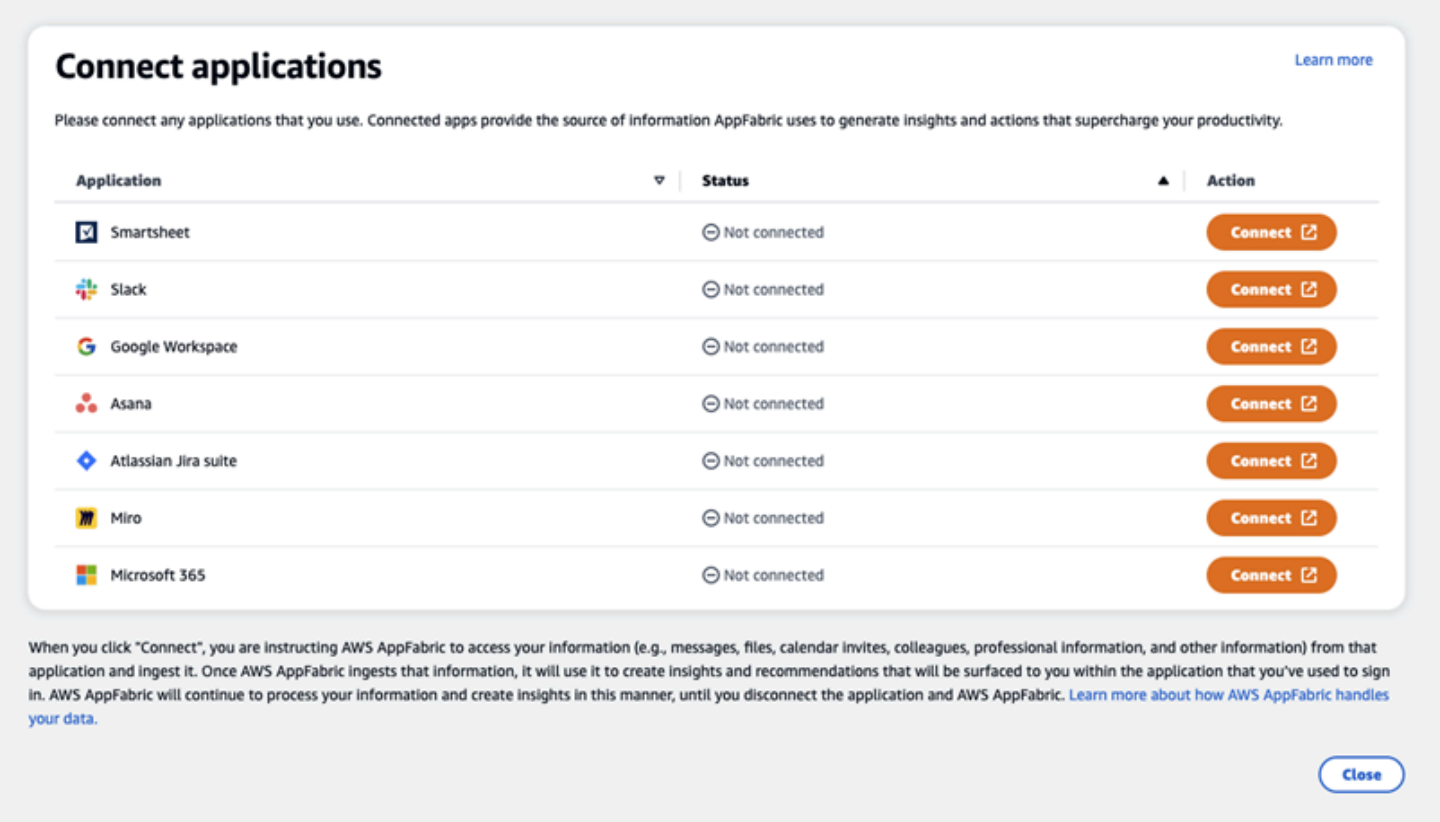
Google Workspace correos electrónicos y eventos del calendario y mostrarlos? Asana Solo tienes que completar este paso de consentimiento una vez por cada aplicación que AppFabric habilites.



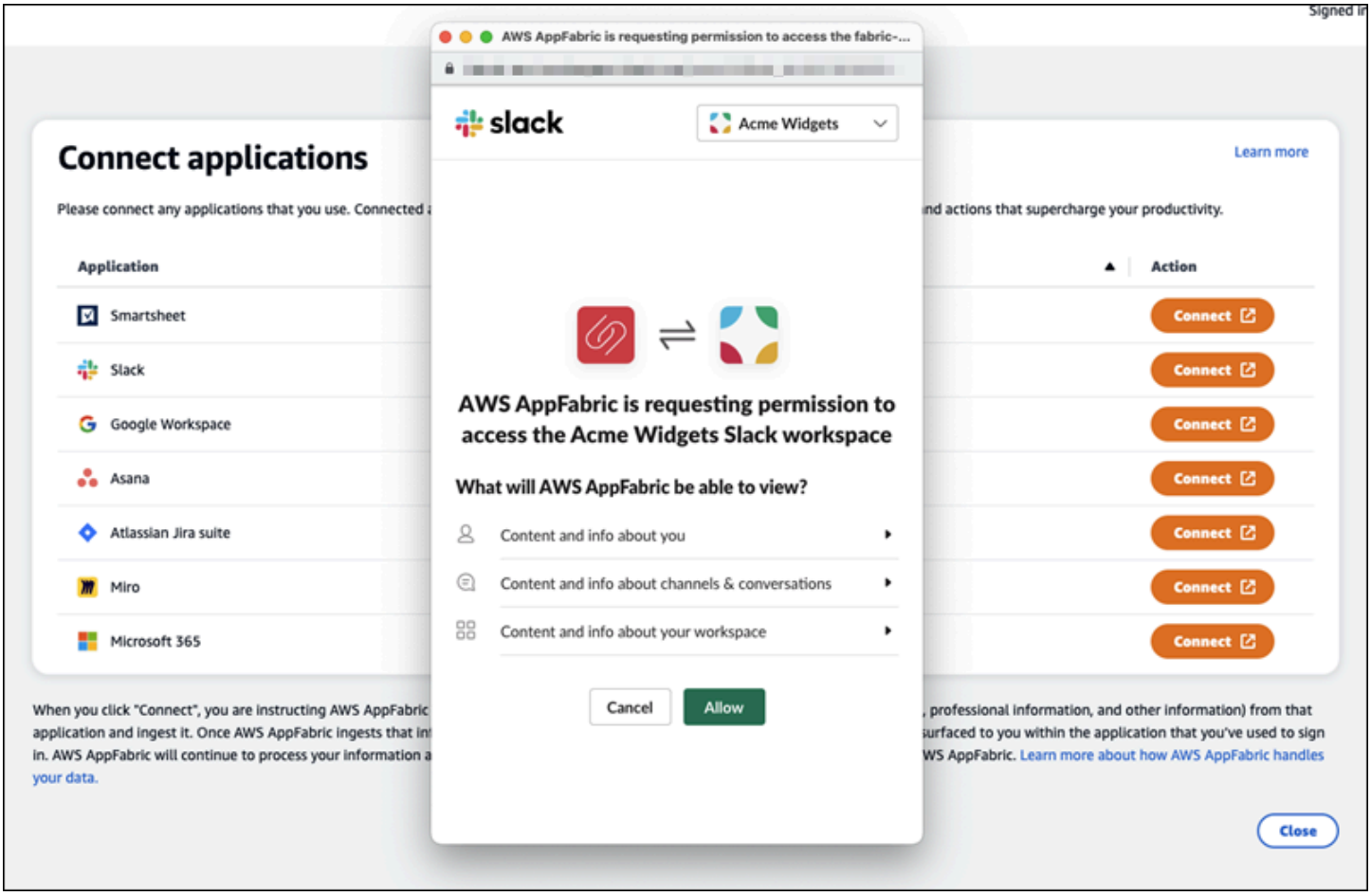
Paso 3. Conecte sus aplicaciones para generar información y acciones

Tras completar la página de consentimiento, accederá a la página Conectar aplicaciones, donde podrá conectar, desconectar o volver a conectar aplicaciones individuales que se utilizarán para generar información y acciones entre aplicaciones. En la mayoría de los casos, después de iniciar sesión y dar su consentimiento, se seguirá utilizando esta página para administrar las aplicaciones conectadas.

Para conectar una aplicación, pulse el botón Conectar situado junto a cualquier aplicación que utilice.



Deberás proporcionar tus credenciales de inicio de sesión en la solicitud y conceder AppFabric permiso para acceder a tus datos a fin de generar información y completar acciones.

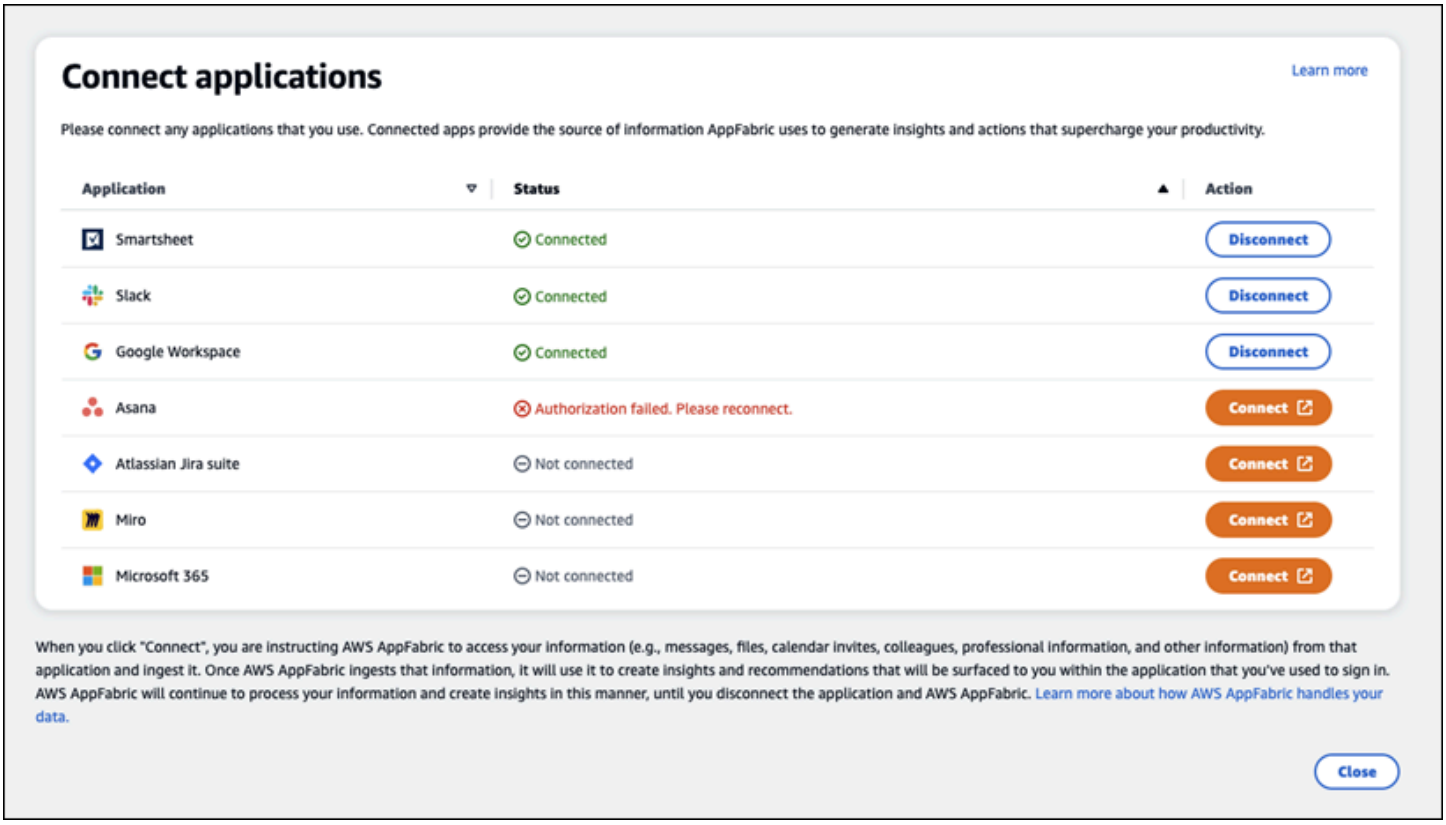


Una vez que haya conectado correctamente una aplicación, el estado de esa aplicación cambiará de “No conectada” a “Conectada”. Recordatorio: Debe completar este paso de autorización para cada solicitud que desee que se utilice para generar información y acciones.

Una vez que conecta una aplicación, esta no está conectada para siempre. Debe volver a conectar las aplicaciones periódicamente. Lo hacemos para asegurarnos de que aún contamos con su permiso para generar información.

