Guia de administração

AWS AppFabric

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS AppFabric: Guia de administração

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que AWS AppFabric é 1
Produtos 1
Benefícios 1
Casos de uso 2
Como AppFabric funciona 2
Definição de preço 3
Disponibilidade 3
O que é AWS AppFabric para segurança? 3
Benefícios 1
Casos de uso 2
Acessando AppFabric para fins de segurança 4
Serviços relacionados 5
Esquema OCSF 6
Pré-requisitos e recomendações 7
Conceitos básicos 13
Aplicações compatíveis 23
Ferramentas de segurança compatíveis 123
Excluir recursos 138
O que AWS AppFabric significa produtividade? 140
Benefícios 1
Casos de uso 2
Acesso AppFabric para produtividade 4
Introdução para desenvolvedores de aplicações 143
Introdução para usuários finais 171
AppFabric APIs de produtividade 188
Processamento de dados 213
Terminologia e conceitos 215
Segurança 219
Proteção de dados 220
Criptografia em repouso 221
Criptografia em trânsito 221
Gerenciamento de chaves 221
Política de chave 222
Como AppFabric usa subsídios em AWS KMS 224

Monitorando suas chaves de criptografia para AppFabric 225
Gerenciamento de identidade e acesso 227
Público 227
Autenticando com identidades 228
Gerenciando acesso usando políticas 232
Como AWS AppFabric funciona com o IAM 234
Exemplos de políticas baseadas em identidade 242
Usar funções vinculadas ao serviço 252
AWS políticas gerenciadas 255
Solução de problemas 261
Validação de conformidade 263
Melhores práticas de segurança 264
Monitorar o aplicativo sem acesso de administrador 264
Monitor de AppFabric eventos 264
Resiliência 265
Segurança da infraestrutura 265
Análise de configuração e vulnerabilidade 265
Monitoramento 266
Monitoramento com CloudWatch 266
CloudTrail troncos 267
AppFabric informações em CloudTrail 268
Entendendo as entradas do arquivo de AppFabric log 269
Cotas 271
Histórico do documento 273
..... cclxxvii

O que AWS AppFabric é

AWS AppFabric conecta rapidamente aplicativos de software como serviço (SaaS) em toda a organização, para que as equipes de TI e segurança possam gerenciar e proteger aplicativos com facilidade usando um esquema padrão, e os funcionários possam concluir as tarefas diárias com mais rapidez usando a IA generativa.

Tópicos

- Produtos
- Benefícios
- Casos de uso
- Como AppFabric funciona
- Definição de preço
- Disponibilidade
- O que é AWS AppFabric para segurança?
- O que AWS AppFabric significa produtividade?

Produtos

Explore as duas facetas AWS AppFabric: AppFabric para segurança, projetada para gerenciamento e segurança simplificados, e AppFabric para produtividade (versão prévia), aprimorada com recursos generativos de IA. Para obter mais informações, consulte os tópicos a seguir.

- O que é AWS AppFabric para segurança?
- O que AWS AppFabric significa produtividade?

Benefícios

Você pode usar AppFabric para fazer o seguinte:

- Conectar seus aplicativos em minutos e reduza os custos operacionais.
- Aumentar a visibilidade dos dados do aplicativo SaaS para elevar sua postura de segurança.
- Facilitar automaticamente as tarefas em todas as aplicações com IA generativa.

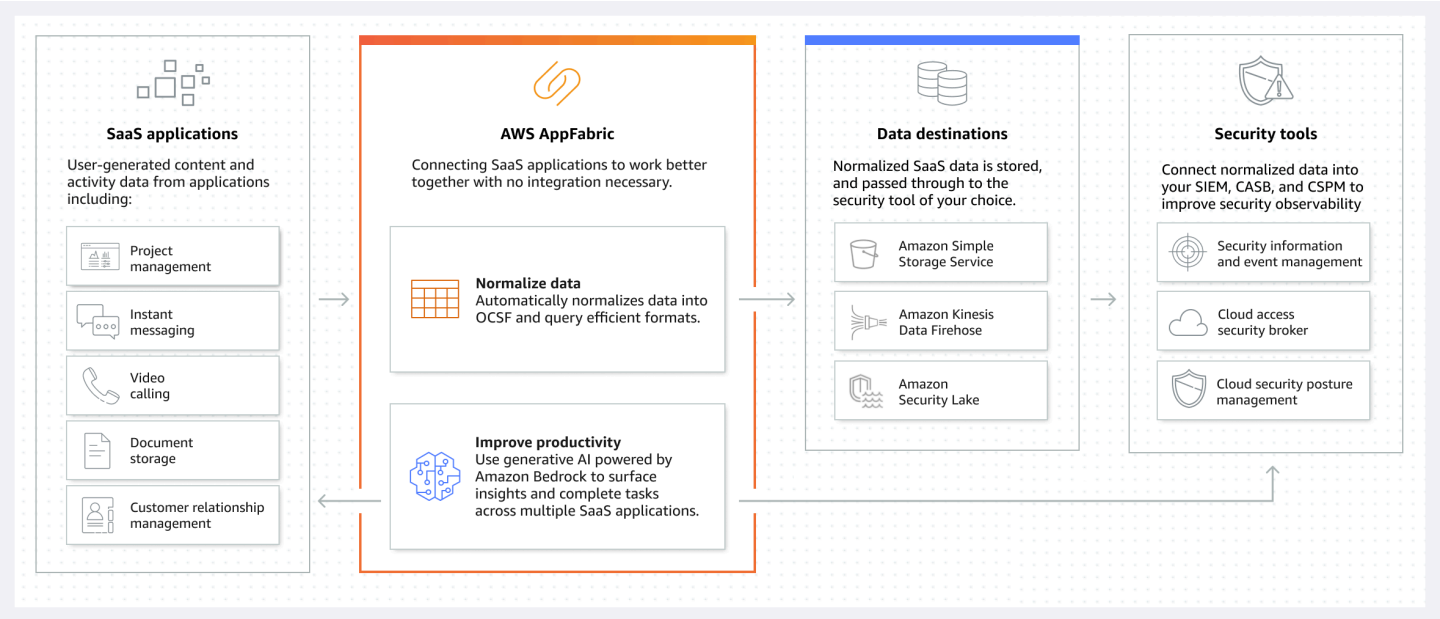
Casos de uso

Você pode usar AppFabric para:

- Conectar seus aplicativos SaaS rapidamente
  - AppFabric for security conecta de forma nativa os principais aplicativos de produtividade e segurança de SaaS entre si, fornecendo uma solução de interoperabilidade SaaS totalmente gerenciada.
- Elevar sua postura de segurança
  - Os dados do aplicativo são normalizados automaticamente, permitindo que os administradores definam políticas comuns, padronizem alertas de segurança e gerenciem facilmente o acesso dos usuários em vários aplicativos.
- Reinventar a produtividade
  - Com um assistente generativo comum de IA, o AppFabric for productivity capacita os funcionários a obter respostas rapidamente, automatizar o gerenciamento de tarefas e gerar insights em seus aplicativos de produtividade SaaS.

Como AppFabric funciona

AppFabric conecta rapidamente vários aplicativos SaaS sem a necessidade de codificação para aumentar a produtividade e a segurança. O diagrama a seguir mostra os benefícios do AppFabric.



> **Note**
>
> AppFabric para produtividade está atualmente lançado como uma prévia e está disponível no Leste dos EUA (Norte da Virgínia) Região da AWS. Para obter mais informações sobre Regiões da AWS, consulte AWS AppFabric endpoints e cotas no. Referência geral da AWS

Definição de preço

Para obter detalhes e exemplos de AppFabric preços, consulte AWS AppFabric Preços.

Disponibilidade

Para ver as AWS regiões e endpoints atualmente suportados AppFabric, consulte AWS AppFabric endpoints e cotas na AWS Referência geral.

O que é AWS AppFabric para segurança?

AWS AppFabric para segurança, conecta rapidamente os aplicativos de software como serviço (SaaS) em toda a organização, para que as equipes de TI e segurança possam gerenciar e proteger aplicativos com facilidade usando um esquema padrão.

Tópicos

- Benefícios
- Casos de uso
- Acessando AppFabric para fins de segurança
- Serviços relacionados
- Open Cybersecurity Schema Framework
- Pré-requisitos e recomendações
- Introdução AWS AppFabric à segurança
- Aplicações compatíveis
- Ferramentas e serviços de segurança compatíveis
- Excluir AWS AppFabric para recursos de segurança

Benefícios

Você pode usar como AppFabric medida de segurança para fazer o seguinte:

- Conectar seus aplicativos em minutos e reduza os custos operacionais.
- Aumentar a visibilidade dos dados do aplicativo SaaS para elevar sua postura de segurança.

Casos de uso

Você pode usar como segurança AppFabric para:

- Conectar seus aplicativos SaaS rapidamente
  - AppFabric for security conecta de forma nativa os principais aplicativos de produtividade e segurança de SaaS entre si, fornecendo uma solução de interoperabilidade SaaS totalmente gerenciada.
- Elevar sua postura de segurança
  - Os dados do aplicativo são normalizados automaticamente, permitindo que os administradores definam políticas comuns, padronizem alertas de segurança e gerenciem facilmente o acesso dos usuários em vários aplicativos.

Acessando AppFabric para fins de segurança

AppFabric para fins de segurança, está disponível no Leste dos EUA (Norte da Virgínia), Europa (Irlanda) e Ásia-Pacífico (Tóquio) Regiões da AWS. Para obter mais informações sobre Regiões da AWS, consulte AWS AppFabric endpoints e cotas no. Referência geral da AWS

Em cada região, você pode acessar AppFabric para fins de segurança de qualquer uma das seguintes formas:

AWS Management Console

AWS Management Console É uma interface baseada em navegador que você pode usar para criar e gerenciar AWS recursos. O AppFabric console fornece acesso aos seus AppFabric recursos. Você pode usar o AppFabric console para criar e gerenciar todos os AppFabric recursos.

AppFabric API

Para acessar AppFabric programaticamente, use a AppFabric API e emita solicitações HTTPS diretamente para o serviço. Para obter mais informações, consulte a Referência AWS AppFabric da API.

AWS Command Line Interface (AWS CLI)

Com o AWS CLI, você pode emitir comandos na linha de comando do seu sistema para interagir com AppFabric outros Serviços da AWS. Se você quiser criar scripts que realizem tarefas, as ferramentas da linha de comando também são úteis. Para obter informações sobre como instalar e usar o AWS CLI, consulte o Guia AWS Command Line Interface do usuário da versão 2. Para obter informações sobre os AWS CLI comandos para AppFabric, consulte a AppFabric seção da AWS CLI Referência.

Serviços relacionados

Você pode usar o seguinte AppFabric para Serviços da AWS fins de segurança:

Amazon Data Firehose

O Amazon Data Firehose é um serviço de extração, transformação e carregamento (ETL) que captura, transforma e entrega dados de streaming de forma confiável para lagos de dados, armazenamentos de dados e serviços de análise. Ao usar AppFabric, você pode optar por enviar seus registros de auditoria normalizados ou brutos do Open Cybersecurity Schema Framework (OCSF) no formato JSON para um stream do Firehose como seu destino. Para obter mais informações, consulte Criar um local de saída no Firehose.

Amazon Security Lake

O Amazon Security Lake centraliza automaticamente os dados de segurança de AWS ambientes, provedores de SaaS, fontes locais e na nuvem em um data lake criado especificamente e armazenado em sua conta. Você pode integrar dados de log de AppFabric auditoria com o Security Lake selecionando o Amazon Data Firehose como destino e configurando o Firehose para entregar dados no formato e caminho corretos no Security Lake. Para obter mais informações, consulte Coleta de dados de fontes personalizadas no Guia do usuário do Amazon Security Lake.

Amazon Simple Storage Service

O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos oferecendo escalabilidade líder do setor, disponibilidade de dados, segurança e desempenho. Ao usar AppFabric, você pode optar por enviar seus registros de auditoria OCSF normalizados (JSON

ouApache Parquet) ou brutos (JSON) para um bucket Amazon S3 novo ou existente como seu destino. Para obter mais informações, consulte Criar um local de saída do Amazon S3.

Amazon QuickSight

A Amazon QuickSight capacita organizações orientadas por dados com inteligência de negócios (BI) unificada em hiperescala. Com QuickSight, todos os usuários podem atender a diferentes necessidades analíticas a partir da mesma fonte confiável por meio de painéis interativos modernos, relatórios paginados, análises incorporadas e consultas em linguagem natural. Você pode analisar os dados do log de AppFabric auditoria escolhendo o bucket do Amazon S3 em QuickSight que seus AppFabric registros são armazenados como sua fonte. Para obter mais informações, consulte Criação de um conjunto de dados usando arquivos do Amazon S3 no Guia do usuário da QuickSight Amazon. Você também pode importar AppFabric dados do Amazon S3 para o Amazon Athena e selecionar o Amazon Athena como fonte de dados em. QuickSight Para obter mais informações, consulte Criação de um conjunto de dados usando dados do Amazon Athena no Guia do usuário da QuickSight Amazon.

AWS Key Management Service

Com AWS Key Management Service (AWS KMS), você pode criar, gerenciar e controlar chaves criptográficas em seus aplicativos e. Serviços da AWS Ao criar um pacote de aplicativos AppFabric, você configura uma chave de criptografia para proteger com segurança os dados do aplicativo autorizado. Essa chave criptografa seus dados dentro do AppFabric serviço. AppFabric pode usar uma chave Chave pertencente à AWS criada e gerenciada por AppFabric em seu nome ou uma chave gerenciada pelo cliente na qual você cria e gerencia AWS KMS. Para obter mais informações, consulte Criar uma AWS KMS chave.