Los posibles estados de la aplicación son:

- Conectado: AppFabric está autorizado y genera información con los datos de esta aplicación.
- No está conectado: AppFabric no genera información con los datos de esta aplicación. Puede conectarse para empezar a generar información.
- Error de autorización. Vuelva a conectar. - Es posible que se haya producido un error de autorización en una aplicación específica. Si le aparece este error, intente reconectar la aplicación y usar el botón Conectar.



La configuración ha finalizado y ya puede volver a la aplicación. Empezar a ver información valiosa en sus aplicaciones puede tardar al menos unas horas.

Si es necesario, puede volver a esta página para administrar las aplicaciones conectadas. Si decide desconectar una aplicación, AppFabric dejará de usar los datos de esa aplicación o de recopilar nuevos datos para generar nueva información. Los datos de las aplicaciones desconectadas se eliminarán automáticamente en un plazo de 7 días si decide no volver a conectar la aplicación en ese momento.

Paso 4. Comience a ver información valiosa y ejecute acciones entre aplicaciones en su aplicación

Una vez que conectes tus aplicaciones AppFabric, tendrás acceso a información valiosa y podrás realizar acciones entre aplicaciones directamente desde la aplicación que prefieras. Nota: esta funcionalidad no está garantizada en todas las aplicaciones y depende totalmente de las funciones AppFabric de productividad que el desarrollador de la aplicación haya decidido habilitar.

Información entre aplicaciones

AppFabric for productivity ofrece dos tipos de información:

- Información útil: AppFabric analiza la información de los correos electrónicos, los eventos del calendario, las tareas y los mensajes de las aplicaciones conectadas y genera información clave que puede ser importante priorizar. Además, AppFabric puede generar acciones recomendadas (como enviar correos electrónicos, programar una reunión y crear una tarea) que puede editar y ejecutar sin dejar de utilizar la aplicación que prefiera. Por ejemplo, puede recibir información que indique que hay un aumento del número de clientes que abordar y que se le sugiera una próxima acción para programar una reunión con su cliente.
- Información sobre la preparación de las reuniones: esta característica le ayuda a prepararse mejor para las próximas reuniones. AppFabric analizará tus próximas reuniones y generará un resumen conciso sobre el propósito de la reunión. Además, mostrará artefactos pertinentes (como correos electrónicos, mensajes y tareas) de las aplicaciones conectadas que le ayudarán a preparar la reunión de manera eficiente sin tener que cambiar de aplicación para buscar contenido.

Acciones entre aplicaciones

Para obtener información específica, también AppFabric puede generar acciones recomendadas, como enviar un correo electrónico, programar una reunión o crear una tarea. Al generar acciones, AppFabric puede rellenar previamente determinados campos en función del contenido y el contexto de las aplicaciones conectadas. Por ejemplo, AppFabric puede generar una sugerencia de respuesta por correo electrónico o un nombre de tarea en función de la información. Al hacer clic en una acción sugerida, accederás a una interfaz de AppFabric usuario propia donde podrás editar el contenido rellenado previamente antes de ejecutar la acción. AppFabric no ejecutará acciones sin la previa revisión y entrada de los usuarios, ya que la IA generativa y los grandes modelos lingüísticos (LLM) subyacentes pueden tener alucinaciones de vez en cuando.

> **Note**
>
> Usted tiene la responsabilidad de validar y confirmar los resultados del AppFabric LLM. AppFabric no garantiza la precisión o la calidad de sus salidas de LLM. Para obtener más información, consulte Política de IA responsable de AWS.

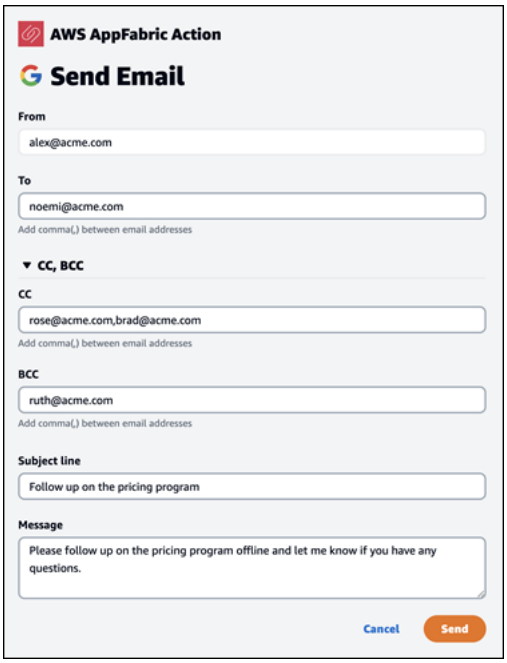
Crear correos electrónicos (Google Workspace, Microsoft 365)

AppFabric le permite editar y enviar un correo electrónico desde la aplicación que prefiera. Admitimos campos de correo electrónico básicos, como los campos de origen, destino, cc/bcc, asunto del correo electrónico y cuerpo del mensaje. AppFabric puede generar contenido en estos campos para

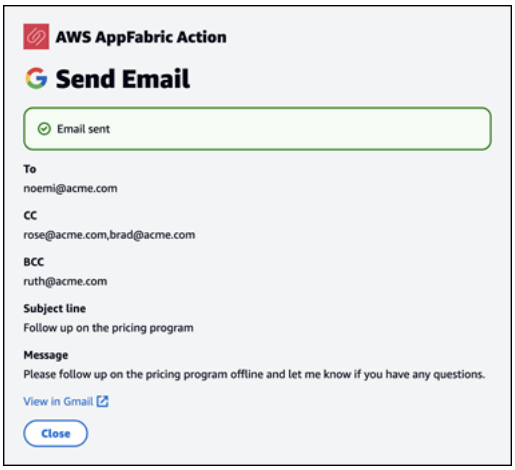
ayudarle a reducir el tiempo necesario para completar la tarea. Cuando haya terminado de editar el correo electrónico, elija Enviar para enviar el correo electrónico.

Los siguientes campos son obligatorios para enviar un correo electrónico:

- Se requiere al menos uno de los correos electrónicos del destinatario (Para, CC y CCO) y debe ser una dirección de correo electrónico válida.
- Campos de asunto y mensaje.



Una vez enviado el correo electrónico, verás una confirmación de que se ha enviado el correo electrónico. Además, verás un enlace para ver el correo electrónico en la aplicación designada. Puede usar este enlace para navegar rápidamente a la aplicación y verificar que se ha enviado el correo electrónico.

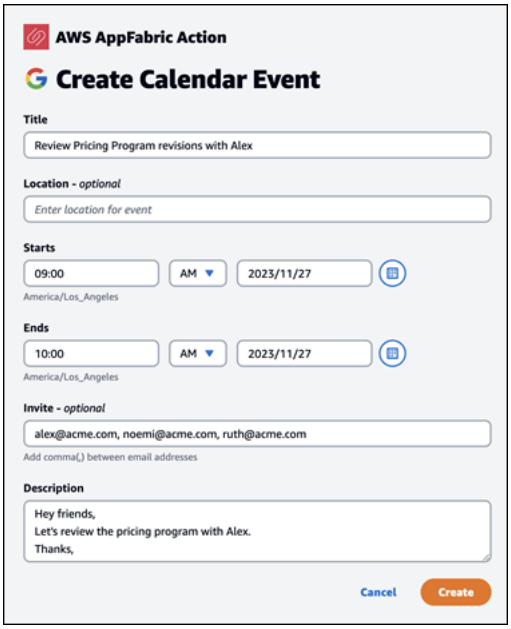


Crear eventos de calendario (Google Workspace, Microsoft 365)

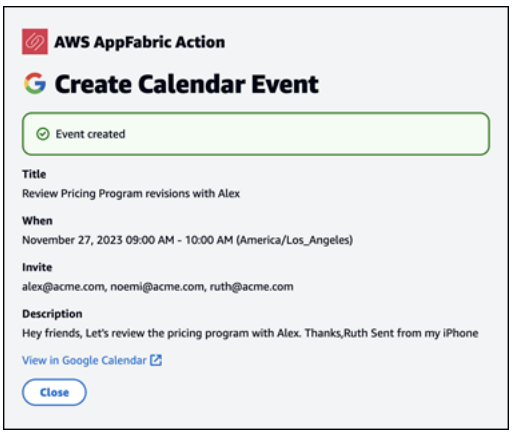
AppFabric le permite editar y crear un calendario de eventos desde la aplicación que prefiera. Admitimos campos básicos de eventos del calendario, como el título del evento, la ubicación, la fecha y hora de inicio y finalización, la lista de invitados y los detalles del evento. AppFabric puede generar contenido en estos campos para ayudarte a reducir el tiempo necesario para completar la tarea. Cuando haya terminado de editar el evento del calendario, elija Crear para crear el evento.

Los siguientes campos son obligatorios para crear un evento de calendario:

- Campos de título, inicio, fin y descripción.
- La hora y la fecha de inicio no deben ser anteriores a la hora y fecha de finalización.
- El campo de invitación es opcional, pero requiere direcciones de correo electrónico válidas si se completa el campo.



Después de enviar el evento del calendario, verá una confirmación de que el evento se ha creado. Además, verá un enlace para ver el evento en la aplicación designada. Puede usar este enlace para navegar rápidamente a la aplicación y verificar que se creó el evento.

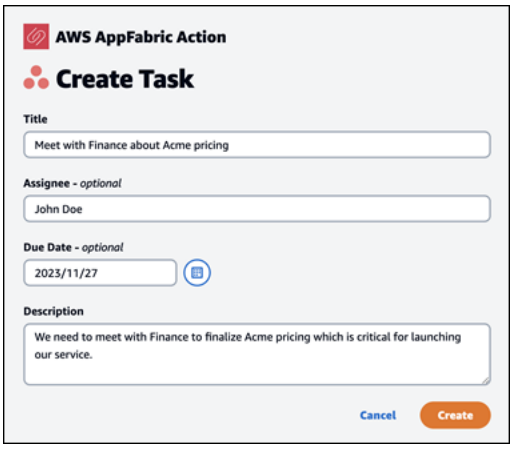


Crear tareas (Asana)

AppFabric le permite editar y crear una tarea Asana desde la aplicación que prefiera. Admitimos campos de tareas básicos como el nombre de la tarea, el propietario de la tarea, la fecha de vencimiento y la descripción de la tarea. AppFabric puede generar contenido en estos campos para ayudarte a reducir el tiempo necesario para crear la tarea. Cuando haya terminado de editar la tarea, elija Crear para crearla. Las tareas se crean en el espacio de trabajo de Asana, proyecto o tarea correspondiente, según lo sugerido por el LLM.

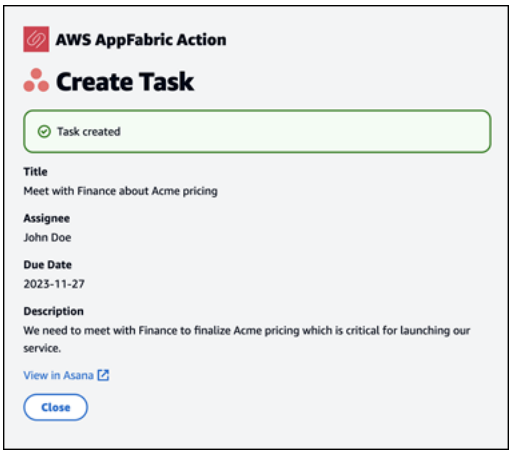
Los siguientes campos son obligatorios para crear una tarea de Asana:

- Campos de título y descripción.
- El remitente debe ser una dirección de correo electrónico válida si se modifica.



Una vez creada la tarea, verá una confirmación de que la tarea se creó en Asana Además, verá un enlace para ver la tarea en Asana. Puede usar este enlace para ir rápidamente a la aplicación y

comprobar que la tarea se ha creado, o moverla al espacio de trabajo de Asana, proyecto o tarea adecuados.

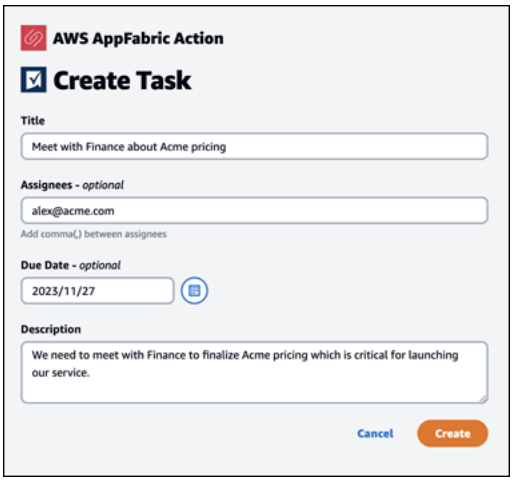


Crear tareas (Smartsheet)

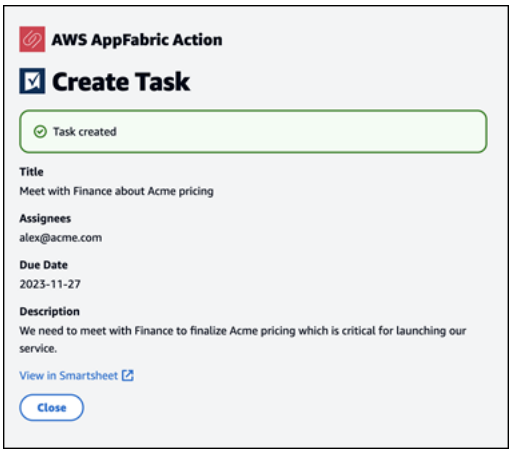
AppFabric le permite editar y crear una tarea Smartsheet desde la aplicación que prefiera. Admitimos campos de tareas básicos como el nombre de la tarea, el propietario de la tarea, la fecha de vencimiento y la descripción de la tarea. AppFabric puede generar contenido en estos campos para ayudarte a reducir el tiempo necesario para crear la tarea. Cuando haya terminado de editar la tarea, elija Crear para crearla. En el caso de Smartsheet las tareas, AppFabric creará una nueva Smartsheet hoja privada y rellenará las tareas creadas. Esto se hace para ayudar a centralizar las acciones AppFabric generadas en un solo lugar de forma estructurada.

Los siguientes campos son obligatorios para crear una tarea de Smartsheet:

- Campos de título y descripción.
- Si se completa el campo, el remitente debe ser una dirección de correo electrónico válida.



Una vez creada la tarea, verá una confirmación de que la tarea se creó en Smartsheet Además, verá un enlace para ver la tarea en Smartsheet. Puede usar este enlace para navegar rápidamente a la aplicación y ver la tarea en la hoja de Smartsheet creada. Todas las futuras tareas de Smartsheet se completarán en esta hoja. Si se borra la hoja, AppFabric se creará una nueva.



Atención, administradores de TI y seguridad: administración del acceso a AppFabric las funciones de productividad (versión preliminar)

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

El portal AppFabric para usuarios de productividad es de acceso público para todos los usuarios de aplicaciones SaaS que se hayan integrado con funciones AppFabric de productividad (vista previa). Si es un administrador de TI que desea administrar el acceso a estas características de la IA generativa en su organización, considere estas opciones:

- Restringir el inicio de sesión del proveedor de identidad (IdP): puede bloquear el acceso de inicio de sesión a través de su proveedor de identidad para controlar el acceso de los usuarios a las características de la IA generativa.
- Deshabilitar OAuth para aplicaciones específicas: implemente restricciones descendentes al deshabilitar OAuth. Esta acción impide que los usuarios conecten las aplicaciones que requieren la autenticación de OAuth al espacio de trabajo de la empresa.

Resolución de problemas

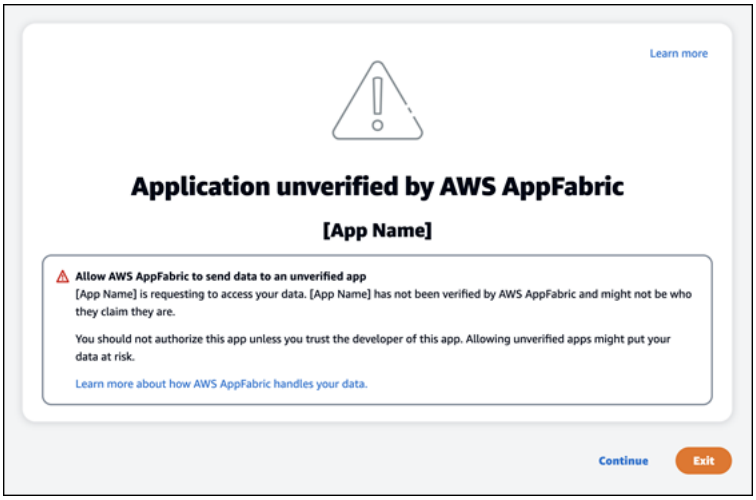
La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

En esta sección se describen los errores más comunes y la solución de AppFabric problemas relacionados con la productividad.

Aplicación sin verificar

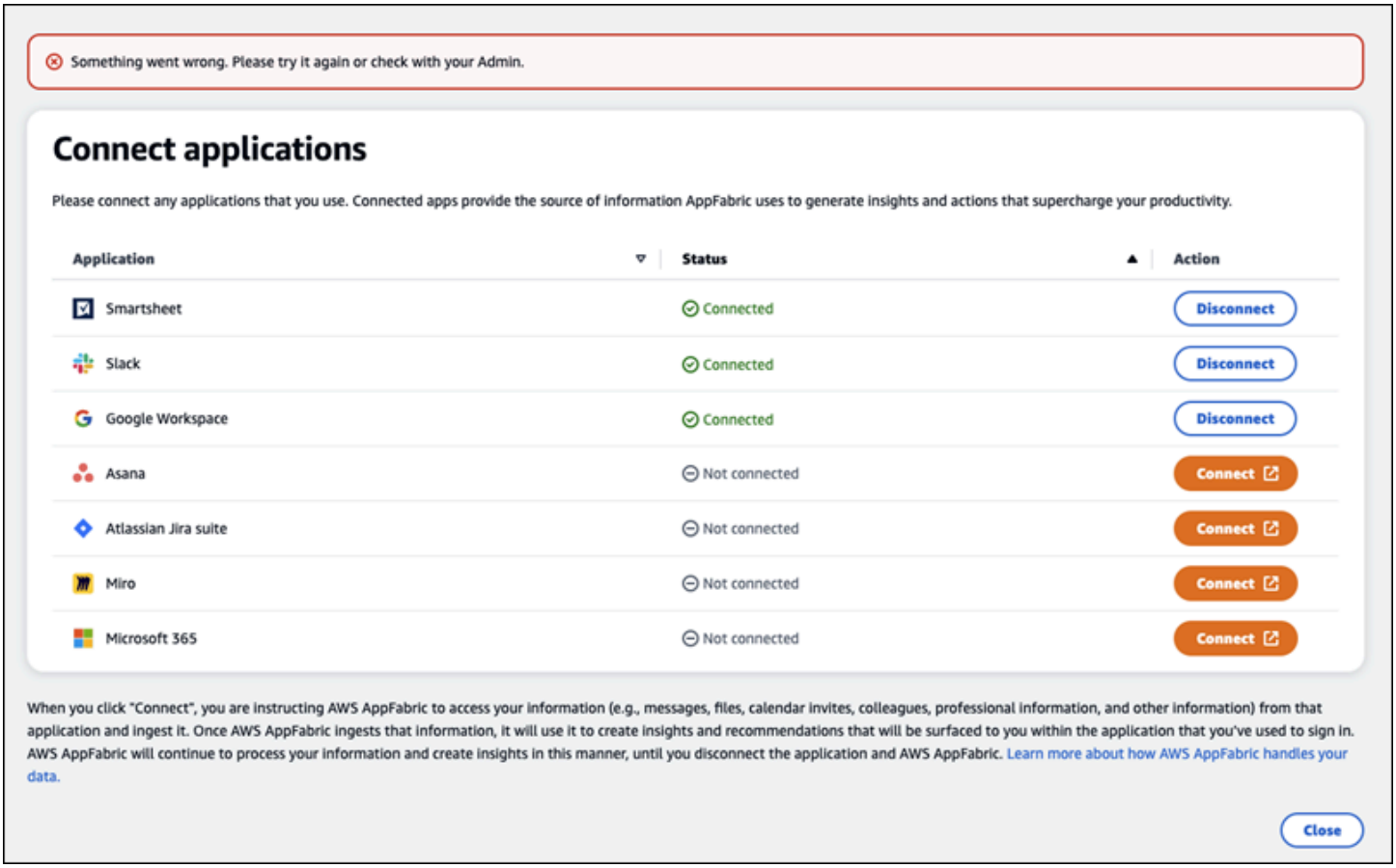
Las aplicaciones que utilizan la productividad AppFabric para enriquecer su experiencia con las aplicaciones se someterán a un proceso de verificación antes de lanzar sus funciones a los usuarios finales. Si al intentar iniciar sesión aparece un mensaje que indica que la aplicación no está verificada AppFabric, significa que la aplicación no se ha sometido a un proceso AppFabric de verificación que confirme la identidad del desarrollador de la aplicación y la precisión de la información de registro de la aplicación. Todas las aplicaciones comienzan como no verificadas y cambian a verificadas solo cuando se completa el proceso de verificación.

Tenga cuidado al utilizar una aplicación no verificada. Si no está seguro de los desarrolladores de la aplicación, puede esperar a que la aplicación obtenga el estado de verificación antes de continuar.



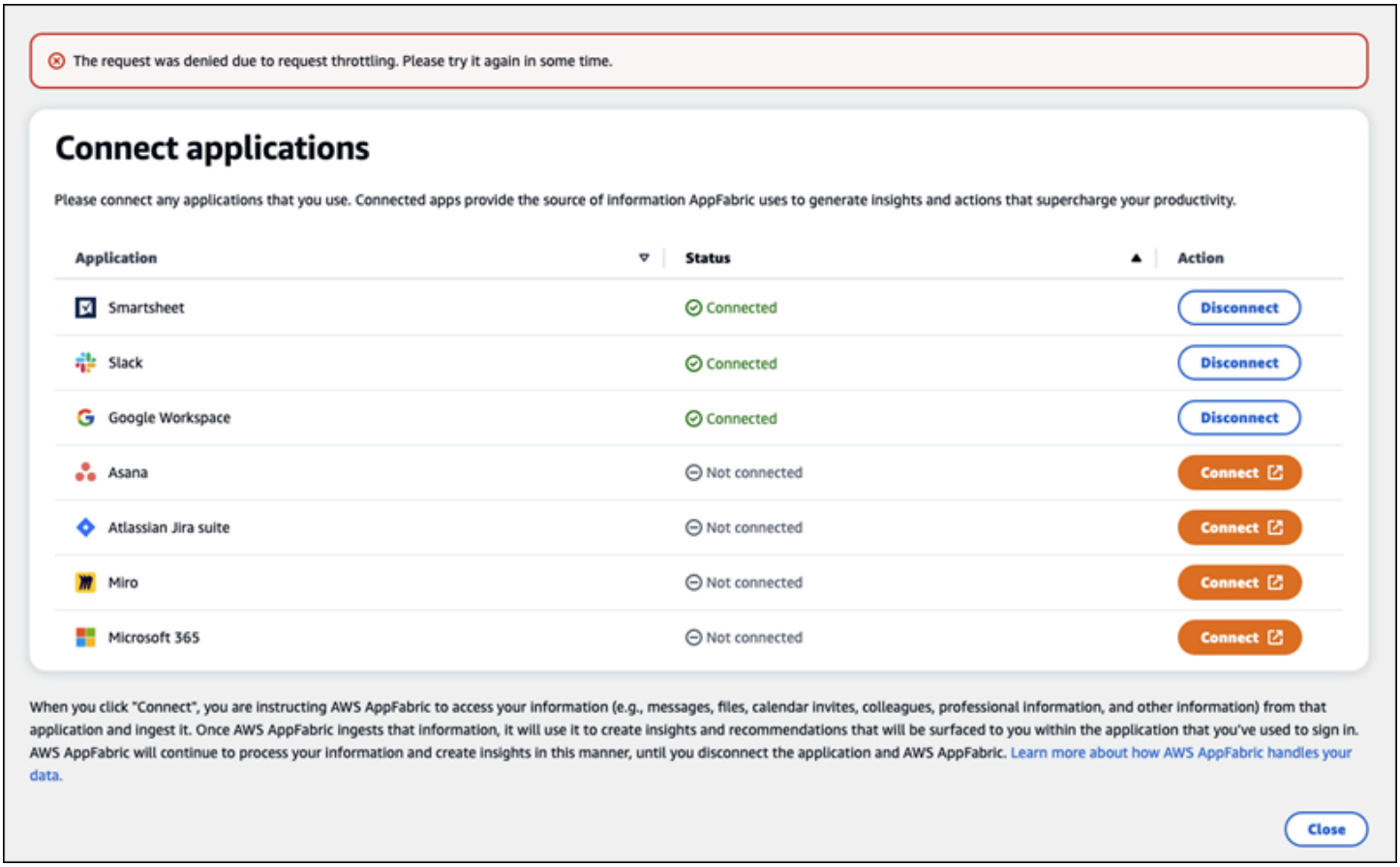
Algo ha salido mal. Inténtelo de nuevo o póngase en contacto con su administrador (**`InternalServerException`**)

Es posible que recibas este mensaje cuando el portal de AppFabric usuario no muestre la lista de aplicaciones o desconecte una aplicación debido a un error, una excepción o una falla desconocidos. Inténtelo de nuevo más tarde.