Open Cybersecurity Schema Framework

O Open Cybersecurity Schema Framework (OCSF) é um esforço colaborativo AWS e de código aberto de parceiros líderes no setor de segurança cibernética. O OCSF fornece um esquema padrão para eventos de segurança comuns, define critérios de versionamento para facilitar a evolução do esquema e inclui um processo de auto-governança para produtores e consumidores de logs de segurança. O código-fonte público do OCSF está hospedado em. GitHub

Esquema baseado em OCSF em AppFabric

AWS AppFabric Para segurança, o esquema baseado no OCSF 1.0.0-rc.3 é adaptado especificamente para atender às suas necessidades de observabilidade normalizada, consistente

e de baixo esforço de seu portfólio de software como serviço (SaaS). AppFabric, em colaboração com a comunidade de código aberto do OCSF, introduziu novas categorias de eventos, classes de eventos, atividades e objetos do OCSF para que o OCSF seja aplicável aos eventos de aplicativos SaaS. AppFabric normaliza automaticamente os eventos de auditoria que recebe de aplicativos SaaS e entrega esses dados aos serviços Amazon Simple Storage Service (Amazon S3) ou Amazon Data Firehose em seu. Conta da AWS Para um destino do Amazon S3, você pode escolher entre duas opções de normalização (OCSF ou Raw) e duas opções de formato de dados (JSON ou Parquet). Ao entregar para o Firehose, você também pode escolher entre duas opções de normalização (OCSF ou Raw), mas o formato dos dados é limitado ao JSON.

Categorias de eventos e classes do OCSF

AppFabric usa as duas categorias de eventos do OCSF a seguir:

- Identity and Access Management — AppFabric para fins de segurança, usa as seguintes classes de eventos dentro dessa categoria:
  - Alteração de conta
  - Autenticação
  - Gerenciamento de acesso de usuários
  - Gerenciamento de grupos
- Atividade do aplicativo — AppFabric para fins de segurança, usa as seguintes classes de eventos dentro dessa categoria:
  - Atividade de recursos da Web
  - Atividade de acesso a recursos da Web

Pré-requisitos e recomendações

Se você for um AWS cliente novo, preencha os pré-requisitos de configuração listados nesta página antes de começar a usar AWS AppFabric para fins de segurança. Para esses procedimentos de configuração, utilize o serviço do AWS Identity and Access Management (IAM). Para obter informações completas sobre o IAM, consulte o Guia do usuário do IAM.

Tópicos

- Inscreva-se para um Conta da AWS
- Criar um usuário com acesso administrativo
- (Obrigatório) Concluir os pré-requisitos do aplicativo

- (Opcional) Crie um local de saída
- (Opcional) Crie uma AWS KMS chave

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário raiz.

Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use o URL de login que foi enviado ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

(Obrigatório) Concluir os pré-requisitos do aplicativo

AppFabric Para usar como segurança o recebimento de informações do usuário e registros de auditoria dos aplicativos, muitos aplicativos exigem que você tenha tipos específicos de funções e planos. Verifique se você revisou os pré-requisitos de segurança de cada aplicativo que deseja autorizar e se tem os planos e funções adequados. AppFabric Para obter mais informações sobre os pré-requisitos específicos do aplicativo, consulte Aplicativos compatíveis ou escolha um dos seguintes tópicos específicos do aplicativo.

- 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) Crie um local de saída

AppFabric para fins de segurança, oferece suporte ao Amazon Simple Storage Service (Amazon S3) e ao Amazon Data Firehose como destinos de ingestão de registros de auditoria.

Amazon S3

Você pode criar um novo bucket do Amazon S3 usando o AppFabric console ao criar um destino de ingestão. Você também pode criar um bucket usando o serviço do Amazon S3. Se você optar por criar seu bucket usando o serviço Amazon S3, deverá criar o bucket antes de criar o destino de AppFabric ingestão e, em seguida, selecionar o bucket ao criar o destino de ingestão. Você pode optar por usar um bucket Amazon S3 existente no seu Conta da AWS, desde que ele atenda aos seguintes requisitos para buckets existentes:

- AppFabric para fins de segurança, é necessário que seu bucket do Amazon S3 esteja nos Região da AWS mesmos recursos do Amazon S3.
- Você pode criptografar seu bucket usando uma das seguintes opções:
  - Criptografia do lado do servidor com chaves gerenciadas pelo Amazon S3 (SSE-S3)
  - Criptografia do lado do servidor com chaves AWS Key Management Service (AWS KMS) (SSE-KMS) usando o padrão (). Chave gerenciada pela AWS `aws/s3`

Amazon Data Firehose

Você pode optar por usar o Amazon Data Firehose como seu destino de ingestão AppFabric para dados de segurança. Para usar o Firehose, você pode criar o stream de entrega do Firehose no seu Conta da AWS antes de criar uma ingestão ou enquanto estiver criando um destino de ingestão em. AppFabric Você pode criar um stream de entrega do Firehose usando o AWS Management Console, AWS CLI, ou as AWS APIs ou SDKs. Para obter instruções de configuração de stream, consulte os tópicos a seguir:

- AWS Management Console instruções — Criação de um stream de entrega do Amazon Data Firehose no Guia do desenvolvedor do Amazon Data Firehose
- AWS CLI instruções — create-delivery-streamna Referência de AWS CLI Comandos
- AWS Instruções de APIs e SDKs — CreateDeliveryStreamna referência de API do Amazon Data Firehose

Os requisitos ao usar o Amazon Data Firehose como destino de saída AppFabric de segurança são os seguintes:

- Você deve criar o fluxo da Região da AWS mesma forma que o seu AppFabric para recursos de segurança.
- Você deve selecionar Direct PUT como fonte.
- Anexe a política AmazonKinesisFirehoseFullAccess AWS gerenciada ao seu usuário ou anexe as seguintes permissões ao seu usuário:

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

O Firehose oferece suporte à integração com uma variedade de ferramentas de segurança de terceiros, como e. Splunk Logz.io Para obter informações sobre como configurar adequadamente o Amazon Kinesis para que ele envie dados para essas ferramentas, consulte Configurações de destino no Guia do desenvolvedor do Amazon Data Firehose.

(Opcional) Crie uma AWS KMS chave

No processo de criação de um pacote AppFabric de aplicativos de segurança, você selecionará ou configurará uma chave de criptografia para proteger com segurança seus dados de todos os aplicativos autorizados. Essa chave será usada para criptografar seus dados no AppFabric serviço.

AppFabric por segurança, criptografa os dados por padrão. AppFabric para fins de segurança, pode usar uma chave Chave pertencente à AWS criada e gerenciada por AppFabric em seu nome ou uma

chave gerenciada pelo cliente que você cria e gerencia em AWS Key Management Service (AWS KMS). Chaves pertencentes à AWS são uma coleção de AWS KMS chaves que um AWS service (Serviço da AWS) possui e gerencia para uso em várias Contas da AWS. As chaves gerenciadas pelo cliente são AWS KMS chaves Conta da AWS que você cria, possui e gerencia. Para obter mais informações sobre Chaves pertencentes à AWS chaves gerenciadas pelo cliente, consulte Chaves e AWS chaves do cliente no Guia do AWS Key Management Service desenvolvedor.

Se você quiser usar uma chave gerenciada pelo cliente para criptografar seus dados, como tokens de autorização, AppFabric por segurança, você pode criar uma com AWS KMS. Para obter mais informações sobre a política de permissões que concede acesso à sua chave gerenciada pelo cliente AWS KMS, consulte a seção Política de chaves deste guia.

Introdução AWS AppFabric à segurança

AWS AppFabric Para começar a usar a segurança, você deve primeiro criar um pacote de aplicativos e depois autorizar e conectar os aplicativos ao seu pacote de aplicativos. Depois que as autorizações do aplicativo forem conectadas aos aplicativos, você poderá usá-las AppFabric para recursos de segurança, como ingestão de registros de auditoria e acesso de usuários.

Esta seção explica como começar a usar AppFabric no AWS Management Console.

Tópicos

- Pré-requisitos
- Etapa 1: criar um pacote de aplicativos
- Etapa 2: autorizar aplicativos
- Etapa 3: configurar a ingestão de logs de auditoria
- Etapa 4: usar a ferramenta de acesso do usuário
- Etapa 5: Conecte-se AppFabric para obter dados de segurança em ferramentas de segurança e outros destinos

Pré-requisitos

Antes de começar, você deve primeiro criar um Conta da AWS e um usuário administrativo. Para obter mais informações, consulte Inscreva-se para um Conta da AWS e Criar um usuário com acesso administrativo.

Etapa 1: criar um pacote de aplicativos

Um pacote de aplicativos armazena todas as suas autorizações e AppFabric ingestões de aplicativos para fins de segurança. Para criar um pacote de aplicativos, você configura uma chave de criptografia para proteger com segurança os dados do aplicativo autorizado.

1. Abra o AppFabric console em https://console.aws.amazon.com/appfabric/.
2. No seletor Selecionar uma região no canto superior direito da página, selecione um. Região da AWS AppFabric está disponível somente nas regiões Leste dos EUA (Norte da Virgínia), Europa (Irlanda) e Ásia-Pacífico (Tóquio).
3. Escolha Conceitos básicos.
4. Na página Conceitos básicos, vá para a Etapa 1. Criar um pacote de aplicativos, escolha Criar pacote de aplicativos.
5. Na seção Criptografia, configure uma chave de criptografia para proteger com segurança seus dados de todos os aplicativos autorizados. Essa chave é usada para criptografar seus dados no serviço AppFabric de segurança.

   AppFabric por segurança, criptografa os dados por padrão. AppFabric pode usar uma chave Chave pertencente à AWS criada e gerenciada por AppFabric em seu nome ou uma chave gerenciada pelo cliente que você cria e gerencia em AWS Key Management Service (AWS KMS).
6. Para a Chave do AWS KMS , escolha Usar Chave pertencente à AWS ou Chave gerenciada pelo cliente.

   Se você optar por usar uma chave gerenciada pelo cliente, insira o Nome do recurso da Amazon (ARN) ou a ID da chave existente que você deseja usar, ou escolha Criar uma chave AWS KMS

   Considere o seguinte ao escolher uma chave gerenciada pelo cliente Chave pertencente à AWS ou uma chave gerenciada pelo cliente:

   - Chaves pertencentes à AWSsão uma coleção de chaves AWS Key Management Service (AWS KMS) que um AWS service (Serviço da AWS) possui e gerencia para uso em várias Contas da AWS. Embora não Chaves pertencentes à AWS estejam na sua Conta da AWS, um AWS service (Serviço da AWS) homem pode usar um Chave pertencente à AWS para proteger os recursos da sua conta. Chaves pertencentes à AWS não conte com as AWS KMS cotas da sua conta. Você não precisa criar ou manter a chave ou sua política de chave. A

rotação de Chaves pertencentes à AWS varia entre os serviços. Para obter informações sobre a rotação de um Chave pertencente à AWS for AppFabric, consulte Criptografia em repouso.

- As chaves gerenciadas pelo cliente são chaves KMS Conta da AWS que você cria, possui e gerencia. Você tem controle total sobre essas AWS KMS chaves. Você pode stabelecer e manter políticas de chaves, políticas AWS Identity and Access Management (IAM) e concessões. Você pode ativá-los e desativá-los, girar seu material criptográfico, adicionar tags, criar aliases que se referem às AWS KMS chaves e programar a exclusão das AWS KMS chaves. As chaves gerenciadas pelo cliente aparecem na página Chaves gerenciadas AWS Management Console pelo cliente do formulário AWS KMS.

  Para identificar definitivamente uma chave gerenciada pelo cliente, use a operação `DescribeKey`. Para chaves gerenciadas pelo cliente, o valor do campo `KeyManager` da resposta `DescribeKey` é `CUSTOMER`. Você pode usar sua chave gerenciada pelo cliente em operações criptográficas e auditar o uso em AWS CloudTrail registros. Com muitas Serviços da AWS que se integram AWS KMS, você pode especificar uma chave gerenciada pelo cliente para proteger os dados armazenados e gerenciados para você. As chaves gerenciadas pelo cliente têm uma taxa mensal e uma taxa pelo uso que exceda o nível AWS gratuito. As chaves gerenciadas pelo cliente são contabilizadas nas AWS KMS cotas da sua conta.

Para obter mais informações sobre Chaves pertencentes à AWS chaves gerenciadas pelo cliente, consulte Chaves e AWS chaves do cliente no Guia do AWS Key Management Service desenvolvedor.

> **Note**
>
> Quando um pacote de aplicativos é criado, AppFabric por segurança, também cria uma função especial do IAM em sua Conta da AWS chamada função vinculada ao serviço (SLR) para. AppFabric Ele permite que o serviço envie métricas para a Amazon CloudWatch. Depois de adicionar um destino de log de auditoria, a SLR permite que o serviço AppFabric de segurança acesse seus recursos da AWS (buckets do Amazon S3, fluxos de entrega do Amazon Data Firehose). Para ter mais informações, consulte Usar funções vinculadas ao serviço do AppFabric.

7. (Opcional) Para Tags, você tem a opção de adicionar tags ao seu pacote de aplicativos. As tags são pares de chave-valor que atribuem metadados a recursos que você cria. Para obter mais informações, consulte Como marcar seus AWS recursos no Guia do usuário do AWS Tag Editor.
8. Para criar um pacote de aplicativos, escolha Criar pacote de aplicativos.

Etapa 2: autorizar aplicativos

Depois que seu pacote de aplicativos for criado com sucesso, agora você pode autorizar a segurança AppFabric a se conectar e interagir com cada um dos seus aplicativos. Os aplicativos autorizados são criptografados e armazenados em seu pacote de aplicativos. Para configurar várias autorizações de aplicativos por pacote de aplicativos, repita a etapa de autorização do aplicativo conforme necessário para cada aplicativo.

Antes de iniciar as etapas para autorizar aplicações, revise e verifique os pré-requisitos de cada aplicação, como o tipo de plano necessário, em Aplicações compatíveis.

1. Na página Conceitos básicos, vá para a Etapa 2. Autorizar aplicativos, escolha Criar autorização de aplicativo.
2. Na seção Autorização do aplicativo, selecione o aplicativo ao qual você deseja conceder permissão de segurança AppFabric para se conectar no menu suspenso Aplicativo. Os aplicativos mostrados são aqueles que atualmente são suportados AppFabric por motivos de segurança.
3. Quando você seleciona um aplicativo, os campos obrigatórios de informações são exibidos. Esses campos incluem ID e nome do locatário e também podem incluir ID do cliente, segredo do cliente ou token de acesso pessoal. Os valores de entrada para esses campos variam de acordo com o aplicativo. Para obter instruções detalhadas específicas do aplicativo sobre como encontrar esses valores, consulte Aplicações compatíveis.
4. (Opcional) Para Tags, você tem a opção de adicionar tags à sua autorização de aplicativos. As tags são pares de chave-valor que atribuem metadados a recursos que você cria. Para obter mais informações, consulte Como marcar seus AWS recursos no Guia do usuário do AWS Tag Editor.
5. Escolha Criar autorizações de aplicativo.
6. Se uma janela pop-up for exibida (dependendo do aplicativo que está sendo conectado), selecione Permitir autorização AppFabric para que a segurança se conecte ao seu aplicativo.

   Se a autorização do seu aplicativo for bem-sucedida, você verá uma mensagem de sucesso da Autorização do aplicativo conectado na página de Conceitos básicos.
7. Você pode verificar o status da autorização do seu aplicativo a qualquer momento na página Autorizações de aplicativos listada no painel de navegação, sob o Status de cada aplicativo. Um status Conectado significa que a autorização do seu aplicativo foi concedida AppFabric para fins de segurança para se conectar ao aplicativo e está concluída.

8. Os possíveis status de autorização do aplicativo são mostrados na tabela a seguir, incluindo as etapas de solução de problemas que você pode seguir para corrigir erros relacionados.

Nome do status	Descrição do status	Etapas de solução de problemas
Pendente	O status Pendente significa que uma autorização de aplicativo para o aplicativo foi criada, mas, AppFabric por motivos de segurança, ainda não está conectada ao aplicativo.	Ao ver esse status, selecione Conectar no menu suspenso Ações da página de Autorização de aplicativos para iniciar uma conexão. Se esse erro persistir, verifique se o bloqueador de pop-ups do seu navegador está desativado. Se houver alguma mensagem de erro, como 400 Bad Request na janela pop-up, verifique se todas as informações, como ID do locatário, ID do cliente e segredo do cliente, foram inseridas corretame nte. Também é possível que a autorizaçã do aplicativ o não tenha sido criada corretamente. Para obter mais informações, consulte Aplicativos compatíveis.
Falha na validação da conexão	Um status de falha na validação da conexão significa que, AppFabric por segurança, não é possível validar a conexão da autorização do aplicativo com um aplicativo.	Verifique se todas as informações, como ID do locatário, ID do cliente e segredo do cliente, foram inseridas corretamente para a autorização de aplicativos.

Nome do status	Descrição do status	Etapas de solução de problemas
Falha na rotação automática do token	Um status de falha na rotação automática do token significa que o token de atualização do OAuth falhou depois que a autorização de aplicativos foi conectada com sucesso.	Se esse erro persistir, verifique o aplicativo de autenticação de aplicativos. Para obter mais informaçõ es, consulte Aplicativos compatíveis.

9. Para autorizar aplicativos adicionais, repita as etapas de 1 a 8 conforme necessário.

Etapa 3: configurar a ingestão de logs de auditoria

Depois de criar pelo menos uma autorização de aplicativos no seu pacote de aplicativos, agora você pode configurar uma ingestão de logs de auditoria. A ingestão de logs de auditoria consome logs de auditoria de um aplicativo autorizado e os normaliza no Open Cybersecurity Schema Framework (OCSF). Em seguida, ele os entrega a um ou mais destinos no AWS. Você também pode optar por entregar arquivos raw JSON aos seus destinos.

1. Na página Conceitos básicos, vá para a Etapa 3. Seção Configurar ingestões de logs de auditoria e selecione Configuração rápida de ingestões.

> **Note**
>
> Para uma configuração mais rápida, use a página de Configuração rápida de ingestões, acessível somente na página Conceitos básicos, para criar ingestões para várias autorizações de aplicativos ao mesmo tempo, com o mesmo destino de ingestão. Por exemplo, o mesmo bucket do Amazon S3 ou o mesmo stream de dados do Amazon Data Firehose.
>
> Você também pode criar ingestões na página Ingestões, acessível a partir do painel de navegação. Na página Ingestões, você pode configurar uma ingestão por vez para destinos distintos. Na página Ingestões, você também pode criar uma tag para uma ingestão. As instruções a seguir são para a página de Configuração rápida de ingestões.

2. Em Selecionar autorizações de aplicativos, selecione as autorizações de aplicativos para as quais você deseja criar uma ingestão de logs de auditoria. Os nomes dos inquilinos que

aparecem no menu suspenso Autorizações de aplicativos são os nomes dos inquilinos dos aplicativos para os quais você criou anteriormente uma autorização de aplicativo por motivos de segurança. AppFabric

3. Em Adicionar destino, selecione um destino para as ingestões do log de auditoria dos aplicativos que você selecionou. As opções de destino incluem Amazon S3 — Existing Bucket, Amazon S3 — New Bucket ou Amazon Data Firehose. Se você selecionar vários nomes de locatários, o destino escolhido será aplicado a cada ingestão de uma autorização de aplicativo.
4. Quando você escolhe um destino, campos obrigatórios adicionais aparecem.

   a. Se você escolher Amazon S3 — Novo bucket como destino, deverá inserir o nome do bucket do S3 que deseja criar. Para obter mais instruções sobre como criar um bucket do Amazon S3, consulte Criar um destino de saída.

   b. Se você escolher Amazon S3 — Bucket existente como destino, deverá inserir o nome do bucket do S3 que deseja usar.

   c. Se você escolher o Amazon Data Firehose como seu destino, selecione o nome do stream de entrega na lista suspensa do nome do stream de entrega do Firehose. Para obter mais instruções sobre como criar um stream de entrega do Amazon Data Firehose, consulte Criar um destino de saída e anote a política de permissões necessária AppFabric para fins de segurança.

5. Para Schema & Format, você pode optar por armazenar seus registros de auditoria em Raw - JSON, OCSF - JSON, OCSF - para buckets Amazon S3 ou Raw - JSON ou OCSF-JSON Parquet para Firehose.

   O formato de dados raw fornece seus dados de log de auditoria convertidos em JSON a partir de uma sequência de dados. O formato de dados OCSF normaliza seus dados de log de auditoria AppFabric para o esquema Open Cybersecurity Schema Framework (OCSF) para segurança. Para obter mais informações sobre como AppFabric usa o OCSF, consulte. Open Cybersecurity Schema Framework Você pode selecionar somente um esquema e um tipo de dados de formato por vez para uma ingestão. Se quiser adicionar um esquema adicional e um tipo de dados de formato, você pode configurar um destino de ingestão adicional repetindo o processo de criação da ingestão.

6. (Opcional) Se você quiser adicionar uma tag a uma ingestão, acesse a página Ingestões no painel de navegação. Para acessar a página de detalhes da ingestão, selecione o nome do locatário. Para Tags, você tem a opção de adicionar tags à sua ingestão. As tags são pares de chave-valor que atribuem metadados a recursos que você cria. Para obter mais informações, consulte Como marcar seus AWS recursos no Guia do usuário do AWS Tag Editor.

7. Escolha Configurar ingestões.

   Ao configurar com sucesso uma ingestão, você verá uma mensagem de sucesso da Ingestão criada na página Conceitos básicos.

8. Você também pode verificar o estado de suas ingestões e o status de seus destinos de ingestão a qualquer momento na página Ingestões do painel de navegação. Nessa página, você pode ver o nome do locatário criado ao criar a autorização do aplicativo, o destino e o estado de suas ingestões. Um estado de Ativado para sua ingestão significa que sua ingestão está ativada. Se você escolher o nome do locatário de uma autorização de aplicativo nessa página, poderá ver uma página de detalhes dessa autorização de aplicativo, incluindo detalhes e status do destino. O status Ativo para seu destino de ingestão significa que o destino está configurado corretamente e ativo. Se a autorização do aplicativo tiver o status Conectado e o status do destino da ingestão for Ativo, o log de auditoria deverá ser processado e entregue. Se o status de autorização do aplicativo ou o status do destino da ingestão forem qualquer um dos estados de falha, o log de auditoria não será processado nem entregue, mesmo que o status de ingestão esteja ativado. Para corrigir uma falha na autorização do aplicativo, consulte a Etapa 2. Autorizar aplicativos.

9. Os possíveis status de ingestão e destino da ingestão são mostrados na tabela a seguir, com etapas de solução de problemas que você pode seguir para corrigir qualquer status de erro.

Nome do estado ou status	Descrição	Etapas de solução de problemas
Disabled (Desativado)	Um estado Desativado para a ingestão significa que sua ingestão está desativada.	Você pode ativar a ingestão selecionando Ativar no menu suspenso Ações da página Ingestões.
Com falha	Um estado Com falha para o destino da ingestão significa que o destino da ingestão não está aceitando o log de auditoria. Por exemplo, esse status pode ocorrer devido a um local de armazenamento completo.	Para corrigir esses problemas, acesse os consoles Amazon S3 ou Firehose.

Etapa 4: usar a ferramenta de acesso do usuário

Usando a ferramenta de acesso do usuário AppFabric para segurança, as equipes de segurança e administração de TI podem ver rapidamente quem tem acesso a aplicativos específicos executando uma pesquisa simples usando o endereço de e-mail corporativo do funcionário. Essa abordagem pode ser útil para reduzir o tempo gasto em tarefas como desprovisionamento de usuários, que podem exigir verificação ou auditoria manual do acesso de um usuário em aplicativos SaaS. Se um usuário for encontrado, AppFabric por segurança, fornece o nome do usuário no aplicativo e seu status de usuário no aplicativo (por exemplo, Ativo), se fornecido pelo aplicativo. AppFabric para fins de segurança, pesquisa todos os aplicativos autorizados em um pacote de aplicativos para retornar uma lista dos aplicativos aos quais o usuário tem acesso.

1. Na página Conceitos básicos, vá para a Etapa 4. Usar a ferramenta de acesso do usuário e escolha Pesquisar usuário.
2. No campo Endereço de e-mail, digite o endereço de e-mail do usuário e escolha Pesquisar.
3. Na seção Resultados da pesquisa, você vê uma lista de todos os aplicativos autorizados aos quais o usuário tem acesso. Para mostrar o nome do usuário no aplicativo e seu status (se disponível), selecione um resultado da pesquisa.
4. Uma mensagem de Usuário encontrado na coluna de resultados da pesquisa significa que o usuário pode acessar o aplicativo listado. A tabela a seguir mostra os possíveis resultados da pesquisa, os erros e as ações que você pode tomar para solucioná-los.

Resultado da pesquisa	Descrição
O usuário não foi encontrado	Nenhum usuário foi encontrado com o endereço de e-mail usado.
Um token de autorização não foi encontrado. Conecte a autorização de aplicativos para o aplicativo.	Verifique se todas as informações, como ID do locatário, ID do cliente e segredo do cliente, foram inseridas corretamente para a autorização de aplicativos.
O token de autorização foi revogado. Conecte a autorização de aplicativos para o aplicativo.	Verifique se todas as informações, como ID do locatário, ID do cliente e segredo do cliente, foram inseridas corretamente para a autorização de aplicativos.

Resultado da pesquisa	Descrição
Não foi possível fazer a rotação do token de autorização. Conecte a autorização de aplicativos para o aplicativo.	O token de atualização do OAuth falhou depois que a autorização do aplicativo foi conectada com sucesso. Se esse erro persistir, verifique o aplicativo de autenticação de aplicativos. Para obter mais informações, consulte Aplicativos compatíveis.
As permissões necessárias não foram encontradas. Conecte a autorização de aplicativos para o aplicativo.	Verifique se todas as informações, como ID do locatário, ID do cliente e segredo do cliente, foram inseridas corretamente para a autorização de aplicativos.
A autorização do aplicativo não é válida.	Verifique se todas as informações, como ID do locatário, ID do cliente e segredo do cliente, foram inseridas corretamente para a autorização de aplicativos.
Não foi possível chamar a API do aplicativo devido a permissões insuficientes.	Verifique se todas as informações, como ID do locatário, ID do cliente e segredo do cliente, foram inseridas corretamente para a autorização de aplicativos.
O limite de solicitação do aplicativo foi excedido.	Essa é uma mensagem de erro recebida do aplicativo. Você pode tentar pesquisar um endereço de e-mail mais tarde.
O aplicativo encontrou um erro interno do servidor	Essa é uma mensagem de erro recebida do aplicativo. Você pode tentar pesquisar um endereço de e-mail mais tarde.
O aplicativo encontrou um erro de gateway incorreto	Essa é uma mensagem de erro recebida do aplicativo. Você pode tentar pesquisar um endereço de e-mail mais tarde.