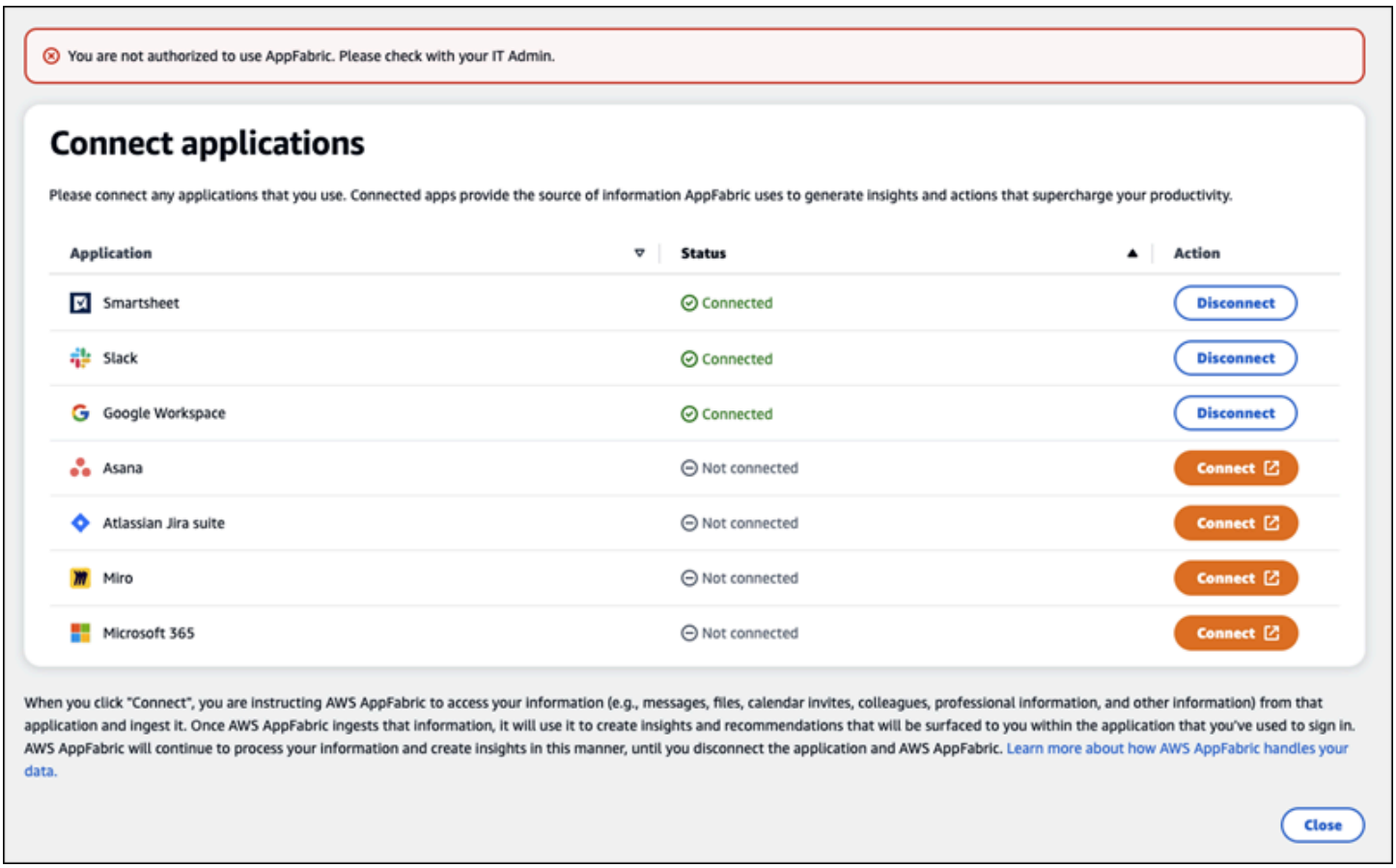
La solicitud fue denegada debido a una limitación de la solicitud. Vuelva a intentarlo más tarde (**`ThrottlingException`**)

Es posible que reciba este mensaje cuando el portal de AppFabric usuario no muestre las aplicaciones o desconecte una aplicación debido a un problema de limitación. Inténtelo de nuevo más tarde.



No está autorizado a utilizarlas. AppFabric AppFabric Vuelva a iniciar sesión (**`AccessDeniedException`**)

Es posible que reciba este mensaje cuando el portal de AppFabric usuario no muestre las aplicaciones o desconecte una aplicación debido a una excepción de acceso denegado. AppFabric Vuelva a iniciar sesión.



AppFabric API de productividad

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Esta sección proporciona las operaciones de la API, los tipos de datos y los errores comunes de las funciones de AWS AppFabric productividad.

> **Note**
>
> Para ver el resto de AppFabric las API, consulta la referencia AWS AppFabric de las API.

Temas

- Acciones
- Tipos de datos
- Errores comunes

Acciones

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Las funciones de AppFabric productividad admiten las siguientes acciones.

Para ver el resto de las acciones de la AppFabric API, consulta las Acciones AWS AppFabric de la API.

Temas

- Autorizar
- CreateAppClient
- DeleteAppClient
- GetAppClient
- ListActionableInsights
- ListAppClients
- ListMeetingInsights
- PutFeedback
- Token
- UpdateAppClient

Autorizar

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Autoriza un AppClient.

Temas

- Cuerpo de la solicitud

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Parámetro	Descripción
app_client_id	El ID del que se va AppClient a autorizar.
redirect_uri	El URI al que se redirige a los usuarios finales tras la autorizac ión.
state	Un valor único para mantener el estado entre la solicitud y la devolución de llamada.

CreateAppClient

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Crea un AppClient.

Temas

- Cuerpo de la solicitud
- Elementos de respuesta

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Parámetro	Descripción
appName	El nombre de la aplicación. Tipo: string Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 255 caracteres. Obligatorio: sí
clientToken	Especifique un identificador único, sensible a mayúsculas y minúsculas, para garantizar la idempotencia de la solicitud.

Parámetro	Descripción
	Esto le permite volver a intentar la solicitud de forma segura sin realizar accidentalmente la misma operación por segunda vez. Pasar el mismo valor a una llamada posterior a una operación requiere que también se pase el mismo valor para todos los demás parámetros. Se recomienda utilizar un tipo de valor UUID. Si no proporciona este valor, AWS generará uno aleatorio para usted. Si se vuelve a intentar la operación con el mismo `ClientToken`, pero con diferentes parámetros, se produce un error de `IdempotentParameterMismatch`. Tipo: String Patrón: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatorio: no

Parámetro	Descripción
customerManagedKeyIdentificador	El ARN del clave administrada por el cliente generado por. AWS Key Management Service La clave se utiliza para cifrar datos. Si no se especifica ninguna clave, se Clave administrada de AWS utiliza una. Un mapa de los pares clave-valor para la etiqueta o etiquetas asignadas al recurso. Para obtener más información sobre Claves propiedad de AWS las claves administradas por el cliente, consulte Claves y AWS claves del cliente en la Guía para AWS Key Management Service desarrolladores. Tipo: string Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 1011. Patrón: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatorio: no
description	Una descripción de la aplicación. Tipo: cadena Obligatorio: sí
iconUrl	La URL del icono o logotipo del AppClient. Tipo: cadena Requerido: no

Parámetro	Descripción
redirectUrls	El URI al que se redirige a los usuarios finales tras la autorización. Puede agregar hasta 5 redirectUrls. Por ejemplo, `https://localhost:8080` . Tipo: matriz de cadenas Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos. Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 2048 caracteres. Patrón: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` Obligatorio: sí
starterUserEmails	Las direcciones de correo electrónico iniciales de los usuarios a los que se les permite acceder para recibir información hasta que AppClient se verifique. Tipo: matriz de cadenas Miembros de la matriz: número fijo de 1 elemento. Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 320. Patrón: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Obligatorio: sí

Parámetro	Descripción
etiquetas	Un mapa de los pares clave-valor para la etiqueta o etiquetas asignadas al recurso. Tipo: matriz de objetos de etiqueta Miembros de la matriz: número mínimo de 0 artículos. Número máximo de 50 artículos. Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201.

El servicio devuelve los datos siguientes en formato JSON.

Parámetro	Descripción
appClientSummary	Contiene un resumen de AppClient. Tipo: objeto AppClientSummary

DeleteAppClient

La función AWS AppFabric de productividad está en vista previa y está sujeta a cambios.

Elimina un cliente de aplicación.

Temas

- Cuerpo de la solicitud
- Elementos de respuesta

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Parámetro	Descripción
appClientIdentifier	El nombre del recurso de Amazon (ARN) o el identificador único universal (UUID) que se utilizará en AppClient la solicitud. Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 1011. Patrón: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 204 con un cuerpo HTTP vacío.

GetAppClient

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Devuelve información sobre un AppClient.

Temas

- Cuerpo de la solicitud
- Elementos de respuesta

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Parámetro	Descripción
appClientIdentifier	El nombre del recurso de Amazon (ARN) o el identificador único universal (UUID) que se utilizará en AppClient la solicitud.

Parámetro	Descripción
	Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 1011. Patrón: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatorio: sí

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Parámetro	Descripción
appClient	Contiene información sobre un. AppClient Tipo: objeto AppClient

ListActionableInsights

> La función AWS AppFabric de productividad está en vista previa y está sujeta a cambios.

Enumera los mensajes de correo electrónico, las tareas y otras actualizaciones más importantes y procesables.

Temas

- Cuerpo de la solicitud
- Elementos de respuesta

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Parámetro	Descripción
nextToken	Si se obtiene `nextToken` , hay más resultados disponibles. El valor de `nextToken` es un token de paginación único para cada página. Vuelva a realizar la llamada con el token devuelto para recuperar la página siguiente. Conserve todos los demás argumentos sin cambios. Cada token de paginación caduca tras 24 horas. El uso de un token de paginación caducado devolverá un InvalidToken error HTTP 400.

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201.

El servicio devuelve los datos siguientes en formato JSON.

Parámetro	Descripción
ActionableInsightsList	Enumera la información procesable, incluidos el título, la descripción, las acciones y la marca temporal creada. Para obtener más información, consulte ActionableInsights.
nextToken	Si se obtiene `nextToken` , hay más resultados disponibles. El valor de `nextToken` es un token de paginación único para cada página. Vuelva a realizar la llamada con el token devuelto para recuperar la página siguiente. Conserve todos los demás argumentos sin cambios. Cada token de paginación caduca tras 24 horas. El uso de un token de paginación caducado devolverá un error HTTP 400 InvalidToken . Tipo: cadena

ListAppClients

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Devuelve una lista de todos AppClients.

Temas

- Cuerpo de la solicitud
- Elementos de respuesta

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Parámetro	Descripción
maxResults	El número máximo de resultados que se van a devolver por llamada. Se puede utilizar `nextToken` para obtener más páginas de resultados. Este es solo un límite superior. El número real de resultados devueltos por llamada puede ser inferior al máximo especific ado. Rango válido: valor mínimo de 1. Valor máximo de 100.
nextToken	Si se obtiene `nextToken` , hay más resultados disponibles. El valor de `nextToken` es un token de paginación único para cada página. Vuelva a realizar la llamada con el token devuelto para recuperar la página siguiente. Conserve todos los demás argumentos sin cambios. Cada token de paginación caduca tras 24 horas. El uso de un token de paginación caducado devolverá un InvalidToken error HTTP 400.

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Parámetro	Descripción
appClientList	Contiene una lista de AppClient resultados. Tipo: matriz de objetos AppClientSummary
nextToken	Si se obtiene `nextToken` , hay más resultados disponibles. El valor de `nextToken` es un token de paginación único para cada página. Vuelva a realizar la llamada con el token devuelto para recuperar la página siguiente. Conserve todos los demás argumentos sin cambios. Cada token de paginación caduca tras 24 horas. El uso de un token de paginación caducado devolverá un InvalidToken error HTTP 400. Tipo: cadena

ListMeetingInsights

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Enumera los eventos del calendario más importantes y procesables.

Temas

- Cuerpo de la solicitud
- Elementos de respuesta

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Parámetro	Descripción
nextToken	Si se obtiene `nextToken` , hay más resultados disponibles. El valor de `nextToken` es un token de paginación único para cada página. Vuelva a realizar la llamada con el token devuelto para recuperar la página siguiente. Conserve todos los demás

Parámetro	Descripción
	argumentos sin cambios. Cada token de paginación caduca tras 24 horas. El uso de un token de paginación caducado devolverá un InvalidToken error HTTP 400.

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201.

El servicio devuelve los datos siguientes en formato JSON.

Parámetro	Descripción
MeetingInsightList	Enumera la información procesable sobre las reuniones. Para obtener más información, consulte MeetingInsights.
nextToken	Si se obtiene `nextToken` , hay más resultados disponibles. El valor de `nextToken` es un token de paginación único para cada página. Vuelva a realizar la llamada con el token devuelto para recuperar la página siguiente. Conserve todos los demás argumentos sin cambios. Cada token de paginación caduca tras 24 horas. El uso de un token de paginación caducado devolverá un error HTTP 400 InvalidToken . Tipo: cadena

PutFeedback

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Permite a los usuarios enviar comentarios sobre una idea o acción determinada.

Temas

- Cuerpo de la solicitud
- Elementos de respuesta

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Parámetro	Descripción
id	El ID del objeto para el que se envían los comentarios. Puede ser el InsightId o el ActionId.
feedbackFor	El tipo de información para la que se envían los comentarios. Valores posibles: `ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION`
feedbackRating	Calificación de los comentarios de 1 a 5. Cuanto más alta sea la calificación, mejor.