Resultado da pesquisa	Descrição
O aplicativo não está pronto para lidar com a solicitação	Essa é uma mensagem de erro recebida do aplicativo. Você pode tentar pesquisar um endereço de e-mail mais tarde.
O aplicativo encontrou um erro de solicitação incorreta.	Essa é uma mensagem de erro que recebemos do aplicativo. Você pode tentar pesquisar um e-mail novamente mais tarde.
O aplicativo encontrou um erro de serviço indisponível.	Essa é uma mensagem de erro que recebemos do aplicativo. Você pode tentar pesquisar um e-mail novamente mais tarde.

Etapa 5: Conecte-se AppFabric para obter dados de segurança em ferramentas de segurança e outros destinos

Os dados normalizados (ou brutos) do AppFabric aplicativo são compatíveis com qualquer ferramenta que ofereça suporte à ingestão de dados do Amazon S3 e à integração com o Firehose, incluindo ferramentas de segurança Barracuda XDR como,,,Dynatrace,,, Splunk e Logz.io Netskope NetWitnessRapid7, ou sua solução de segurança proprietária. Para obter dados normalizados (ou brutos) do aplicativo AppFabric, siga as etapas anteriores de 1 a 3. Para obter mais detalhes sobre como configurar ferramentas e serviços de segurança específicos, consulte Ferramentas e serviços de segurança compatíveis.

Aplicações compatíveis

AWS AppFabric para segurança, suporta a integração com os seguintes aplicativos. Escolha o nome de um aplicativo para obter mais informações sobre como configurar a segurança AppFabric para se conectar a ele.

Tópicos

- 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

1Passwordé um gerenciador de senhas que ajuda você a criar, armazenar e usar senhas fortes para todas as suas contas online. Ele também protege seus dados com criptografia, alerta sobre violações e permite que você compartilhe senhas.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuário1Password, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para 1Password
- Conectando-se AppFabric à sua 1Password conta

AppFabric suporte para 1Password

AppFabric suporta o recebimento de informações do usuário e registros de auditoria do1Password.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria 1Password de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter um plano de assinatura 1Password Business ou Enterprise pago ativo. Para obter mais informações, consulte 1PasswordEnterprise no 1Password site.
- Você deve ter uma função de administrador ou proprietário da equipe na 1Password conta. Para obter mais informações, consulte Grupos no site de 1Password suporte.

Considerações sobre limites de taxa

A API de 1Password AuditLog eventos limita as solicitações a 600 por minuto e até 30.000 por hora. Exceder esses limites retorna um erro. Para obter mais informações, consulte Limites de taxa de 1Password API na referência da API de 1Password eventos.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como

às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua 1Password conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. 1Password Para encontrar as informações necessárias para autorizar 1Password AppFabric, use as etapas a seguir.

Crie um token de 1Password acesso pessoal

1Passwordsuporta tokens de acesso pessoal para clientes públicos. Conclua as etapas a seguir para gerar um token de acesso pessoal.

1. Faça login na sua conta da 1Password.
2. Escolha Integrações no painel de navegação.
3. Se as integrações existentes estiverem presentes, escolha Diretório. Caso contrário, siga para a próxima etapa.
4. Escolha Outro em Integração de relatórios de eventos.
5. Na página Adicionar integração, insira o nome do sistema de gerenciamento de eventos e informações de segurança (SIEM) (por exemplo, AppFabric Seguro)
6. Escolha Adicionar integração e conclua as etapas a seguir na página Configurar token.
    a. Forneça o nome do token a ser usado no ambiente AppFabric seguro.
    b. Recomendamos que você escolha Nunca na lista suspensa Expira depois. Se qualquer outro valor for selecionado, o token será 1Password revogado após o término do prazo de expiração.
    c. Na seção Eventos a serem relatados, escolha Tentativas de login, Eventos de uso do item e Eventos de auditoria.
7. Escolha Emitir token para criar o token.
8. Escolha Salvar em 1Password e conclua as etapas a seguir.
    a. O título será preenchido automaticamente com base nos nomes do sistema e do token.
    b. Escolha Privado em Selecionar um cofre.
    c. Escolha Salvar.

Para obter mais informações, consulte Introdução aos relatórios de 1Password eventos no 1Password site.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do inquilino AppFabric será seu endereço de 1Password login. Conclua as etapas a seguir para encontrar seu ID de inquilino.

1. Faça login na sua conta da 1Password.
2. Selecione Configurações no painel de navegação.
3. Seu 1Password login está listado na página. Por exemplo, example-account.1password.com.

Nome do locatário

Insira um nome que identifique essa 1Password organização exclusiva. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

Token de contas de serviço

Você deve ter um token de conta de serviço de uma conta de 1Password serviço para entrar na autorização do AppFabric 1Password aplicativo. Se você ainda não tem um token de conta de serviço, siga estas instruções:

AppFabric solicitará um token de conta de serviço. O token da conta de serviço AppFabric é o token de acesso pessoal que você criou. Conclua as etapas a seguir no portal do 1Password para encontrar o token de acesso pessoal.

1. Escolha Dashboard.
2. Escolha Pessoas.
3. Escolha o nome do proprietário da conta.
4. Selecione Private (Privado).
5. Escolha Exibir cofre.
6. Escolha o nome do token.

Autorização do cliente

Crie uma autorização de aplicativo AppFabric usando o ID do inquilino, o nome do inquilino e o token da conta de serviço. Em seguida, escolha Connect para ativar a autorização.

Asana

Asana é uma plataforma de gerenciamento de trabalho que ajuda colaboradores, equipes e organizações a orquestrar suas atividades, desde tarefas diárias até iniciativas estratégicas multifuncionais. Fornece um sistema orgânico de clareza onde todos podem se comunicar, colaborar e coordenar o trabalho. Com o Asana, as equipes integram ferramentas de negócios essenciais em um só lugar para que o trabalho avance, não importa onde ele seja realizado.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioAsana, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Asana
- Conectando-se AppFabric à sua Asana conta

AppFabric suporte para Asana

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doAsana.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Asana de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter uma Conta empresarial com Asana. Para obter mais informações sobre como criar ou atualizar para uma Asana Conta empresarial, consulte Asana Empresa no Asana site.
- Você deve ter um usuário com o perfil de Super Administrador em sua conta do Asana. Para obter mais informações sobre perfis, consulte Perfis de administrador e super administrador no Asana, no site do Asana.

Considerações sobre limites de taxa

O Asana impõe limites de taxa na API do Asana. Para obter mais informações sobre os limites de taxas de API do Asana, consulte Limites de taxa no site Guia de desenvolvedores do Asana. Se a combinação de seus Asana aplicativos existentes AppFabric e seus aplicativos excederem o limite, os registros de auditoria que aparecem AppFabric podem ser atrasados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Asana conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Asana Para encontrar as informações necessárias para autorizar Asana AppFabric, use as etapas a seguir.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do inquilino em AppFabric é chamado de ID de domínio emAsana. Para encontrar a ID do domínio, siga estas instruções na tela inicial do Asana:

1. Escolha a foto do perfil da sua conta e selecione Console de administração.
2. Depois selecione Configurações.
3. Role até Configurações do domínio.
4. Insira o ID do domínio desta seção na configuração do ID do AppFabric locatário.

Nome do locatário

Insira um nome que identifique essa organização exclusiva do Asana. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

Token de contas de serviço

Você deve ter um token de conta de serviço de uma conta de Asana serviço para entrar na autorização do AppFabric Asana aplicativo. Se você ainda não tem um token de conta de serviço, siga estas instruções:

1. Para criar uma conta de serviço, siga as instruções em Contas de serviço no site do Guia do Asana.
2. Copie e salve o token disponível na parte inferior da página Adicionar conta de serviço na primeira vez que você visualizar a página Adicionar conta de serviço.
3. Se fechar a página Adicionar conta de serviço antes de salvar o token, você deverá editar sua conta de serviço, gerar um novo token e salvá-lo.

Azure Monitor

Azure Monitoré uma solução de monitoramento abrangente para coletar, analisar e responder aos dados de monitoramento de seus ambientes locais e na nuvem. Você pode usar Azure Monitor para maximizar a disponibilidade e o desempenho de seus aplicativos e serviços. Ele ajuda você a entender o desempenho de seus aplicativos e permite que você responda manual e programaticamente aos eventos do sistema.

Azure Monitorcoleta e agrega os dados de cada camada e componente do seu sistema em várias assinaturas e inquilinos do Azure e não do Azure. Ele os armazena em uma plataforma de dados comum para consumo por um conjunto comum de ferramentas que podem correlacionar, analisar, visualizar e/ou responder aos dados. Você também pode integrar outras ferramentas da Microsoft e de outras empresas. O registro de Azure Monitor atividades é um registro da plataforma que fornece informações sobre eventos em nível de assinatura. O registro de atividades inclui informações como quando um recurso é modificado ou uma máquina virtual é iniciada.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioAzure Monitor, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Azure Monitor
- Conectando-se AppFabric à sua Azure Monitor conta

AppFabric suporte para Azure Monitor

AppFabric é capaz de receber informações do usuário e registros de auditoria dos seguintes Azure Monitor serviços:

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

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Azure Monitor de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você precisa ter uma Microsoft Azure conta com um teste gratuito ou uma pay-as-you-go assinatura.
- É necessária pelo menos uma assinatura para obter os eventos dentro dessa assinatura.

Considerações sobre limites de taxa

Azure Monitorimpõe limites de taxa ao responsável pela segurança (usuário ou aplicativo) que faz as solicitações e ao ID da assinatura ou ID do inquilino. Para obter mais informações sobre os limites de taxa da Azure Monitor API, consulte Entenda Azure Resource Manager como limitar as solicitações no site do Azure Monitordesenvolvedor.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Azure Monitor conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Azure Monitor Para encontrar as informações necessárias para autorizar Azure Monitor AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric integra-se ao Azure Monitor uso do OAuth2. Conclua as etapas a seguir para criar um aplicativo OAuth2 em: Azure Monitor

1. Navegue até o Microsoft AzurePortal e faça login.
2. Navegue até Microsoft EntraID.
3. Escolha Registros de aplicativos.
4. Escolha Novo registro.
5. Insira um nome para o cliente, como Cliente Azure Monitor OAuth. Esse será o nome do aplicativo registrado.
6. Verifique se os tipos de conta compatíveis estão definidos como Inquilino único.
7. Para o URI de redirecionamento, selecione Web como plataforma e adicione um URI de redirecionamento. Use o seguinte formato para o URI de redirecionamento:

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

   Nesse endereço, *<region>* está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

   A resposta de autenticação será enviada para o URI fornecido após a autenticação bem-sucedida do usuário. Fornecer isso agora é opcional e pode ser alterado posteriormente, mas um valor é necessário para a maioria dos cenários de autenticação.
8. Escolha Register.
9. No aplicativo registrado, escolha Certificados e segredos e depois Novo segredo do cliente.
10. Adicione uma descrição para o segredo.
11. Selecione a duração da expiração secreta. Você pode selecionar qualquer duração predefinida no menu suspenso ou definir uma duração personalizada.
12. Escolha Adicionar. Os valores secretos do cliente só podem ser visualizados imediatamente após a criação. Certifique-se de salvar o segredo em algum lugar seguro antes de sair da página.

Permissões obrigatórias

Você deve adicionar as seguintes permissões para seu aplicativo OAuth: Para adicionar permissões, siga as instruções na seção Adicionar permissões para acessar sua API da web do Guia do Microsoft Entra desenvolvedor.

- Microsoft GraphAPI de acesso do usuário > User.Read.All (selecione o tipo delegado)
- Microsoft GraphAPI de acesso do usuário > offline_access (selecione o tipo delegado)
- AzureAPI de log de auditoria do Service Management > user_impersonation (selecione o tipo delegado)

Depois de adicionar as permissões, para conceder o consentimento do administrador para as permissões, siga as instruções na seção Botão de consentimento do administrador do Guia do Microsoft Entra desenvolvedor.

Autorizações do aplicativo

AppFabric suporta o recebimento de informações do usuário e registros de auditoria da sua Azure Monitor conta. Para receber os registros de auditoria e os dados do usuárioAzure Monitor, você deve criar duas autorizações de aplicativos, uma nomeada Azure Monitorna lista suspensa de autorização do aplicativo e outra chamada Registros de Azure Monitor auditoria na lista suspensa de autorização do aplicativo. Você pode usar a mesma ID de locatário, ID do cliente e segredo do cliente para as autorizações do aplicativo. Para receber registros de auditoria, Azure Monitor você precisa das autorizações do aplicativo Azure Monitore do Azure MonitorAudit Logs. Para usar a ferramenta de acesso do usuário sozinha, somente a autorização do Azure Monitoraplicativo é necessária.