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 201 con un cuerpo HTTP vacío.

Token

> La función AWS AppFabric de productividad está en vista previa y está sujeta a cambios.

Contiene información que permite AppClients intercambiar un código de autorización por un token de acceso.

Temas

- Cuerpo de la solicitud
- Elementos de respuesta

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Parámetro	Descripción
Código	El código de autorización recibido del punto de conexión de autorización. Tipo: string Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 2048 caracteres. Obligatorio: no
grant_type	El tipo de concesión del token. Debe ser `authorization_code` o `refresh_token` . Tipo: cadena Obligatorio: sí
app_client_id	El ID de la AppClient. Tipo: String Patrón: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatorio: sí
redirect_uri	El URI de redirección proporcionado al punto de conexión. Tipo: cadena Requerido: no
refresh_token	El token de actualización recibido de la solicitud de token inicial. Tipo: string Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 4096 caracteres.

Parámetro	Descripción
	Obligatorio: no

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Parámetro	Descripción
appfabric_user_id	Identificación del usuario para el token. Se devuelve solo para las solicitudes que utilizan el tipo de concesión `authorization_code` . Tipo: cadena
expires_in	El número de segundos hasta que vence el token. Tipo: largo
refresh_token	El token de actualización que se utilizará en una solicitud posterior. Tipo: string Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 2048 caracteres.
token	El token de acceso. Tipo: string Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 2048 caracteres.
token_type	El tipo de token. Tipo: cadena

UpdateAppClient

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Actualiza un AppClient.

Temas

- Cuerpo de la solicitud
- Elementos de respuesta

Cuerpo de la solicitud

La solicitud acepta los siguientes datos en formato JSON.

Parámetro	Descripción
appClientIdentifier	El nombre del recurso de Amazon (ARN) o el identificador único universal (UUID) que se utilizará en AppClient la solicitud. Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 1011. Patrón: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatorio: sí
redirectUrls	El URI al que se redirige a los usuarios finales tras la autorización. Puede agregar hasta 5 redirectUrls. Por ejemplo, `https://localhost:8080` . Tipo: matriz de cadenas Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos. Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 2048 caracteres.

Parámetro	Descripción
	Patrón: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

Elementos de respuesta

Si la acción se realiza correctamente, el servicio devuelve una respuesta HTTP 200.

El servicio devuelve los datos siguientes en formato JSON.

Parámetro	Descripción
appClient	Contiene información sobre un. AppClient Tipo: objeto AppClient

Tipos de datos

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

La AppFabric API contiene varios tipos de datos que utilizan diversas acciones. En esta sección se describen en detalle los tipos de datos de las funciones de AppFabric productividad.

Para ver todos los demás tipos de datos de la AppFabric API, consulte los tipos de datos de la AWS AppFabric API.

> **Important**
>
> No se garantiza el orden de cada elemento en una estructura de tipo de datos. Las aplicaciones no deben adoptar un orden determinado.

Temas

- ActionableInsights
- AppClient
- AppClientSummary

- MeetingInsights
- VerificationDetails

ActionableInsights

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Contiene un resumen de las acciones importantes y adecuadas para un usuario que se basa en los correos electrónicos, las invitaciones del calendario, los mensajes y las tareas de su cartera de aplicaciones. Los usuarios pueden ver información proactiva de todas sus aplicaciones para ayudarles a orientar mejor su jornada. Estas ideas justifican por qué un usuario debería preocuparse por el resumen de la información, junto con referencias, como los enlaces integrados, a aplicaciones individuales y artefactos que generaron la información.

Parámetro	Descripción
insightId	El identificador único de la información generada.
insightContent	Esto devuelve un resumen de la información y enlaces integrados a los artefactos utilizados para generar la información. Sería un contenido HTML que contiene enlaces incrustados (<a> etiquetas).
insightTitle	El título de la información generada.
createdAt	Cuándo se generó la información.
actions	Una lista de acciones recomendadas para la información generada. El objeto de acción contiene los siguientes parámetros: • `actionId`: el identificador único de la acción generada. • `actionIconUrl` : la URL del icono de la aplicación en la que se sugiere ejecutar la acción. • `actionTitle` : el título de la acción generada.

Parámetro	Descripción
	• `actionUrl` — La URL única para que el usuario final vea y ejecute la acción en el portal AppFabric de usuarios. Para ejecutar acciones, las aplicaciones ISV redirigirán a los usuarios al portal de AppFabric usuarios (pantalla emergente) mediante esta URL. • `actionExecutionStatus` : una enumeración que indica el estado de la acción. Los valores posibles son: `EXECUTED | NOT_EXECUTED`

AppClient

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Contiene información sobre un AppClient.

Parámetro	Descripción
appName	Nombre de la aplicación. Tipo: cadena Obligatorio: sí
arn	El nombre del recurso de Amazon (ARN) del. AppClient Tipo: string Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 1011. Patrón: `arn:.+` Obligatorio: sí

Parámetro	Descripción
description	Una descripción de la aplicación. Tipo: cadena Obligatorio: sí
iconUrl	La URL del icono o logotipo del AppClient. Tipo: cadena Requerido: no
redirectUrls	Las direcciones URL de redireccionamiento permitidas para. AppClient Tipo: matriz de cadenas Miembros de la matriz: número mínimo de 1 elemento. La cantidad máxima es de 5 artículos. Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 2048 caracteres. Patrón: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` Obligatorio: sí

Parámetro	Descripción
starterUserEmails	Las direcciones de correo electrónico iniciales de los usuarios a los que se les permite acceder para recibir información hasta que AppClient se verifique. Tipo: matriz de cadenas Miembros de la matriz: número fijo de 1 elemento. Limitaciones de longitud: longitud mínima de 0. Longitud máxima de 320. Patrón: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Obligatorio: sí
verificationDetails	Contiene el estado y el motivo de la AppClient verificación. Tipo: objeto VerificationDetails Obligatorio: sí
customerManagedKeyArn	El nombre del recurso de Amazon (ARN) del clave administrada por el cliente generado por AWS Key Management Service para el. AppClient Tipo: string Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 1011. Patrón: `arn:.+` Obligatorio: no

Parámetro	Descripción
appClientId	El ID de la AppClient. Diseñado para usarse en los flujos de autenticación automática para el cliente de la aplicación. Tipo: String Patrón: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatorio: no

AppClientSummary

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Contiene información sobre un AppClient.

Parámetro	Descripción
arn	El nombre del recurso de Amazon (ARN) del. AppClient Tipo: string Limitaciones de longitud: longitud mínima de 1. Longitud máxima de 1011. Patrón: `arn:.+` Obligatorio: sí
verificationStatus	El estado AppClient de verificación. Tipo: cadena Valores válidos: `pending_verification | verified | rejected`

Parámetro	Descripción
	Obligatorio: sí
appClientId	El ID de la AppClient. Diseñado para usarse en los flujos de autenticación automática para el cliente de la aplicación. Tipo: String Patrón: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obligatorio: no

MeetingInsights

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Contiene un resumen de las tres reuniones principales junto con el propósito de la reunión, los artefactos relacionados entre aplicaciones y las actividades de las tareas, los correos electrónicos, los mensajes y los eventos del calendario.

Parámetro	Descripción
insightId	El identificador único de la información generada.
insightContent	La descripción de la información que resalta los detalles en formato de cadena. Por ejemplo, ¿por qué es importante esta información?
insightTitle	El título de la información generada.
createdAt	Cuándo se generó la información.
calendarEvent	El evento o reunión importante del calendario en el que el usuario debe centrarse. Objeto calendarEvent:

Parámetro	Descripción
	• `startTime` : la hora de inicio del evento. • `endTime`: la hora de finalización del evento. • `eventUrl`: la URL del evento del calendario en la aplicación ISV.
resources	La lista que contiene los demás recursos relacionados con la generación de información. Objetos de recursos: • `appName`: el nombre de la aplicación a la que pertenece el recurso. • `resourceTitle` : el título del recurso. • `resourceType` : el tipo del recurso. Los valores posibles son: `EMAIL | EVENT | MESSAGE | TASK` • `resourceUrl` : la URL del recurso de la aplicación. • `appIconUrl` : la URL de la imagen de la aplicación a la que pertenece el recurso.
nextToken	El token de paginación para obtener el siguiente conjunto de información. Es un campo opcional que, si se devuelve nulo, significa que no hay más información que cargar.

VerificationDetails

La función AWS AppFabric de productividad está en vista previa y está sujeta a cambios.

Contiene el estado y el motivo de la AppClient verificación.

Parámetro	Descripción
verificationStatus	El estado AppClient de la verificación.

Parámetro	Descripción
	Tipo: cadena Valores válidos: `pending_verification | verified | rejected` Obligatorio: sí
statusReason	El motivo del estado de la AppClient verificación. Tipo: string Limitaciones de longitud: longitud mínima de 1. La longitud máxima es de 1024 caracteres. Obligatorio: no

Errores comunes

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

En esta sección se enumeran los errores comunes a las acciones de la API para las funciones de AWS AppFabric productividad.

Para ver todos los demás errores AppFabric comunes de la API, consulta Resolución de problemas los errores comunes de la AWS AppFabric API en la Referencia de la AWS AppFabric API.

Nombre de excepción	Descripción
TokenException	La solicitud de token no es válida. Código de estado HTTP: 400

Procesamiento de datos

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

AppFabric toma medidas para almacenar el contenido de los usuarios de forma individual, en un bucket de Amazon S3 gestionado por y por separado AppFabric, lo que ayuda a garantizar que generamos información específica sobre los usuarios. Utilizamos medidas de seguridad razonables para proteger su contenido, que pueden incluir el cifrado en reposo y en tránsito. Hemos configurado nuestros sistemas para eliminar automáticamente el contenido de los clientes en un plazo de 30 días a partir de su ingesta. AppFabric no genera información a partir de artefactos de datos a los que el usuario ya no tiene acceso. Por ejemplo, cuando un usuario desconecta una fuente de datos (una aplicación), AppFabric deja de recopilar datos de esa aplicación y no utiliza ningún artefacto persistente de las aplicaciones desconectadas para generar información. AppFabricLos sistemas están configurados para eliminar dichos datos en un plazo de 30 días.

AppFabric no utiliza el contenido de los usuarios para capacitar o mejorar los grandes modelos lingüísticos subyacentes que se utilizan para generar información. Para obtener más información sobre AppFabric la función de IA generativa, consulte las preguntas frecuentes de Amazon Bedrock.

Cifrado en reposo

AWS AppFabric admite el cifrado en reposo, una función de cifrado del lado del servidor que cifra de AppFabric forma transparente todos los datos relacionados con los usuarios cuando se conservan en el disco y los descifra cuando se accede a los datos.

Cifrado en tránsito

AppFabric protege todo el contenido en tránsito mediante TLS 1.2 y firma las solicitudes de servicios a la API con la versión 4 de Signature. AWS AWS

Terminología y conceptos

En este tema se describen la terminología y los conceptos clave AWS AppFabric para ayudarle a empezar.

Agrupación de aplicaciones

Un paquete de AppFabric aplicaciones almacena todas las autorizaciones e ingestas de AppFabric aplicaciones (consulta la siguiente definición de ingestión). Puedes crear un paquete de aplicaciones por cada uno. Cuenta de AWS Región de AWS

AppClient (también cliente de aplicación y cliente de aplicación)

Un OAuth AppClient para la aplicación receptora de datos. Cada aplicación receptora de datos debe registrarse y acceder AppClient AppFabric a los datos. Un usuario desarrollador necesita una AWS cuenta para registrarse AppClient. Cada AWS cuenta solo puede registrar una AppClient. AppFabric venderá los tokens de acceso en función de AppClient. AppClient contendrá información sobre la aplicación receptora de datos que accederá a AppFabric los datos a través de ella. AppClient

Autorización de la aplicación

La autorización de una aplicación otorga AppFabric permiso para conectarse e interactuar con sus aplicaciones. Permite ingerir los registros de auditoría de sus aplicaciones con credenciales OAuth (autorización abierta: un estándar abierto que permite delegar el acceso a las aplicaciones) o mediante credenciales de token de acceso personal (PAT). Puede configurar múltiples autorizaciones de aplicaciones (hasta 50) por agrupación de aplicaciones. Esto AppFabric permite incorporar los registros de auditoría de varios inquilinos de aplicaciones, repitiendo el paso de creación de la autorización de la aplicación según sea necesario para cada inquilino de la aplicación. Las credenciales que se comparten se cifran con una Clave propiedad de AWS o una clave gestionada por el cliente de AWS Key Management Service (AWS KMS) y se almacenan en AppFabric.

Ingesta

Una AppFabric ingestión utiliza la autorización de una aplicación para extraer los registros de auditoría de una aplicación a través de las API públicas de la aplicación. A continuación, envía los registros de auditoría a uno o más (hasta cinco) destinos.