ID de locatário

AppFabric solicitará seu ID de inquilino. Conclua as etapas a seguir para encontrar sua ID de cliente no Azure Monitor:

1. Navegue até o Microsoft AzurePortal.
2. Navegue até o Azure Active Directory.
3. Na seção Registros de aplicativos, escolha o aplicativo que foi criado anteriormente.
4. Na seção Visão geral, copie a ID do inquilino do campo ID do diretório (inquilino).

Nome do locatário

Insira um nome que identifique essa Azure Monitor assinatura exclusiva. AppFabric usa o nome do inquilino para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

> **Note**
>
> O nome do inquilino deve ter no máximo 2.048 caracteres consistindo em números, letras maiúsculas/minúsculas e os seguintes caracteres especiais: ponto (.), sublinhado (_), traço (-) e espaço vazio.

ID de cliente

AppFabric solicitará um ID de cliente. Conclua o procedimento a seguir para encontrar seu ID de cliente emAzure Monitor:

1. Navegue até o Microsoft AzurePortal.
2. Navegue até o Azure Active Directory.
3. Na seção Registros de aplicativos, escolha o aplicativo que foi criado anteriormente.
4. Na seção Visão geral, copie a ID do cliente do campo ID do aplicativo (cliente).

Segredo do cliente

AppFabric solicitará um segredo do cliente. O segredo do cliente para o aplicativo OAuth registrado é o que você gerou na Etapa 11 da seção de criação do aplicativo OAuth. Se você perder o segredo do cliente gerado durante a criação do aplicativo OAuth, repita as etapas de 8 a 11 na seção de criação do aplicativo OAuth para regenerar um novo.

Autorização do aplicativo

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up Microsoft Azure para aprovar a autorização. Faça login na sua conta pela janela e aprove a AppFabric autorização escolhendo Permitir.

Atlassian Confluence

Crie, colabore e organize todo o seu trabalho em um só lugar. O Confluence é um espaço de trabalho em equipe onde o conhecimento e a colaboração se encontram. As páginas dinâmicas

oferecem à sua equipe um lugar para criar, capturar e colaborar em qualquer projeto ou ideia. Os espaços ajudam sua equipe a estruturar, organizar e compartilhar o trabalho, para que cada membro da equipe tenha visibilidade do conhecimento institucional e acesso às informações necessárias para fazer seu melhor trabalho. Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioConfluence, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Atlassian Confluence
- Conectando-se AppFabric à sua Atlassian Confluence conta

AppFabric suporte para Atlassian Confluence

AppFabric suporta o recebimento de registros de auditoria doAtlassian Confluence.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Atlassian Confluence de destinos compatíveis, você deve atender aos seguintes requisitos:

- Para acessar os logs de auditoria, você precisa ter uma conta padrão, premium ou corporativa. Para obter mais informações sobre a criação ou atualização para o tipo de plano aplicável do Confluence, consulte Definição de preços do Confluence no site do Atlassian.
- Para acessar os logs de auditoria corporativa, você precisa ter permissões de administrador em sua conta. Para obter mais informações sobre perfis, consulte Conceder permissões de administrador aos usuários no site de suporte do Atlassian.

Considerações sobre limites de taxa

O Confluence impõe limites de taxa na API do Atlassian Confluence. Se a combinação de seus aplicativos de Atlassian Confluence API existentes AppFabric e seus aplicativos Atlassian Confluence de API excederem os limites, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como

às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Atlassian Confluence conta

Depois de criar seu pacote de aplicativos no AppFabric serviço, você deve autorizar AppFabric com. Atlassian Confluence Para encontrar as informações necessárias para autorizar Atlassian Confluence AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Atlassian Confluence uso do OAuth. Para criar um aplicativo OAuth no Atlassian Confluence, siga as etapas abaixo:

1. Navegue até o Console do desenvolvedor do Atlassian.
2. Escolha o ícone do seu perfil no canto superior direito e escolha Console do desenvolvedor.
3. Ao lado de Meus aplicativos, escolha Criar, Integração do OAuth 2.0.
4. Escolha Permissões no painel de navegação à esquerda e escolha Adicionar ao lado da API do Confluence.
5. Em Escopos clássicos, selecione Ler usuário (`read:confluence-user`).
6. Em Escopos granulares, selecione Exibir logs de auditoria (`read:audit-log:confluence`).
7. Escolha Autorização no painel de navegação à esquerda e escolha Adicionar ao lado de OAuth 2.0 (3LO).
8. Use um URL com o formato a seguir na caixa de texto URL de retorno de chamada e escolha Salvar alterações.

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

   Nesse URL, <region>está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Escopos necessários

Você deve adicionar um dos escopos a seguir à sua aplicação OAuth do Atlassian Confluence. Para obter mais informações sobre escopos, consulte Escopos para aplicações OAuth 2.0 (3LO) e Forge no site do desenvolvedor do Atlassian. Use o escopo clássico quando disponível.

- Escopos clássicos:
  - `read:confluence-user`
- Escopos granulares:
  - `read:audit-log:confluence`

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do locatário em AppFabric é o subdomínio da sua Atlassian Confluence instância. Você pode encontrar seu subdomínio da instância do Atlassian Confluence na barra de endereço do seu navegador entre https:// e .atlassian.net.

Nome do locatário

Insira um nome que identifique essa organização exclusiva do Atlassian Confluence. AppFabric usa o nome do inquilino para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. Para encontrar sua ID de cliente no Atlassian Confluence, siga as etapas abaixo:

1. Navegue até o Console do desenvolvedor do Atlassian.
2. Escolha o ícone do seu perfil no canto superior direito e escolha Console do desenvolvedor, Minhas aplicações.
3. Selecione o aplicativo OAuth que você usa para se conectar. AppFabric
4. Insira a ID do cliente na página Configurações no campo ID do cliente em AppFabric.

Segredo do cliente

AppFabric solicitará um segredo do cliente. Para descobrir seu segredo do cliente no Atlassian Confluence, siga as etapas abaixo:

1. Navegue até o Console do desenvolvedor do Atlassian.
2. Escolha o ícone do seu perfil no canto superior direito e escolha Console do desenvolvedor, Minhas aplicações.
3. Selecione o aplicativo OAuth que você usa para se conectar. AppFabric
4. Insira o segredo da página Configurações no campo Segredo do cliente em AppFabric.

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up Atlassian Confluence para aprovar a autorização. Para aprovar a AppFabric autorização, escolha permitir.

Atlassian Jira suite

A Atlassian libera o potencial de todas as equipes. Seu software ágil e DevOps ágil de gerenciamento de serviços de TI e gerenciamento de trabalho ajuda as equipes a organizar, discutir e concluir o trabalho compartilhado. A maioria das empresas da Fortune 500 e mais de 240.000 empresas de todos os portes mundo afora, incluindo a NASA, Kiva, Deutsche Bank e Salesforce, confiam nas soluções da Atlassian para ajudar suas equipes a trabalharem melhor juntas e apresentarem resultados de qualidade no prazo. Saiba mais sobre os produtos da Atlassian, incluindo Jira Software, Confluence, Jira Service Management, Trello, Bitbucket e Jira Align em Atlassian.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuário do Jira suite (excetoJira Align), normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para o Jira suite
- Conectando-se AppFabric à sua Jira conta

AppFabric suporte para o Jira suite

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doJira suite, com exceção doJira Align.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria dos Jira suite destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter um plano Standard ou superior do Jira. Para obter mais informações sobre os recursos dos planos do Jira, consulte as páginas de preços de Software do Jira, Gestão de serviços do Jira, Gestão de trabalho do Jira e Descoberta de produtos do Jira.
- Você deve ter um usuário com o perfil de Administrador da organização em sua conta do Jira. Para obter mais informações sobre perfis, consulte Conceder permissões de administrador aos usuários no site de suporte do Atlassian.

Considerações sobre limites de taxa

O Jira impõe limites de taxa na API do Jira. Para obter mais informações sobre os limites de taxas de API do Jira suite, consulte Limitação de taxa no site Guia de desenvolvedores do Atlassian. Se a combinação de seus aplicativos de Jira API existentes AppFabric e seus aplicativos excederem o limite, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Jira conta

Depois de criar seu pacote de aplicativos no AppFabric serviço, você deve autorizar AppFabric com. Jira Para encontrar as informações necessárias para autorizar Jira AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Jira suite uso do OAuth. Para criar um aplicativo OAuth no Jira, siga as etapas abaixo:

1. Navegue até o Console do desenvolvedor do Atlassian.
2. Ao lado de Meus aplicativos, escolha Criar, Integração do OAuth 2.0.
3. Dê um nome para o aplicativo e escolha Criar.
4. Navegue até a seção Autorização e escolha Adicionar ao lado de OAuth 2.0.
5. Use um URL com o seguinte formato no campo URL de retorno de chamada e escolha Salvar alterações.

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

   Nesse URL, <region>está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
6. Navegue até a seção Configurações, copie o ID do cliente e o segredo do cliente e salve-os para usar na autorização do AppFabric aplicativo.

Escopos necessários

Você deve adicionar os seguintes escopos à página Permissões do seu aplicativo OAuth do Jira:

- Em escopos clássicos:
  - Jira API > `read:jira-user`
- Em escopos granulares:
  - Jira API > `read:audit-log:jira`
  - Jira API > `read:user:jira`

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do locatário em AppFabric é o subdomínio da sua Jira instância. Você pode encontrar seu subdomínio da instância do Jira na barra de endereço do seu navegador entre https:// e .atlassian.net.

Nome do locatário

Insira um nome que identifique esse Jira servidor exclusivo. AppFabricusa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará seu ID de cliente. Para encontrar sua ID de cliente no Jira, siga as etapas abaixo:

1. Navegue até o Console do desenvolvedor do Atlassian.
2. Selecione o aplicativo OAuth que você usa para se conectar. AppFabric
3. Insira a ID do cliente na página Configurações no campo ID do cliente em AppFabric.

Segredo do cliente

AppFabric solicitará o segredo do seu cliente. O segredo do cliente AppFabric é o segredo que entraJira. Para descobrir seu Segredo no Jira, siga as etapas abaixo:

1. Navegue até o Console do desenvolvedor do Atlassian.
2. Selecione o aplicativo OAuth que você usa para se conectar. AppFabric
3. Insira o segredo da página Configurações no campo Segredo do cliente em AppFabric.

Aprovar autorização

Depois de criar a autorização do aplicativo, AppFabric você receberá uma janela pop-up Jira para aprovar a autorização. Para aprovar a AppFabric autorização, escolha Permitir.

Box

Boxé a principal nuvem de conteúdo, uma plataforma única que capacita as organizações a gerenciar todo o ciclo de vida do conteúdo, trabalhar com segurança em qualquer lugar e integrar vários aplicativos. best-of-breed

Você pode usar AWS AppFabric para receber registros de auditoria e dados do usuárioBox, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para o Box
- Conectando-se AppFabric à sua Box conta

AppFabric suporte para o Box

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doBox.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Box de destinos compatíveis, você deve atender aos seguintes requisitos:

- Para acessar os registros de auditoria, você precisa ter uma assinatura paga ativa dos planos Business, Business Plus, Enterprise ou Enterprise Plus.
- Você deve ter um usuário com privilégios de administrador.
- Você deve ter a autenticação de dois fatores ativada em sua Box conta para visualizar e copiar o segredo do cliente do aplicativo na guia de configuração.

Considerações sobre limites de taxa

O Box impõe limites de taxa na API do Box. Para obter mais informações sobre os limites de taxa da Box API, consulte Limites de taxa no site do Box Developers Guide. Se a combinação de seus Box aplicativos existentes AppFabric e seus aplicativos excederem o limite, os registros de auditoria que aparecem AppFabric podem ser atrasados.

Considerações sobre o atraso de dados

Você pode ver um atraso de até 30 minutos em um evento de auditoria para ser entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizável em nível de conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Box conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você precisa AppFabric autorizar com. Box Para encontrar as informações necessárias para autorizar Box AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Box uso do OAuth. Use as etapas a seguir para criar um aplicativo OAuth em. Para obter mais informaçõesBox, consulte Criação de um aplicativo OAuth no site. Box

1. Faça login Box e acesse o Developer Console.
2. Selecione Create novo aplicativo.
3. Escolha Aplicativo personalizado na lista de tipos de aplicativos. Um modal aparecerá para solicitar uma seleção para a próxima etapa.
4. Insira o nome e a descrição do aplicativo.
5. Escolha Integração na lista suspensa Propósito.
    a. Escolha Segurança e conformidade na lista suspensa Categorias.
    b. Entre AWS AppFabric Secureno campo Com qual sistema externo você está se integrando? caixa de texto.
6. Escolha Autenticação do servidor (concessão de credenciais do cliente) se quiser verificar a identidade do aplicativo com uma ID e um segredo do cliente.
7. Escolha Criar aplicativo.
8. Escolha a guia Configuração.
9. Na seção Nível de acesso do aplicativo da página, escolha App + Enterprise Access.
10. Na seção Escopos da aplicação da página, escolha Gerenciar usuários e Gerenciar propriedades corporativas.
11. Escolha Salvar alterações.

    Um Box administrador precisa autorizar o aplicativo no Box Admin Console antes que o aplicativo possa ser usado. Conclua as etapas a seguir para solicitar uma autorização.
    a. Escolha a guia Autorização para seu aplicativo no Developer Console.
    b. Escolha Revisar e Enviar para enviar um e-mail ao administrador Box da sua empresa para aprovação. Para obter mais informações, consulte Autorização no Boxguia.

> **Note**
>
> Você deve reenviar seu aplicativo se alguma alteração for feita após o envio.

Escopos necessários

Os seguintes escopos de aplicação são obrigatórios. Para obter mais informações sobre escopos, consulte o site de documentação do Scopes on the Box.

- Gerenciar propriedades corporativas (`manage_enterprise_properties`)
- Gerenciar usuários (`manage_managed_users`)

Autorizações do aplicativo

ID de locatário

AppFabric solicitará um ID de inquilino. A ID do inquilino AppFabric é a Box Enterprise ID. A Box Enterprise ID pode ser encontrada no console do administrador em Conta e faturamento > Informações da conta > ID corporativa. Para obter mais informações, consulte o site de documentação do Enterprise ID on the Box.

Nome do locatário

Insira um nome que identifique essa organização exclusiva do Box. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e qualquer ingestão criada a partir da autorização do aplicativo.

ID e segredo do cliente

1. Faça login Box e acesse o Developer Console.
2. Escolha Meus aplicativos no menu de navegação.
3. Escolha o aplicativo OAuth que você usa para se conectar. AppFabric
4. Escolha a guia Configuração.
5. Role até a seção Credenciais do Oauth 2.0 da página.
6. Insira o ID do cliente do OAuth no campo ID do cliente em. AppFabric
7. Escolha Buscar segredo do cliente.
8. Insira o segredo do cliente do seu segredo do cliente OAuth no campo Segredo do cliente em. AppFabric

Cisco Duo

Cisco Duoprotege contra violações com um pacote líder de gerenciamento de acesso que fornece fortes defesas em várias camadas e recursos inovadores que permitem que usuários legítimos entrem e afastem os malfeitores. Para qualquer organização preocupada com violações e que precisa de uma solução Cisco Duo rápida, permite uma forte segurança e, ao mesmo tempo, melhora a produtividade do usuário. Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioCisco Duo, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Cisco Duo
- Conecte-se AppFabric à sua Cisco Duo conta

AppFabric suporte para Cisco Duo

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doCisco Duo.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Cisco Duo de destinos compatíveis, você deve atender aos seguintes requisitos:

- Para acessar os registros de auditoria, você precisa ter uma assinatura ativa das edições Duo Essentials, Duo Advantage ou Duo Premier. Como alternativa, novos clientes com um teste Advantage ou Premier também podem acessar. Para obter mais informações sobre Cisco Duo edições, consulte Edições e preços.
- Você precisa ser um administrador com função de proprietário para criar ou modificar a API de administrador.
- Você precisa adicionar as permissões “Grant read log resource” para acessar os registros de auditoria na API de administração.

Considerações sobre limites de taxa

O Cisco Duo impõe limites de taxa na API do Cisco Duo. Para obter mais informações sobre os limites de taxa da Cisco Duo API, consulte os limites de taxa em Registros de autenticação. Se a combinação de seus aplicativos de Cisco Duo API existentes AppFabric e seus aplicativos Cisco Duo

de API excederem os limites, os registros de auditoria que aparecem AppFabric podem ser adiados. Entre em contato com o Cisco Duo se precisar aumentar o limite de taxa.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conecte-se AppFabric à sua Cisco Duo conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Cisco Duo Para encontrar as informações necessárias para autorizar Cisco Duo AppFabric, use as etapas a seguir.

Crie um aplicativo Cisco Duo de API de administração

AppFabric se integra ao Cisco Duo uso de um token de serviço de API. Para criar um aplicativo emCisco Duo, use as etapas a seguir.

- Para criar um aplicativo da API Cisco Duo Admin, siga as instruções nas primeiras etapas da API Cisco Duo Admin.

Permissões obrigatórias

Você deve adicionar os seguintes escopos ao seu Cisco Duo aplicativo:

- Conceder registro de leitura
- Conceder recurso de leitura

Autorizações do aplicativo

ID de locatário

AppFabric solicitará um ID de inquilino. Você pode encontrar o ID do inquilino no nome do Cisco Duo host. Para encontrar o nome do host emCisco Duo, siga estas etapas.

1. Navegue até a página de login do Cisco Duo administrador e faça login.
2. Navegue até Aplicativos e escolha Proteger um aplicativo.

3. Localize a entrada da API Admin na lista de aplicativos e escolha Proteger na extrema direita para configurar seu aplicativo e obter o nome de host da API.
4. O nome do host da API é formatado como`api-<tenant-id>.duosecurity.com`, no qual *`<tenant-id>`* está o ID do locatário.

Nome do locatário

Insira um nome que identifique essa organização exclusiva do Cisco Duo. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

Token de serviço

AppFabric solicitará um token de serviço. O token de serviço é uma chave de integração separada por dois pontos e uma chave secreta com o seguinte formato.

```
integrationkey:secretkey
```

Para encontrar sua chave de integração e chave secretaCisco Duo, use as etapas a seguir.

1. Navegue até a página de login do Cisco Duo administrador e faça login.
2. Navegue até Aplicativos e escolha Proteger um aplicativo.
3. “Clique em Proteger um aplicativo e localize a entrada da API Admin na lista de aplicativos. Clique em Proteger na extrema direita para configurar o aplicativo. Role para baixo até a seção de escopos **`Grant read log`** e adicione e. **`Grant read resource`**

Dropbox

Dropbox ajuda sua organização a realizar um trabalho melhor com mais rapidez ao unir seu pessoal, não importa em que estejam trabalhando, onde estejam trabalhando ou que tipo de ferramentas estejam usando. Permite que os usuários acelerem a inovação e a eficiência fornecendo uma maneira simples e segura de compartilhar conteúdo. Dropbox é um lugar para manter a vida organizada e manter o trabalho em andamento. Com mais de 700 milhões de usuários registrados em 180 países, Dropbox tem a missão de criar uma forma mais esclarecida de trabalhar.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioDropbox, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF)

e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Dropbox
- Conectando-se AppFabric à sua Dropbox conta

AppFabric suporte para Dropbox

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doDropbox.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Dropbox de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter uma conta empresarial de Dropbox. Para obter mais informações sobre como criar ou atualizar para uma conta empresarial de Dropbox, consulte DropboxNegócios no site Dropbox.
- Você deve ter um usuário com o perfil de Administrador da equipe em sua conta do Dropbox. Para obter mais informações sobre funções, consulte Como alterar os direitos de administrador da sua Dropboxequipe no site da DropboxCentral de Ajuda.

Considerações sobre limites de taxa

O Dropbox impõe limites de taxa na API do Dropbox. Para obter mais informações sobre os limites de taxas de API do Dropbox, consulte Limites de taxa no site Guia de desempenho do Dropbox. Se a combinação de seus aplicativos de Dropbox API existentes AppFabric e seus aplicativos de API excederem o limite, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Dropbox conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Dropbox Para encontrar as informações necessárias para autorizar Dropbox AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Dropbox uso do OAuth. Para criar um aplicativo OAuth no Dropbox, siga estas etapas:

1. Escolha Criar aplicativo no Dropbox App Console em https://www.dropbox.com/developers/apps.
2. Na nova página de configuração do aplicativo, escolha Acesso com escopo para a API.
3. Em seguida, selecione Completo Dropbox para o tipo de acesso.
4. Nomeie seu aplicativo OAuth e escolha Criar aplicativo para concluir a configuração inicial do aplicativo OAuth.
5. Na página de informações do aplicativo, adicione um URL de redirecionamento com o seguinte formato no campo URIs de redirecionamento do OAuth2.

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

   Nesse URL, *<region>* está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
6. Escolha Adicionar.
7. Copie e salve a chave e o segredo do aplicativo para uso na autorização do AppFabric aplicativo.
8. Você pode deixar todos os outros campos na guia Configurações com seus valores padrão.

Escopos necessários

Você deve adicionar os seguintes escopos ao seu aplicativo Dropbox usando a guia Permissões na tela de informações do aplicativo:

- `account_info.read`
- `team_data.member`

- `events.read`
- `members.read`
- `team_info.read`

Escolha Enviar depois de terminar.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. Insira qualquer valor que identifique sua conta do Dropbox de forma exclusiva, como nome de equipe.

Nome do locatário

Insira um nome que identifique essa Dropbox conta exclusiva. AppFabricusa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. O ID do cliente AppFabric é a chave Dropbox do seu aplicativo. Para descobrir o segredo do aplicativo DropBox, siga estas etapas:

1. Navegue até o Dropbox App Console em https://www.dropbox.com/developers/apps.
2. Encontre o aplicativo que você usa para se conectar AppFabric.
3. Encontre a chave do aplicativo na seção Status da página de informações do aplicativo.
4. Insira a chave do Dropbox aplicativo no campo ID do cliente em AppFabric.

Segredo do cliente

AppFabric solicitará um segredo do cliente. O segredo do cliente AppFabric é o segredo Dropbox do seu aplicativo. Para descobrir o segredo do aplicativo Dropbox, siga estas etapas:

1. Navegue até o Dropbox App Console em https://www.dropbox.com/developers/apps.
2. Encontre o aplicativo que você usa para se conectar AppFabric.
3. Encontre a chave do aplicativo na seção Status da página de informações do aplicativo.

4. Insira o segredo do Dropbox aplicativo no campo Segredo do cliente em AppFabric.

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up Dropbox para aprovar a autorização. Para aprovar a AppFabric autorização, escolha Permitir.

Genesys Cloud

Genesys Cloudcria conversas fluidas em canais digitais e de voz em uma all-in-one interface fácil. Isso posiciona as empresas para fornecer experiências excepcionais para funcionários e clientes e colher os benefícios de implantações rápidas, complexidade reduzida e administração simples. Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioGenesys Cloud, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Genesys Cloud
- Conectando-se AppFabric à sua Genesys Cloud conta

AppFabric suporte para Genesys Cloud

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doGenesys Cloud.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Genesys Cloud de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter uma conta da Genesys Cloud.
- Você deve ter um usuário com o perfil de Administrador em sua conta do Genesys Cloud.

Considerações sobre limites de taxa

O Genesys Cloud impõe limites de taxa na API do Genesys Cloud. Para obter mais informações sobre os limites de taxas de API do Genesys Cloud, consulte Limites de taxa no site do Genesys Cloud Developer.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Genesys Cloud conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Genesys Cloud Para encontrar as informações necessárias para autorizar Genesys Cloud AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Genesys Cloud uso do OAuth. Para criar um aplicativo OAuth no Genesys Cloud, siga estas etapas:

1. Siga as instruções em Criar um cliente OAuth no site da Central de recursos da Genesys Cloud.

   Em tipos de concessão, escolha Autorização de código.
2. Use um URL de redirecionamento com o formato a seguir como URIs de redirecionamento autorizados.

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

   Nesse URL, <region>está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
3. Selecione a caixa Escopo para exibir uma lista de escopos disponíveis para sua aplicação. Selecione o escopo `audits:readonly` `users:readonly` e. Para obter informações sobre escopos, consulte Escopos de OAuth na Central do desenvolvedor da Genesys Cloud.
4. Escolha Salvar. A Genesys Cloud criará um ID de cliente e um segredo do cliente (token).

Escopos necessários

Você deve adicionar os seguintes escopos ao seu aplicativo OAuth do Genesys Cloud:

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

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do inquilino em AppFabric é o nome da sua Genesys Cloud instância. É possível encontrar sua ID de locatário na barra de endereços do navegador. Por exemplo, `usw2.pure.cloud` é a ID de locatário no seguinte URL `https://login.usw2.pure.cloud`.

Nome do locatário

Insira um nome que identifique essa organização exclusiva do Genesys Cloud. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. Para encontrar sua ID de cliente no Genesys Cloud, siga as etapas abaixo:

1. Escolha Admin.
2. Em Integrações, escolha OAuth.
3. Escolha o cliente OAuth para obter o ID do cliente.

Segredo do cliente

AppFabric solicitará um segredo do cliente. Para descobrir seu segredo do cliente no Genesys Cloud, siga as etapas abaixo:

1. Escolha Admin.
2. Em Integrações, escolha OAuth.
3. Escolha o cliente OAuth para obter o ID do cliente.

GitHub

O GitHub é uma plataforma e um serviço baseado em nuvem para desenvolvimento de software e controle de versão usando o Git, permitindo que os desenvolvedores armazenem e gerenciem seus códigos. Ele fornece o controle de versão distribuído do Git, além de controle de acesso, rastreamento de bugs, solicitações de recursos de software, gerenciamento de tarefas, integração contínua e wikis para cada projeto. Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioGitHub, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para GitHub
- Conectando-se AppFabric à sua GitHub conta

AppFabric suporte para GitHub

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doGitHub.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria GitHub de destinos compatíveis, você deve atender aos seguintes requisitos:

- Para acessar os logs de auditoria, você precisa ter uma conta corporativa.
- Para acessar os logs de auditoria corporativa, você precisa ter a função de administrador em sua conta corporativa.
- Para obter logs de auditoria da organização, você precisa ser o proprietário da organização.

Considerações sobre limites de taxa

O GitHub impõe limites de taxa na API do GitHub. Para obter mais informações sobre os limites de taxas de API do GitHub, consulte Limites de solicitação de API e alocações no site do GitHub. Se a combinação de seus aplicativos de GitHub API existentes AppFabric e seus aplicativos de API excederem GitHub's os limites, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua GitHub conta

Depois de criar seu pacote de aplicativos no AppFabric serviço, você deve autorizar AppFabric com. GitHub Para encontrar as informações necessárias para autorizar GitHub AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao GitHub uso do OAuth. Use as etapas a seguir para criar uma aplicação OAuth no GitHub. Para obter mais informações, consulte Criação de GitHubs aplicativos no GitHubsite.