ID de cliente

Al crear una autorización de aplicación para conectarse con una aplicación que usa el flujo de OAuth, es AppFabric posible que se te pida el ID y el secreto del cliente. El ID y el secreto de cliente se encuentran en la aplicación de autenticación de la aplicación. Para obtener instrucciones sobre dónde encontrar el ID de cliente en una aplicación de autenticación determinada, consulte Aplicaciones compatibles. El ID de cliente y el secreto de cliente que se comparten se cifran con una clave Clave propiedad de AWS o una AWS KMS clave gestionada por el cliente y se almacenan en. AppFabric

Secreto del cliente

Al crear una autorización de aplicación para conectarse con una aplicación que utiliza el flujo de OAuth, es AppFabric posible que te pida el ID y el secreto del cliente. El ID y el secreto de cliente se encuentran en la aplicación de autenticación de la aplicación. Para obtener instrucciones sobre dónde encontrar el secreto de cliente en una aplicación de autenticación determinada, consulte Aplicaciones compatibles. El ID de cliente y el secreto de cliente que se comparten se cifran con una clave Clave propiedad de AWS o una AWS KMS clave gestionada por el cliente y se almacenan en. AppFabric

Destino de ingestión

Un destino de ingestión define dónde deben almacenarse los registros de auditoría extraídos de una ingestión. Cada ingesta puede enviar los registros de auditoría a uno o más destinos (hasta cinco), que pueden ser un bucket de Amazon Simple Storage Service (Amazon S3) o una Amazon Data Firehose en su interior. Cuenta de AWS Para cada destino, puede definir si desea que los registros estén sin procesar o estén normalizados en un esquema de Open Cybersecurity Schema Framework (OCSF). Al seleccionar el esquema OCSF, puede definir el formato de los registros (JSON o Apache Parquet). El formato Apache Parquet solo se puede usar si se selecciona Amazon S3 como destino.

Aplicaciones receptoras de datos

Aplicaciones de las que se AppFabric necesitará obtener información generada. AppFabric

OAuth

OAuth es un protocolo abierto que permite la autorización segura de un método simple y estándar desde aplicaciones web, móviles y de escritorio. AppFabric usa OAuth para crear algunas autorizaciones de aplicaciones.

Open Cybersecurity Schema Framework (OCSF)

El Open Cybersecurity Schema Framework (OCSF) es un proyecto de código abierto que ofrece un marco extensible para desarrollar esquemas, junto con un esquema de seguridad básico independiente del proveedor. Los proveedores y otros productores de datos pueden adoptar y ampliar el esquema para sus dominios específicos. El objetivo es proporcionar un estándar abierto, que se adopte en cualquier entorno, aplicación o solución y que complemente los estándares y procesos de seguridad existentes. AppFabric ha ampliado este esquema para crear una estructura de eventos centrada en el software como servicio (SaaS) a la que se normalizarán todos los registros de auditoría de aplicaciones de SaaS compatibles AppFabric . Para obtener más información, consulte Marco de esquema de ciberseguridad abierto.

Token de acceso personal (PAT)

Un token de acceso personal (PAT) es una cadena de caracteres que se puede usar para acceder a un sistema informático en lugar de la contraseña habitual. Al crear una autorización de aplicación para conectarse con una aplicación que utiliza el flujo PAT, es AppFabric posible que le pida una PAT. El PAT se encuentra en la aplicación de autenticación de la aplicación. Para obtener instrucciones sobre dónde encontrar el PAT en una aplicación de autenticación específica, consulte Aplicaciones compatibles. Los tokens de la cuenta de servicio que se comparten se cifran con una clave Clave propiedad de AWS o una AWS KMS clave gestionada por el cliente y se almacenan en AppFabric.

Token de cuenta de servicio

Al crear una autorización de AppFabric aplicación para conectarse a una aplicación, algunas aplicaciones requerirán la creación de una cuenta de servicio para la autenticación de la aplicación. AppFabric puede solicitar el token de la cuenta de servicio como parte del proceso de autorización de la aplicación. Para obtener instrucciones sobre dónde encontrar el token de la cuenta de servicio en una aplicación de autenticación determinada, consulte Aplicaciones compatibles. Los tokens de las cuentas de servicio que se comparten se cifran con una clave Clave propiedad de AWS o una AWS KMS clave gestionada por el cliente y se almacenan en AppFabric.

ID de inquilino

Al crear una autorización de aplicación, AppFabric es posible que te pida el ID y el nombre del inquilino de la aplicación. El ID de inquilino es un identificador único para el inquilino de la aplicación. Cada aplicación puede tener términos diferentes para un inquilino, como ID de espacio de trabajo para Slack o ID de dominio para Asana. Para obtener instrucciones sobre dónde encontrar el ID de inquilino en una aplicación específica, consulte Aplicaciones compatibles.

Nombre de inquilino

Al crear una autorización de aplicación, AppFabric es posible que te pida el ID y el nombre del inquilino de la aplicación. El nombre de inquilino es un nombre único que se le asigna al ID del inquilino para que se utilice dentro de un paquete de aplicaciones. Este valor se usa para etiquetar la autorización de la aplicación y cualquier ingestión relacionada.

Seguridad en AWS AppFabric

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que se ejecuta Servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS AppFabric, consulte AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS servicios incluidos .
- Seguridad en la nube: su responsabilidad viene determinada por lo Servicio de AWS que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AppFabric. Los siguientes temas muestran cómo configurarlo AppFabric para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros Servicios de AWS que le ayuden a supervisar y proteger sus AppFabric recursos.

Temas

- Protección de datos en AWS AppFabric
- Gestión de identidad y acceso para AWS AppFabric
- Validación de conformidad para AWS AppFabric
- Mejores prácticas de seguridad para AWS AppFabric
- Resiliencia en AWS AppFabric
- Seguridad de la infraestructura en AWS AppFabric
- Análisis de configuración y vulnerabilidad en AWS AppFabric

Protección de datos en AWS AppFabric

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS AppFabric. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja AppFabric o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o

diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

> **Note**
>
> Para obtener más información sobre la protección de datos en lo que respecta a AppFabric la seguridad, consulteProcesamiento de datos.

Cifrado en reposo

AWS AppFabric admite el cifrado en reposo, una función de cifrado del lado del servidor que cifra de AppFabric forma transparente todos los datos relacionados con los paquetes de aplicaciones cuando se conservan en el disco y los descifra cuando se accede a los datos. De forma predeterminada, AppFabric cifra los datos mediante un from (). Clave propiedad de AWS AWS Key Management Service AWS KMS También puede optar por cifrar sus datos con su propia clave gestionada por el cliente desde. AWS KMS

Al eliminar una agrupación de aplicaciones, todos sus metadatos se eliminan de forma permanente.

Cifrado en tránsito

Al configurar un paquete de aplicaciones, puede elegir una clave gestionada por el cliente Clave propiedad de AWS o una clave gestionada por el cliente. Al recopilar y normalizar los datos para una ingesta de registros de auditoría, los AppFabric almacena temporalmente en un bucket intermedio de Amazon Simple Storage Service (Amazon S3) y los cifra con esta clave. Este bucket intermedio se elimina después de 30 días y está sujeto a una política de ciclo de vida de bucket.

AppFabric protege todos los datos en tránsito mediante TLS 1.2 y firma las solicitudes de API con Signature V4. Servicios de AWS AWS

Administración de claves

AppFabric admite el cifrado de datos con una Clave propiedad de AWS o varias claves gestionadas por el cliente. Le recomendamos que use una clave gestionada por el cliente, ya que esta opción le permite controlar por completo sus datos cifrados. Al elegir una clave gestionada por el cliente, AppFabric adjunta una política de recursos a la clave gestionada por el cliente que le concede acceso a la clave gestionada por el cliente.

Clave administrada por clientes

Para crear una clave gestionada por el cliente, siga los pasos para Creación de claves de KMS de cifrado simétrico que encontrará en la Guía del desarrollador de AWS KMS .

Política de claves

Las políticas de claves controlan el acceso a las claves administradas por el cliente. Cada clave administrada por el cliente debe tener exactamente una política de clave, que contiene instrucciones que determinan quién puede usar la clave y cómo puede utilizarla. Cuando crea la clave administrada por el cliente, puede especificar una política de clave. Para obtener información sobre cómo modificar una política de claves, consulte Creación de una política de claves en la Guía del desarrollador de AWS KMS .

Para usar una clave administrada por el cliente AppFabric, el usuario o rol AWS Identity and Access Management (de IAM) que crea AppFabric los recursos debe tener permiso para usar la clave administrada por el cliente. Le recomendamos que cree una clave que utilice únicamente con AppFabric y añada a sus AppFabric usuarios como usuarios de la clave. Este método limita el alcance del acceso a sus datos. Sus usuarios necesitarán los siguientes permisos:

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Decrypt`

La AWS KMS consola le guía a través de la creación de una clave con la política de claves adecuada. Para obtener más información acerca de las políticas de claves, consulte Políticas de claves en AWS KMS en la Guía para desarrolladores de AWS KMS .

A continuación se muestra un ejemplo de política de claves que permite:

- El control Usuario raíz de la cuenta de AWS total de la clave.
- Los usuarios pueden AppFabric utilizar su clave gestionada por el cliente con AppFabric.
- Una política de claves para la configuración de una agrupación de aplicaciones en `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"
                }
            }
        }
    ]
}
```

¿Cómo se AppFabric utilizan las subvenciones en AWS KMS

AppFabric requiere una concesión para utilizar la clave gestionada por el cliente. Para obtener más información, consulte Concesiones de AWS KMS en la Guía para desarrolladores de AWS KMS .

Al crear un paquete de aplicaciones, AppFabric crea una subvención en tu nombre enviando una `CreateGrant` solicitud a AWS KMS. Las subvenciones AWS KMS se utilizan para dar AppFabric acceso a una AWS KMS clave de la cuenta de un cliente. AppFabric requiere que la concesión utilice la clave gestionada por el cliente para las siguientes operaciones internas:

- Envíe `GenerateDataKey` solicitudes AWS KMS para generar claves de datos cifradas por su clave gestionada por el cliente.
- Envíe `Decrypt` solicitudes AWS KMS para descifrar las claves de datos cifradas para que puedan usarse para cifrar sus datos y para descifrar los tokens de acceso a las aplicaciones en tránsito.
- Envíe `Encrypt` solicitudes para cifrar los tokens de acceso AWS KMS a las aplicaciones en tránsito.

A continuación, se muestra un ejemplo de una concesión.

```
{
  "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"
    }
  }
},
```

Cuando eliminas un paquete de aplicaciones, AppFabric se retiran las subvenciones emitidas en tu clave gestionada por el cliente.

Supervisar tus claves de cifrado para AppFabric

Cuando utilizas claves gestionadas por el AWS KMS cliente con AppFabric, puedes utilizar AWS CloudTrail los registros para realizar un seguimiento de las solicitudes que se AppFabric envían a AWS KMS.

A continuación se muestra un ejemplo de un CloudTrail evento registrado cuando se AppFabric utiliza como clave gestionada `CreateGrant` por el cliente.


```
{
    "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"
    }
}
```

Gestión de identidad y acceso para AWS AppFabric

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AppFabric La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- ¿Cómo AWS AppFabric funciona con IAM
- Ejemplos de políticas basadas en identidades de AWS AppFabric
- Uso de roles vinculados a servicios de AppFabric
- AWS políticas gestionadas para AWS AppFabric
- Solución de problemas AWS AppFabric de identidad y acceso

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AppFabric

Usuario del servicio: si utiliza el AppFabric servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AppFabric funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función en AppFabric, consulteSolución de problemas AWS AppFabric de identidad y acceso.

Administrador de servicios: si está a cargo de AppFabric los recursos de su empresa, probablemente tenga acceso total a ellos AppFabric. Su trabajo consiste en determinar a qué AppFabric funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM AppFabric, consulte¿Cómo AWS AppFabric funciona con IAM.

Administrador de IAM: si es administrador de IAM, tal vez le interese obtener más información sobre cómo redactar políticas para administrar el acceso. AppFabric Para ver ejemplos de políticas AppFabric basadas en la identidad que puede usar en IAM, consulte. Ejemplos de políticas basadas en identidades de AWS AppFabric

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la

contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute

aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.

- Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS AppFabric funciona con IAM

Antes de utilizar IAM para gestionar el acceso AppFabric, infórmese sobre las funciones de IAM disponibles para su uso. AppFabric

Funciones de IAM que puede utilizar con AWS AppFabric

Característica de IAM	AppFabric soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí

Característica de IAM	AppFabric soporte
Recursos de políticas	Sí
Claves de condición de política	No
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	No
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo Servicios de AWS funcionan la mayoría de las funciones de IAM AppFabric y otras funciones, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para AppFabric

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en

una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para AppFabric

Para ver ejemplos de políticas AppFabric basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS AppFabric

Políticas basadas en recursos dentro de AppFabric

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para AppFabric

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de AppFabric acciones, consulta las acciones definidas AWS AppFabric en la Referencia de autorización del servicio.

Las acciones políticas AppFabric utilizan el siguiente prefijo antes de la acción:

```
appfabric
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "appfabric:action1",
      "appfabric:action2"
         ]
```

Puede especificar varias acciones utilizando caracteres comodín (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `List`, incluya la siguiente acción.