1. Escolha sua foto do perfil localizada no canto superior direito da página e escolha Configurações.
2. No painel de navegação à esquerda, escolha Configurações.
3. No painel de navegação à esquerda, escolha Aplicativos OAuth.
4. Escolha Novo aplicativo OAuth.

> **Note**
>
> Esse botão estará rotulado como Registrar um novo aplicativo se você ainda não tiver criado um aplicativo OAuth.

5. Insira o nome do seu aplicativo na caixa de texto Nome do aplicativo.
6. Insira o URL completo da instância do aplicativo na caixa de texto URL da página inicial.
7. (Opcional) Insira uma descrição para seu aplicativo na caixa de texto Descrição do aplicativo. Os usuários verão essa descrição.
8. Insira um URL com o seguinte formato na caixa de texto URL de retorno de chamada de autorização.

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

Nesse URL, <region>está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

9. Escolha Ativar fluxo de dispositivos se seu aplicativo OAuth usar o fluxo de dispositivos para identificar e autorizar usuários. Para obter mais informações sobre o fluxo de dispositivos, consulte Autorização de aplicativos OAuth no site GitHub.
10. Escolha Registrar aplicativo.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. A ID do locatário deve ser fornecido em um dos seguintes formatos:

Log de auditoria corporativa:

Use o log de auditoria da empresa se quiser conhecer as ações agregadas de todas as organizações pertencentes à sua conta corporativa.

Para usar o log de auditoria corporativo, a ID do locatário é a ID corporativa da sua conta. É possível encontrar sua ID corporativa na barra de endereços do navegador. Por exemplo, *`exampleenterprise`* é a ID corporativa no seguinte URL `https://github.com/settings/enterprises/`*`examplenterprise`*.

Ao especificar a ID corporativa para o log de auditoria corporativo, você deve prefixá-lo com `enterprise:`. Portanto, especifique o exemplo anterior como `enterprise:examplenterprise`.

Log de auditoria da organização:

Use o log de auditoria da organização como administrador da organização se quiser conhecer as ações realizadas pelos membros da sua organização. Inclui detalhes como quem executou a ação, qual foi a ação e quando ela foi executada.

Para usar o log de auditoria da organização, a ID do locatário é a ID da sua organização. É possível encontrar sua ID da organização na barra de endereços do navegador. Por exemplo, *`exampleorganization`* é a ID da organização no seguinte URL `https://github.com/settings/organizations/`*`exampleorganization`*.

Ao especificar a ID do locatário para o log de auditoria da organização, você deve prefixá-la com `organization:`. Portanto, especifique o exemplo anterior como `organization:exampleorganization`.

Nome do locatário

Insira um nome que identifique essa GitHub empresa ou organização exclusiva. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. Siga estas etapas para encontrar sua ID de cliente no GitHub.

1. Escolha sua foto do perfil localizada no canto superior direito da página e escolha Configurações.
2. No painel de navegação à esquerda, escolha Configurações.
3. No painel de navegação à esquerda, escolha Aplicativos OAuth.
4. Escolha o aplicativo OAuth específico e, em seguida, procure o valor da ID de cliente.

Segredo do cliente

AppFabric solicitará um segredo do cliente. Siga estas etapas para descobrir seu segredo de cliente no GitHub.

1. Escolha sua foto do perfil localizada no canto superior direito da página e escolha Configurações.
2. No painel de navegação à esquerda, escolha Configurações.
3. No painel de navegação à esquerda, escolha Aplicativos OAuth.
4. Escolha o aplicativo OAuth específico e, em seguida, procure o valor do Segredo do cliente. Se você não conseguir encontrar um segredo de cliente existente, talvez seja necessário gerar um novo.

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up GitHub para aprovar a autorização. Para aprovar a AppFabric autorização, escolha Permitir.

Certifique-se de que suas organizações tenham concedido acesso ao aplicativo OAuth, se as restrições de acesso do aplicativo OAuth estiverem habilitadas.

Google Analytics

Google Analyticsé um serviço de análise da web que fornece estatísticas e ferramentas analíticas básicas para fins de otimização de mecanismos de pesquisa (SEO) e marketing. Google Analyticsé usado para monitorar o desempenho do site e coletar informações dos visitantes. Ele pode ajudar as organizações a determinar as principais fontes de tráfego de usuários, avaliar o sucesso de suas atividades e campanhas de marketing, monitorar a conclusão de metas (como compras, adição de produtos aos carrinhos), descobrir padrões e tendências no engajamento do usuário e obter outras informações do visitante, como dados demográficos. Sites de varejo de pequeno e médio porte costumam ser usados Google Analytics para obter e analisar várias análises do comportamento do cliente, que podem ser usadas para melhorar as campanhas de marketing, direcionar o tráfego do site e reter melhor os visitantes.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioAzure Monitor, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Google Analytics
- Conectando-se AppFabric à sua Google Analytics conta

AppFabric suporte para Google Analytics

AppFabric suporta o recebimento de registros de auditoria doGoogle Analytics.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Google Analytics de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ser administrador da Google Analytics conta.
- AppFabric Para entregar registros, você precisa ativar a API Google Analytics Admin em seu Google Cloud projeto. Certifique-se de usar um novo projeto ao configurar o aplicativo Google Analytics OAuth.

Considerações sobre limites de taxa

O Google Analytics impõe limites de taxa na API do Google Analytics. Para obter mais informações sobre os limites de taxa Google Analytics da API, consulte Limites e cotas no site do Google Analytics. Se a combinação de seus aplicativos existentes da API Google Analytics AppFabric e seus aplicativos excederem o limite, os registros de auditoria que aparecem AppFabric podem ser atrasados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Google Analytics conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Google Analytics Use as etapas a seguir para encontrar as informações necessárias para Google Analytics autorizar AppFabric.

Criar um aplicativo OAuth

AppFabric se integra ao Google Analytics uso do OAuth. Conclua as etapas a seguir para criar um aplicativo OAuth em: Google Analytics

1. Para configurar sua tela de consentimento do OAuth, siga as instruções em Configurar a tela de consentimento do OAuth no Guia do desenvolvedor do Google no site do Google.
2. Escolha Externo para o tipo de usuário
3. Para configurar as credenciais do OAuth para AppFabric, siga as instruções na seção Credenciais do ID do cliente OAuth da página Criar credenciais de acesso no Guia do desenvolvedor do Google.
4. Usar um URL de redirecionamento com o formato a seguir.

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

   Nesse endereço, *<region>* está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte

da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Escopos necessários

Você deve adicionar o seguinte escopo ao seu aplicativo Google Analytics OAuth:

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

Autorizações do aplicativo

ID de locatário

AppFabric solicitará um ID de inquilino. O ID do inquilino AppFabric é o ID Google Analytics da sua conta.

1. Vá para a página Google Analytics inicial.
2. Escolha Admin no painel de navegação.
3. Você encontrará o ID da sua conta em Conta > Configurações da conta > Detalhes da conta > ID da conta.

Nome do locatário

Insira um nome que identifique essa Google Analytics organização exclusiva. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. Use as etapas a seguir para encontrar seu ID de cliente emGoogle Analytics:

1. Acesse a página de Credenciais.
2. Na seção IDs de cliente do OAuth 2.0, escolha a ID do cliente que você criou.
3. O ID do cliente está listado na seção Informações adicionais da página.

Segredo do cliente

AppFabric solicitará um segredo do cliente. Use as etapas a seguir para descobrir o segredo do seu cliente emGoogle Analytics:

1. Acesse a página de Credenciais.
2. Na seção IDs de cliente do OAuth 2.0, escolha o nome do cliente.
3. O segredo do cliente está listado na seção Segredos do cliente da página.

Autorização do aplicativo

Depois de criar a autorização do aplicativo, AppFabric você receberá uma janela pop-up Google Analytics para aprovar a autorização. Para aprovar a AppFabric autorização escolhendo Permitir.

Google Workspace

O Google Workspace é um conjunto de ferramentas, softwares e produtos de computação em nuvem, produtividade e colaboração desenvolvidos e comercializados pelo Google.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioGoogle Workspace, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Google Workspace
- Conectando-se AppFabric à sua Google Workspace conta

AppFabric suporte para Google Workspace

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doGoogle Workspace.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Google Workspace de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve assinar um plano Google Workspace Enterprise Standard. Para obter mais informações sobre como criar ou atualizar para um plano do Enterprise Standard do Google Workspace, o site de Planos do Google Workspace.
- Você deve ter um usuário com o perfil de Administrador no seu Google Workspace.
- AppFabric Para entregar registros, você precisa ativar a API do SDK Admin do Google em seu projeto do Google Cloud. Para obter mais informações, consulte Ativar as APIs do Google Workspace no Guia do desenvolvedor do Google Workspace.

Considerações sobre limites de taxa

O Google Workspace impõe limites de taxa na API do Google Workspace. Para obter mais informações sobre os limites de taxas de API do Google Workspace, consulte Limites e cotas no Guia de Administração do Google Workspace no site do Google Workspace. Se a combinação de seus aplicativos de Google Workspace API existentes AppFabric e seus aplicativos de API excederem o limite, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Você pode ver um atraso de até 30 minutos na maioria dos eventos de auditoria e até 4 horas de atraso para que determinados eventos de auditoria sejam entregues ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. Para obter mais informações, consulte Retenção de dados e tempos de espera no site de ajuda do WorkSpace administrador do Google. No entanto, isso pode ser personalizado ao nível da conta. Para obter assistência, entre em contato AWS Support.

Conectando-se AppFabric à sua Google Workspace conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Google Workspace Para encontrar as informações necessárias para autorizar Google Workspace AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Google Workspace uso do OAuth. Para criar um aplicativo OAuth no Google Workspace, siga as etapas abaixo:

1. Para configurar sua tela de consentimento do OAuth, siga as instruções em Configurar a tela de consentimento do OAuth no Guia do desenvolvedor do Google Workspace no site do Google Workspace.

Escolha Interno para o Tipo de usuário.

2. Para configurar as credenciais do OAuth para AppFabric, siga as instruções na seção Credenciais de ID do cliente OAuth da página Criar credenciais de acesso no Guia do desenvolvedor. Google Workspace
3. Usar um URL de redirecionamento com o formato a seguir.

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

Nesse URL, *<region>* está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Escopos necessários

Você deve adicionar os seguintes escopos ao seu aplicativo OAuth do Google Workspace:

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

Se você não visualizar esses escopos, adicione a API Admin SDK à sua biblioteca de APIs da nuvem do Google.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do inquilino AppFabric é o ID Google Workspace do seu projeto. Para encontrar a ID do projeto, consulte Localizar a ID do projeto no site de Ajuda do Console de APIs do Google.

Nome do locatário

Insira um nome que identifique esse Google Workspace exclusivo. AppFabric usa o nome do inquilino para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará seu ID de cliente. Para encontrar sua ID de cliente, siga as etapas abaixo:

1. Encontre sua ID de cliente usando as informações na seção Exibir credenciais da página Gerenciar credenciais no Guia do desenvolvedor do Google Workspace.
2. Insira o ID do cliente do seu cliente OAuth no campo ID do cliente em. AppFabric

Segredo do cliente

AppFabric solicitará o segredo do seu cliente. Para descobrir o segredo do cliente, siga as etapas abaixo:

1. Descubra seu segredo de cliente consultando as informações na seção Exibir credenciais da página Gerenciar credenciais no Guia do desenvolvedor do Google Workspace.
2. Se você precisar redefinir o segredo do cliente, siga as instruções na seção Redefinir o segredo do cliente da página Gerenciar credenciais no Guia do desenvolvedor do Google Workspace.
3. Insira o segredo do seu cliente no campo Segredo do cliente em AppFabric.

Aprovar autorização

Depois de criar a autorização do aplicativo, AppFabric você receberá uma janela pop-up Google Workspace para aprovar a autorização. Para aprovar a AppFabric autorização, escolha permitir.

HubSpot

O HubSpot é uma plataforma para clientes com todo o software, integrações e recursos de que você precisa para conectar seu marketing, vendas, gerenciamento de conteúdo e atendimento ao cliente. A plataforma conectada do HubSpot permite que você expanda seus negócios com mais rapidez, concentrando-se no que é mais importante: seus clientes. Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioHubSpot, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para HubSpot
- Conectando-se AppFabric à sua HubSpot conta

AppFabric suporte para HubSpot

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doHubSpot.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria HubSpot de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter uma conta com a assinatura Enterprise no HubSpot para acessar os logs de auditoria. Para obter mais informações sobre assinaturas do HubSpot, consulte Gerenciamento da sua assinatura do HubSpot na Base de conhecimento do HubSpot.
- Você deve ter uma conta de desenvolvedor e uma aplicação associada à conta.
- Você deve ser um superadministrador para instalar aplicações em sua conta do HubSpot, ou ter a permissão de acesso ao App Marketplace, além das permissões do usuário, para aceitar os escopos que a aplicação está solicitando.