```
"Action": "appfabric:List*"
```

Para ver ejemplos de políticas AppFabric basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS AppFabric

Recursos de políticas para AppFabric

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de AppFabric recursos y sus ARN, consulte Tipos de recursos definidos AWS AppFabric en la Referencia de autorización de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por. AWS AppFabric

Para ver ejemplos de políticas basadas en la AppFabric identidad, consulte. Ejemplos de políticas basadas en identidades de AWS AppFabric

Claves de condición de la política para AppFabric

Admite claves de condición de políticas específicas del servicio	No

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de AppFabric condición, consulte las claves de condición AWS AppFabric en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS AppFabric.

Para ver ejemplos de políticas AppFabric basadas en la identidad, consulte. Ejemplos de políticas basadas en identidades de AWS AppFabric

ACL en AppFabric

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AppFabric

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de

entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Utilizar credenciales temporales con AppFabric

Compatible con el uso de credenciales temporales	No

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda

generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para AppFabric

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en él AWS, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para AppFabric

Compatible con roles de servicio	No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio puede interrumpir AppFabric la funcionalidad. Edite las funciones de servicio solo cuando se AppFabric proporcionen instrucciones para hacerlo.

Funciones vinculadas al servicio para AppFabric

Compatible con roles vinculados al servicio	Sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre la creación o la administración de funciones AppFabric vinculadas al servicio, consulte. Uso de roles vinculados a servicios de AppFabric

Ejemplos de políticas basadas en identidades de AWS AppFabric

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar AppFabric recursos. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos AppFabric, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte las claves de condición, recursos y acciones de la Referencia de autorización de servicios. AWS AppFabric

Contenido

- Prácticas recomendadas sobre las políticas
- Mediante la consola de AppFabric
- AppFabric para ver ejemplos de políticas de IAM de seguridad
  - Cómo permitir el acceso a las agrupaciones de aplicaciones
  - Cómo restringir el acceso a las agrupaciones de aplicaciones
  - Cómo restringir la eliminación o detención de incorporaciones
- AppFabric para ver ejemplos de políticas de IAM de productividad
  - Permiso de acceso de solo lectura a las características de productividad
  - Permiso de acceso completo a las características de productividad
  - Permita el acceso para crear AppClients
  - Permita el acceso para obtener detalles de AppClients

  - Permitir el acceso a la lista AppClients
  - Permitir el acceso a la actualización AppClients
  - Permitir el acceso para eliminar AppClients
  - Permitir el acceso para autorizar aplicaciones
- Otros ejemplos de políticas de IAM
  - Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear AppFabric recursos de tu cuenta, acceder a ellos o eliminarlos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas

nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.

- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de AppFabric

Adjunta la política `AWSAppFabricReadOnlyAccess` AWS gestionada a tus identidades de IAM para concederles permisos de solo lectura para acceder al AppFabric servicio, incluida la consola del. AppFabric AWS Management Console O bien, puedes adjuntar la política `AWSAppFabricFullAccess` AWS gestionada a tus identidades de IAM para concederles un permiso administrativo completo para el servicio. AppFabric Para obtener más información, consulte AWS políticas gestionadas para AWS AppFabric.

AppFabric para ver ejemplos de políticas de IAM de seguridad

Los siguientes ejemplos de políticas se aplican a las funciones AppFabric de seguridad.

Cómo permitir el acceso a las agrupaciones de aplicaciones

El siguiente ejemplo de política otorga acceso a los paquetes de aplicaciones del AppFabric servicio.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
```

```
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Cómo restringir el acceso a las agrupaciones de aplicaciones

El siguiente ejemplo de política restringe el acceso a los paquetes de aplicaciones del servicio. AppFabric

```
{
    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Cómo restringir la eliminación o detención de incorporaciones

El siguiente ejemplo de política restringe la eliminación o la interrupción de las ingestas en el servicio. 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 para ver ejemplos de políticas de IAM de productividad

La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Los siguientes ejemplos de políticas se aplican a AppFabric las funciones de productividad.

Permiso de acceso de solo lectura a las características de productividad

El siguiente ejemplo de política concede acceso de solo lectura a las funciones AppFabric de productividad.

> **Important**
>
> Es posible que aparezca un error de acción no válido al agregar esta política en el editor de políticas JSON de la consola de IAM. Esto se debe a que las funciones AppFabric de productividad se encuentran actualmente en versión preliminar. Debe ignorar el error y proceder a crear la política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
                "appfabric:ListActionableInsights",
```

```
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights"
            ],
            "Resource": "*"
        }
    ],
    "Version": "2012-10-17"
}
```

Permiso de acceso completo a las características de productividad

El siguiente ejemplo de política otorga acceso completo a AppFabric las funciones de productividad.

> **Important**
>
> Es posible que aparezca un error de acción no válido al agregar esta política en el editor de políticas JSON de la consola de IAM. Esto se debe a que AppFabric las funciones de productividad se encuentran actualmente en versión preliminar. Debe ignorar el error y proceder a crear la política.

```
{
    "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"
}
```

Permita el acceso para crear AppClients

El siguiente ejemplo de política otorga acceso a la creación AppClients. Para obtener más información, consulte Crear una AppFabric para aumentar la productividad AppClient.

> **Important**
>
> Es posible que aparezca un error de acción no válido al agregar esta política en el editor de políticas JSON de la consola de IAM. Esto se debe a que AppFabric las funciones de productividad se encuentran actualmente en versión preliminar. Debe ignorar el error y proceder a crear la política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Permita el acceso para obtener detalles de AppClients

El siguiente ejemplo de política otorga acceso para obtener detalles de AppClients. Para obtener más información, consulte Obtener detalles de un AppClient.

> **Important**
>
> Es posible que aparezca un error de acción no válido al agregar esta política en el editor de políticas JSON de la consola de IAM. Esto se debe a que AppFabric las funciones de productividad se encuentran actualmente en versión preliminar. Debe ignorar el error y proceder a crear la política.

```
{
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Permitir el acceso a la lista AppClients

El siguiente ejemplo de política otorga acceso a la lista AppClients. Para obtener más información, consulte Obtener detalles de un AppClient.

> **Important**
>
> Es posible que aparezca un error de acción no válido al agregar esta política en el editor de políticas JSON de la consola de IAM. Esto se debe a que AppFabric las funciones de productividad se encuentran actualmente en versión preliminar. Debe ignorar el error y proceder a crear la política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:ListAppClients"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Permitir el acceso a la actualización AppClients

El siguiente ejemplo de política otorga acceso a la actualización AppClients. Para obtener más información, consulte Actualizar un AppClient.

> **Important**
>
> Es posible que aparezca un error de acción no válido al agregar esta política en el editor de políticas JSON de la consola de IAM. Esto se debe a que AppFabric las funciones de productividad se encuentran actualmente en versión preliminar. Debe ignorar el error y proceder a crear la política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:UpdateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Permitir el acceso para eliminar AppClients

El siguiente ejemplo de política otorga acceso a la eliminación AppClients. Para obtener más información, consulte Actualizar un AppClient.

> **Important**
>
> Es posible que aparezca un error de acción no válido al agregar esta política en el editor de políticas JSON de la consola de IAM. Esto se debe a que AppFabric las funciones de productividad se encuentran actualmente en versión preliminar. Debe ignorar el error y proceder a crear la política.

```
{
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:DeleteAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Permitir el acceso para autorizar aplicaciones

El siguiente ejemplo de política otorga acceso para autorizar aplicaciones mediante la API del token. Para obtener más información, consulte Autenticar y autorizar su aplicación.

> **Important**
>
> Es posible que aparezca un error de acción no válido al agregar esta política en el editor de políticas JSON de la consola de IAM. Esto se debe a que AppFabric las funciones de productividad se encuentran actualmente en versión preliminar. Debe ignorar el error y proceder a crear la política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:Token"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Otros ejemplos de políticas de IAM

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o 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": "*"
        }
    ]
}
```

Uso de roles vinculados a servicios de AppFabric

AWS AppFabric usa roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AppFabric Las funciones vinculadas al servicio están predefinidas AppFabric e incluyen todos los permisos que el servicio necesita para llamar a otras personas en su nombre. Servicios de AWS

Un rol vinculado a un servicio facilita la configuración AppFabric , ya que no es necesario añadir manualmente los permisos necesarios. AppFabric define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AppFabric puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se puede adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus AppFabric recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios de AppFabric

AppFabric utiliza el rol vinculado al servicio denominado `AWSServiceRoleForAppFabric` — Permite AppFabric colocar datos en un recurso de destino de ingestión, como un bucket de Amazon S3 o una transmisión de entrega de Amazon Data Firehose. También permite colocar datos CloudWatch métricos AppFabric en el espacio de nombres. `AWS/AppFabric`

El rol vinculado al servicio `AWSServiceRoleForAppFabric` depende de los siguientes servicios para asumir el rol:

- `appfabric.amazonaws.com`

La política de permisos de roles denominada `AWSAppFabricServiceRolePolicy` permite AppFabric realizar las siguientes acciones en los recursos especificados:

- Acción: `cloudwatch:PutMetricData` en el espacio de nombres `AWS/AppFabric`. Esta acción otorga permiso AppFabric para colocar datos de métricas en el espacio de CloudWatch `AWS/`

`AppFabric` nombres de Amazon. Para obtener más información sobre las AppFabric métricas disponibles en CloudWatch, consulte. Monitorización AWS AppFabric con Amazon CloudWatch

- Acción: `s3:PutObject` en un bucket de Amazon S3. Esta acción otorga permiso AppFabric para colocar los datos ingeridos en un bucket de Amazon S3 que especifique.
- Acción: `firehose:PutRecordBatch` en una transmisión de entrega de Amazon Data Firehose. Esta acción otorga permiso AppFabric para colocar los datos ingeridos en una transmisión de entrega de Amazon Data Firehose que especifique.

Para obtener más información, consulte las políticas AWS gestionadas de. AppFabric

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Crear un rol vinculado a un servicio para AppFabric

No necesita crear manualmente un rol vinculado a servicios. Al crear un paquete de AppFabric aplicaciones en la AWS Management Console, la o la AWS API AWS CLI, se AppFabric crea automáticamente el rol vinculado al servicio.

Editar un rol vinculado a un servicio para AppFabric

AppFabric no permite editar el rol vinculado al `AWSServiceRoleForAppFabric` servicio. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para AppFabric

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debes eliminar todos los paquetes de AppFabric aplicaciones para poder eliminar el rol vinculado al servicio.

Saneamiento de un rol vinculado a servicios

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol. El rol utiliza los paquetes de aplicaciones que cree. AppFabric Para obtener más información, consulte Eliminar AWS AppFabric para recursos de seguridad.

> **Note**
>
> Si el AppFabric servicio utiliza el rol cuando intentas eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Eliminar manualmente el rol vinculado al servicio

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al `AWSServiceRoleForAppFabric` servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles para los roles vinculados al servicio AppFabric

AppFabric admite el uso de funciones vinculadas al servicio en todos los lugares en los que el servicio Regiones de AWS esté disponible. Para obtener más información, consulte los AppFabric puntos finales y las cuotas en. Referencia general de AWS

AWS políticas gestionadas para AWS AppFabric

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del usuario de IAM.

Servicios de AWS mantener y actualizar las políticas AWS gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada por AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS gestionada proporciona acceso de solo lectura a todos Servicios de AWS los recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte Políticas administradas de AWS para funciones de trabajo en la Guía del usuario de IAM.

AWS política gestionada: AWSAppFabricReadOnlyAccess

Puede adjuntar la política `AWSAppFabricReadOnlyAccess` a las identidades de IAM. Esta política concede permisos de solo lectura al AppFabric servicio.

> **Note**
>
> La `AWSAppFabricReadOnlyAccess` política no concede acceso de solo lectura a las funciones de productividad. AppFabric

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `appfabric`: otorga permiso para obtener una agrupación de aplicaciones, enumerar agrupaciones de aplicaciones, obtener una autorización de aplicación, enumerar autorizaciones de aplicaciones, obtener una incorporación, enumerar las incorporaciones, obtener un destino de incorporación, enumerar los destinos de incorporación y enumerar las etiquetas de recursos.

```
{
    "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 política gestionada: AWSAppFabricFullAccess

Puede adjuntar la política `AWSAppFabricFullAccess` a las identidades de IAM. Esta política concede permisos administrativos al AppFabric servicio.

> **Important**
>
> La `AWSAppFabricFullAccess` política no concede acceso a las funciones AppFabric de productividad porque actualmente se encuentran en versión preliminar. Para obtener más información sobre cómo conceder el acceso a las funciones AppFabric de productividad, consulte[AppFabric para ver ejemplos de políticas de IAM de productividad](#).

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `appfabric`— Otorga el permiso administrativo completo a AppFabric.
- `kms`: otorga permiso para enumerar alias.
- `s3`: otorga permisos para enumerar todos los buckets de Amazon S3 y obtener la ubicación de los buckets.
- `firehose`— Otorga permiso para enumerar las transmisiones de entrega de Amazon Data Firehose y describir las transmisiones de entrega.
- `iam`— Otorga permiso para crear el rol `AWSServiceRoleForAppFabric` vinculado al servicio para. AppFabric Para obtener más información, consulte [Uso de roles vinculados a servicios de 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 política gestionada: AWSAppFabricServiceRolePolicy

No puede adjuntar la política `AWSAppFabricServiceRolePolicy` a sus entidades de IAM. Esta política está asociada a un rol vinculado al servicio que permite AppFabric realizar acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios de AppFabric.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `cloudwatch`— Otorga permiso AppFabric para colocar datos de métricas en el espacio de CloudWatch `AWS/AppFabric` nombres de Amazon. Para obtener más información sobre las AppFabric métricas disponibles en CloudWatch, consulte. Monitorización AWS AppFabric con Amazon CloudWatch
- `s3`— Otorga permiso AppFabric para colocar los datos ingeridos en un bucket de Amazon S3 que usted especifique.
- `firehose`— Otorga permiso AppFabric para incluir los datos ingeridos en una transmisión de entrega de Amazon Data Firehose que especifique.

```
{
    "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 actualizaciones de las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AppFabric desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AppFabric documento.

Cambio	Descripción	Fecha
AWSAppFabricReadOnlyAccess: política nueva	AppFabric agregó una nueva política para conceder permisos de solo lectura al AppFabric servicio.	27 de junio de 2023
AWSAppFabricFullAccess: política nueva	AppFabric agregó una nueva política para conceder permisos administrativos al AppFabric servicio.	27 de junio de 2023
AWSAppFabricServiceRolePolicy: política nueva	AppFabric agregó una nueva política para la función `AWSServiceRoleForAppFabric` vinculada al servicio.	27 de junio de 2023
AppFabric comenzó a rastrear los cambios	AppFabric comenzó a realizar un seguimiento de los	27 de junio de 2023

Cambio	Descripción	Fecha
	cambios de sus políticas AWS gestionadas.	

Solución de problemas AWS AppFabric de identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con un AppFabric IAM.

Temas

- No estoy autorizado a realizar ninguna acción en AppFabric
- No tengo autorización para realizar iam:PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AppFabric recursos

No estoy autorizado a realizar ninguna acción en AppFabric

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `appfabric:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 appfabric:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `appfabric:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No tengo autorización para realizar iam:PassRole

Si recibes un mensaje de error en el que se indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferirle una función AppFabric.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en ella. AppFabric Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis AppFabric recursos

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si AppFabric es compatible con estas funciones, consulte¿Cómo AWS AppFabric funciona con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información acerca del uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Validación de conformidad para AWS AppFabric

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos

el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).

- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Mejores prácticas de seguridad para AWS AppFabric

AWS AppFabric proporciona varias características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no suponen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Cómo supervisar la aplicación sin acceso de administrador

Con el permiso de solo lectura AWS Identity and Access Management (IAM), cualquiera puede integrarse con AppFabric Amazon QuickSight y otras herramientas de gestión de eventos e información de seguridad (SIEM), como. Splunk Para supervisar la seguridad de las aplicaciones, los datos se envían a un bucket de Amazon Simple Storage Service (Amazon S3) o a un flujo de entrega de Amazon Data Firehose.

Supervise los eventos AppFabric

Puedes monitorizar AppFabric con CloudWatch las métricas de Amazon. CloudWatch recopila datos de AppFabric cada minuto y los procesa para convertirlos en métricas. Puede configurar alarmas para activar notificaciones cuando las métricas coincidan con los umbrales especificados. Para obtener más información, consulte Monitorización AWS AppFabric con Amazon CloudWatch.

Resiliencia en AWS AppFabric

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS AppFabric

Como servicio gestionado, AWS AppFabric está protegido por los procedimientos de seguridad de red AWS global que se describen en el documento técnico Amazon Web Services: Overview of Security Processes.

Utiliza las llamadas a la API AWS publicadas para acceder a AppFabric través de la red. Los clientes deben ser compatibles con TLS 1.0 o una versión posterior. Recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. O, para generar credenciales de seguridad temporales para firmar solicitudes, puede utilizar AWS Security Token Service (AWS STS).

Análisis de configuración y vulnerabilidad en AWS AppFabric

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted, nuestro cliente. Para obtener más información, consulte el modelo de responsabilidad AWS compartida.

Monitorización AWS AppFabric

La supervisión es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de AWS AppFabric AWS las demás soluciones. AWS proporciona las siguientes herramientas de monitoreo para observar AppFabric, informar cuando algo anda mal y tomar medidas automáticas cuando sea apropiado:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon EC2 y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus archivos de registro desde instancias de Amazon EC2 y otras fuentes. AWS CloudTrail CloudWatch Los registros pueden monitorear la información de los archivos de registro y notificarle cuando se alcancen ciertos umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la Guía del usuario CloudWatch de Amazon Logs.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por usted o en su nombre Cuenta de AWS y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Monitorización AWS AppFabric con Amazon CloudWatch

Puedes monitorizar el AWS AppFabric uso CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se mantienen durante 15 meses, de forma que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

El AppFabric servicio informa de las siguientes métricas en el espacio de `AWS/AppFabric` nombres.

Métrica	Descripción
AppFabric Estado de autorización de la aplicación	El estado de la autorización de la aplicació n (`1`para estar conectada o `0` para cualquier otra).
AppFabric Latencia de entrega de datos	El tiempo (en segundos) que se tarda en AppFabric recopilar los registros de auditoría de la aplicación SaaS y entregarlos al destino configurado (Amazon S3 o Amazon Data Firehose).
Estado de destinos de ingestión	El estado del destino de ingestión (`1` para un activo o `0` para cualquier otro).
Retraso general de datos	La diferencia de tiempo (en segundos) entre el momento en que se produjeron los eventos en la aplicación SaaS y el momento en que se entregaron los registros de auditoría correspon dientes al destino configurado (Amazon S3 o Amazon Data Firehose) de. AppFabric
Volumen de datos ingeridos	El tamaño de los datos que se envían a Amazon Simple Storage Service (Amazon S3) o Amazon Data Firehose.

Las AppFabric métricas admiten la siguiente dimensión.

Dimensión	Descripción
ARN de destino de ingestión	El nombre de recurso de Amazon (ARN) del destino de ingestión.

Registro de llamadas a la AWS AppFabric API mediante AWS CloudTrail

AWS AppFabric está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un Servicio de AWS usuario AppFabric. CloudTrail captura todas las llamadas a la API AppFabric como eventos. Las llamadas capturadas incluyen llamadas desde la AppFabric consola y llamadas en código a las operaciones de la AppFabric API. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AppFabric. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar a AppFabric qué dirección IP se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información al respecto CloudTrail, consulte la Guía AWS CloudTrail del usuario.

AppFabric información en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AppFabric, esa actividad se registra en un CloudTrail evento junto con otros Servicio de AWS eventos del historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos en la Guía del AWS CloudTrail usuario.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos para AppFabric ti, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros Servicios de AWS para que analicen más a fondo los datos de eventos recopilados en los CloudTrail registros y actúen en función de ellos. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS CloudTrail :

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas AppFabric las acciones se registran CloudTrail y se documentan en la Referencia de la AWS AppFabric API. Por ejemplo, las llamadas a las `CreateAppBundle` `GetAppBundle` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `UpdateAppBundle`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

Para obtener más información, consulte el CloudTrail userIdentityelemento de la Guía del AWS CloudTrail usuario.

Descripción de las entradas de los archivos de AppFabric registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateAppBundle` acción.

```
{
    "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"
    }
```

```
}
```

Cuotas para AWS AppFabric

Cuenta de AWS Tiene cuotas predeterminadas, antes denominadas límites, para cada una de ellas Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas AppFabric, abra la consola Service Quotas. En el panel de navegación, elija AWS servicios y seleccione AppFabric.

Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas. Si la cuota aún no se encuentra disponible en Service Quotas, utilice el formulario de aumento del límite.

Las cuotas relacionadas AppFabric con esas cuotas Cuenta de AWS se muestran en la siguiente tabla.

Nombre	Valor predeterminado	Ajusta	Descripción
Agrupaciones de aplicaciones	Cada región admitida: 1	No	El número máximo de paquetes de aplicaciones que puede crear en una cuenta en la AWS región actual.
Autorizaciones de aplicaciones	Cada región admitida: 50	No	El número máximo de autorizaciones de solicitud que puede crear en una cuenta en la región actual AWS .
Incorporaciones	Cada región admitida: 50	No	El número máximo de incorporaciones que puede crear en una cuenta en la región actual AWS .

Nombre	Valor predeterminado	Ajusta	Descripción
Destinos de incorporación	Cada región admitida: 5	No	El número máximo de destinos de ingesta que puedes crear por ingesta en una cuenta de la región actual. AWS
AppClient	Cada región admitida: 1	No	El número máximo AppClients que puedes crear en una cuenta en la región actual AWS . La función AWS AppFabric de productividad está en versión preliminar y está sujeta a cambios.

Historial de documentos de la Guía AppFabric de administración

En la siguiente tabla se describen las versiones de la documentación de AWS AppFabric.

Cambio	Descripción	Fecha
Nueva aplicación compatible	Se agregó JumpCloud como aplicación compatible. Para obtener más información, consulte Aplicaciones compatibles en AWS AppFabric.	5 de junio de 2024
Nuevas aplicaciones compatibles y herramienta de seguridad	Aplicaciones Google Analytics añadidas Azure Monitor y compatibles. Para obtener más información, consulte Aplicaciones compatibles en AWS AppFabric. Se agregó Singularity Cloud como herramienta de seguridad compatible. Para obtener más información, consulte Herramientas de seguridad compatibles.	30 de abril de 2024
Nueva aplicación compatible	Se agregó SentinelOne como aplicación compatible. Para obtener más información, consulte Aplicaciones compatibles en AWS AppFabric.	25 de abril de 2024
Nueva aplicación compatible	Se agregó 1Password como aplicación compatible. Para	23 de abril de 2024

	obtener más informaci ón, consulte Aplicacio nes compatibles en AWS AppFabric.	
Nueva herramienta de seguridad compatible	Se agregó Dynatrace como herramienta de seguridad compatible. Para obtener más información, consulte Herramientas de seguridad compatibles.	26 de marzo de 2024
Nueva métrica	Se agregó la métrica del estado de autorización de la AppFabric aplicación. Para obtener más informaci ón, consulta Monitorización AWS AppFabric con Amazon CloudWatch Logs.	8 de marzo de 2024
Nueva aplicación compatible	Se agregó IBM Security® Verify como aplicación compatible. Para obtener más información, consulte Aplicacio nes compatibles en AWS AppFabric.	6 de marzo de 2024
Nueva aplicación compatible	Se agregó Box como aplicació n compatible. Para obtener más información, consulte Aplicaciones compatibles en AWS AppFabric.	28 de febrero de 2024

Nuevas aplicaciones y métricas compatibles	Se agregaron Cisco Duo y Terraform Cloud como aplicaciones compatibles. Salesforce Para obtener más información sobre ellas, consulte Aplicaciones compatibles en AWS AppFabric. Se agregaron las AppFabric métricas de latencia de entrega de datos y retraso general de datos. Para obtener más información, consulta Monitorización AWS AppFabric con Amazon CloudWatch Logs.	1 de febrero de 2024
Se agregaron Atlassian Confluence, Genesys Cloud, HubSpot, OneLogin by One Identity, PagerDuty y Ping Identity como aplicaciones compatibles y Barracuda XDR como herramienta de seguridad compatible	Para obtener más información sobre las nuevas aplicaciones compatibles, consulte Aplicaciones compatibles AWS AppFabric y Herramientas de seguridad compatibles.	15 de diciembre de 2023
Se agregaron Atlassian Confluence, Genesys Cloud, HubSpot, OneLogin by One Identity, PagerDuty y Ping Identity como aplicaciones compatibles y Barracuda XDR como herramienta de seguridad compatible	Para obtener más información sobre las nuevas aplicaciones compatibles, consulte Aplicaciones compatibles AWS AppFabric y Herramientas de seguridad compatibles.	15 de diciembre de 2023

Se agregó la documentación de vista previa AWS AppFabric para la productividad	Para obtener más información sobre AppFabric la productividad, consulte ¿Qué es AWS AppFabric la productividad?	27 de noviembre de 2023
GitHub y ServiceNow se agregaron como aplicaciones compatibles	Para obtener más información sobre las nuevas aplicaciones compatibles, consulte Aplicaciones compatibles.	31 de octubre de 2023
Comenzó a rastrear las políticas AWS gestionadas para AWS AppFabric	Para obtener más información sobre las políticas AWS administradas para AppFabric, consulte Políticas AWS administradas para AWS AppFabric.	27 de junio de 2023
Versión inicial	Versión inicial de la Guía AWS AppFabric de administración.	27 de junio de 2023

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.