Considerações sobre limites de taxa

O HubSpot impõe limites de taxa na API do HubSpot. Para obter mais informações sobre os limites de taxa da API do HubSpot, incluindo limites para aplicações que usam OAuth, consulte Limites de taxa no site do HubSpot. Se a combinação de seus aplicativos de HubSpot API existentes AppFabric e seus aplicativos HubSpot de API excederem os limites, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua HubSpot conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. HubSpot Para encontrar as informações necessárias para autorizar HubSpot AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao HubSpot uso do OAuth. Para criar um aplicativo OAuth no HubSpot, siga estas etapas:

1. Siga as instruções na seção Criação de uma aplicação pública no guia do HubSpot no site do HubSpot.
2. Na guia Autorizar, adicione os três escopos listados em Escopos necessários.
3. Use um URL de redirecionamento com o formato a seguir em Redirecionar URL.

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

   Nesse URL, <region>está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
4. Escolha Criar aplicação.

Escopos necessários

Você deve adicionar os seguintes escopos ao seu aplicativo OAuth do HubSpot:

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

Autorizações do aplicativo

ID de locatário

Insira um ID que identifique essa organização exclusiva do HubSpot. Por exemplo, insira o ID da sua conta do HubSpot.

Nome do locatário

Insira um nome que identifique essa organização exclusiva do HubSpot. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. Para encontrar sua ID de cliente no HubSpot, siga as etapas abaixo:

1. Navegue até a página de login do HubSpot e faça login usando as credenciais da sua conta de desenvolvedor.
2. No menu Aplicações, escolha sua aplicação.
3. Na guia Autorizar, procure o valor do ID do cliente.

Segredo do cliente

AppFabric solicitará um segredo do cliente. Para descobrir seu segredo do cliente no HubSpot, siga as etapas abaixo:

1. Navegue até a página de login do HubSpot e faça login usando as credenciais da sua conta de desenvolvedor.
2. No menu Aplicações, escolha sua aplicação.
3. Na guia Autorizar, procure o valor do Segredo do cliente.

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up HubSpot para aprovar a autorização. Faça login na sua conta usando as credenciais da sua conta corporativa (não sua conta de desenvolvedor) para aprovar a autorização. AppFabric Escolha permitir.

IBM Security® Verify

A IBM Security® Verify família fornece recursos automatizados, baseados na nuvem e locais para administrar a governança de identidade, gerenciar a identidade e o acesso da força de trabalho e do consumidor e controlar contas privilegiadas. Se você precisa implantar uma solução na nuvem ou no local, IBM Security® Verify ajuda a estabelecer confiança e se proteger contra ameaças internas à sua força de trabalho e aos consumidores.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioIBM Security® Verify, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para o IBM Security® Verify
- Conectando-se AppFabric à sua IBM Security® Verify conta

AppFabric suporte para o IBM Security® Verify

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doIBM Security® Verify.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria IBM Security® Verify de destinos compatíveis, você deve atender aos seguintes requisitos:

- Para acessar os registros de auditoria, você precisa ter uma conta IBM Security® VerifySaaS.
- Para acessar os registros de auditoria, você precisa ter uma função de administrador na sua conta IBM Security® Verify SaaS.

Considerações sobre limites de taxa

O IBM Security® Verify impõe limites de taxa na API do IBM Security® Verify. Para obter mais informações sobre os limites de taxa IBM Security® Verify da API, consulte os Termos da IBM. Se a combinação de seus aplicativos de IBM Security® Verify API existentes AppFabric e seus aplicativos de API excederem IBM Security® Verify os limites, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Você pode ver um atraso de até 30 minutos em um evento de auditoria para ser entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizável em nível de conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua IBM Security® Verify conta

Depois de criar seu pacote de aplicativos no AppFabric serviço, você deve autorizar AppFabric com. IBM Security® Verify Para encontrar as informações necessárias para autorizar IBM Security® Verify AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao IBM Security® Verify uso do OAuth. Para criar um aplicativo OAuth emIBM Security® Verify, consulte Criar um cliente de API no site de documentação da IBM.

1. Para fazer login pela primeira vez, use o URL de login e as credenciais que foram enviadas para seu endereço de e-mail registrado.
2. Acesse o console de administração em`https://<hostname>.verify.ibm.com/ui/admin/`. Para obter mais informações, consulte Acessar o IBM Security® Verify.
3. No console de administração, em Segurança < Acesso à API < Cliente da API, escolha Adicionar.
4. Selecione as seguintes opções. Eles são necessários para ler o registro de auditoria e os detalhes do usuário.
   - Leia relatórios
   - Grupos e usuários lidos
5. Mantenha a opção Padrão no método de Autenticação do Cliente.

   Não edite o campo Escopos personalizados.
6. Escolha Próximo.
7. Não edite o campo do filtro IP.
8. Escolha Próximo.
9. Não edite o campo Propriedades adicionais.
10. Escolha Próximo.
11. Especifique um nome e uma descrição. A descrição é opcional.
12. Escolha Criar cliente de API.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. Você pode localizar o ID do inquilino no URL IBM Security® Verify padrão. Por exemplo, no `https://hostname.verify.ibm.com/` URL, o ID do locatário é o *`nome do host`* que pode ser encontrado antes `.verify.ibm.com` (ou antes, `ice.ibmcloud.com` se você estiver usando um nome de host antigo). Se você estiver usando uma

URL personalizada, entre em contato com sua equipe de IBM Security® Verify suporte para obter sua URL padrão.

Nome do locatário

Insira um nome que identifique esse IBM Security® Verify inquilino exclusivo. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e qualquer ingestão criada a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. Para encontrar sua ID de cliente no IBM Security® Verify, siga as etapas abaixo:

1. Para fazer login pela primeira vez, use o URL de login e as credenciais que foram enviadas para seu endereço de e-mail registrado.
2. Acesse o console de administração em`https://<hostname>.verify.ibm.com/ui/admin/`. Para obter mais informações, consulte Acessar o IBM Security® Verify.
3. No console de administração, em Segurança < Acesso à API < Cliente da API, escolha as reticências (✓) ao lado do aplicativo OAuth específico.
4. Escolha Detalhes da conexão.
5. Localize o ID do cliente nas credenciais da API.

Segredo do cliente

AppFabric solicitará um segredo do cliente. Para descobrir seu segredo do cliente no IBM Security® Verify, siga as etapas abaixo:

1. Para fazer login pela primeira vez, use o URL de login e as credenciais que foram enviadas para seu endereço de e-mail registrado.
2. Acesse o console de administração em`https://<hostname>.verify.ibm.com/ui/admin/`. Para obter mais informações, consulte Acessar o IBM Security® Verify.
3. No console de administração, em Segurança < Acesso à API < Cliente da API, escolha as reticências (✓) ao lado do aplicativo OAuth específico.
4. Escolha Detalhes da conexão.
5. Localize o segredo do cliente nas credenciais da API.

JumpCloud

JumpCloud Inc. é uma empresa americana de software corporativo que fornece uma plataforma de diretórios baseada em nuvem para gerenciamento de identidades. Ele centraliza e simplifica o gerenciamento de identidades, permitindo que os usuários acessem com segurança seus sistemas, aplicativos, redes e servidores de arquivos com um único conjunto de credenciais, independentemente da plataforma, protocolo, provedor ou localização.

Você pode usar AppFabric a AWS para receber registros de auditoria e dados de usuários JumpCloud, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Kinesis Data Firehose.

Tópicos

- AppFabric suporte para JumpCloud
- Conectando-se AppFabric à sua JumpCloud conta

AppFabric suporte para JumpCloud

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doJumpCloud.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria JumpCloud de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter um plano de JumpCloud assinatura pago ativo. Para obter mais informações, consulte Select a package that's right for youno JumpCloud site.
- Você deve ter a função “Administradores com cobrança”.

Considerações sobre limites de taxa

A JumpCloud não publica limites de taxas. Você deve criar um caso de suporte ou entrar em contato com sua equipe de JumpCloud clientes. Se a combinação de seus aplicativos de JumpCloud API existentes AppFabric e seus aplicativos de API excederem JumpCloud's os limites, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso ocorre devido a atrasos nos eventos de auditoria disponibilizados pelo aplicativo e às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua JumpCloud conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. JumpCloud Para encontrar as informações necessárias para JumpCloud autorizar AppFabric, siga as etapas na próxima seção.

Crie um token de organização a partir da JumpCloud conta

AppFabric usa uma chave de API para integrar com JumpCloud Para criar uma chave de API em JumpCloud, siga estas etapas:.

1. Faça login na sua JumpCloud conta como administrador.
2. No Portal do administrador, escolha as iniciais da sua conta, localizadas no canto superior direito, e escolha Minha chave de API no menu.
3. Escolha Gerar nova chave de API ou selecione uma chave existente.

> **Note**
>
> JumpCloudsó permite uma chave de API ativa. A geração de uma nova chave de API revogará o acesso à chave de API atual. Isso tornará todas as chamadas que usam a chave de API anterior inacessíveis. Você precisará atualizar todas as integrações existentes que usam a chave de API anterior com o novo valor da chave.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. Aqui, “ID da organização” será o ID do inquilino. Para encontrar o “ID da organização”, siga estas etapas.

1. Faça login na sua conta da JumpCloud.

2. No painel de navegação, escolha Configurações, depois Perfil da organização e, em seguida, Geral.
3. Escolha o ícone “olho” para remover a visão obscurecida.
4. Escolha o ícone de “página dupla” para copiar o ID.

Nome do locatário

Insira um nome que identifique essa JumpCloud organização exclusiva. AppFabric usa o nome do inquilino para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

Token de contas de serviço

AppFabric solicitará o token da sua conta de serviço. Em AppFabric, esse é o token de API da organização que você criou anteriormente neste tópico. Crie um token de organização a partir da JumpCloud conta

Microsoft365

Microsoft O 365 é uma família de produtos de software de produtividade, colaboração e serviços baseados em nuvem de propriedade da Microsoft.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados de usuários do Microsoft 365, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Microsoft 365
- Conectando-se AppFabric à sua conta Microsoft 365

AppFabric suporte para Microsoft 365

AppFabric suporta o recebimento de informações do usuário e registros de auditoria do Microsoft 365.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria do Microsoft 365 para destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve assinar um plano Microsoft 365 Enterprise. Para obter mais informações sobre como criar ou atualizar para um plano do Microsoft 365 Enterprise, consulte Planos do Microsoft 365 Enterprise no Microsoft site.
- Você deve ter um usuário com permissões de Administrador em sua conta do Microsoft 365.
- Você deve ativar o registro em log de auditoria para sua organização. Para obter mais informações, consulte Ativar ou desativar a auditoria no Microsoft site.

Considerações sobre limites de taxa

O Microsoft 365 impõe limites de taxa na API do Microsoft 365. Para obter mais informações sobre os limites de taxa da API do Microsoft 365, consulte Limites de controle de utilização específicos do serviço do Microsoft Graph na documentação do Microsoft Graph no site da Microsoft. Se a combinação de seus aplicativos de API Microsoft 365 existentes AppFabric e seus aplicativos existentes excederem o limite, os registros de auditoria que aparecem AppFabric podem ser atrasados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua conta Microsoft 365

Depois de criar seu pacote de aplicativos no AppFabric serviço, você deve autorizar AppFabric com Microsoft 365. Para encontrar as informações necessárias para autorizar o Microsoft 365 AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric integra-se ao Microsoft 365 usando o OAuth. Para criar um aplicativo OAuth no Microsoft 365, siga estas etapas:

1. Siga as instruções na seção Registrar um aplicativo no Guia do Desenvolvedor do Azure Active Directory no site da Microsoft.

   Escolha Contas nesse diretório organizacional somente na configuração de Tipos de contas compatíveis.

2. Siga as instruções na seção Adicionar um URI de redirecionamento no Guia do Desenvolvedor do Azure Active Directory.

   Escolha a plataforma de Web.

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

   Nesse URL, *<region>* está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

   Você pode pular os outros campos de entrada para a plataforma de Web.

3. Siga as instruções na seção Adicionar um segredo de cliente do Guia do Desenvolvedor do Azure Active Directory.

Permissões obrigatórias

Você deve adicionar as seguintes permissões para seu aplicativo OAuth: Para adicionar permissões, siga as instruções na seção Adicionar permissões para acessar sua API da Web do Guia do Desenvolvedor do Azure Active Directory.

- `Microsoft Graph API>` `User.Read` (adicionado automaticamente)
- `Office 365 Management APIs>` `ActivityFeed.Read` (Selecione o tipo delegado)
- `Office 365 Management APIs>` `ActivityFeed.ReadDlp` (Selecione o tipo delegado)
- `Office 365 Management APIs>` `ServiceHealth.Read` (Selecione o tipo delegado)

Depois de adicionar as permissões, para conceder o consentimento do administrador para as permissões, siga as instruções na seção Botão de consentimento do administrador do Guia do Desenvolvedor do Azure Active Directory.

Autorizações do aplicativo

AppFabric suporta o recebimento de informações do usuário e registros de auditoria da sua conta Microsoft 365. Para receber os logs de auditoria e os dados do usuário do Microsoft 365, você deve criar duas autorizações de aplicativo, uma chamada Microsoft365 na lista suspensa de autorização do aplicativo e outra chamada Log de auditoria do Microsoft365 na lista suspensa de autorização do aplicativo. Você pode usar a mesma ID de locatário, ID do cliente e segredo do cliente para as autorizações do aplicativo. Para receber logs de auditoria do Microsoft 365, você precisa das autorizações de aplicativo Microsoft365 e Log de auditoria do Microsoft 365. Para usar a ferramenta de acesso do usuário sozinha, somente a autorização do aplicativo Microsoft 365 é necessária.

ID de locatário

AppFabric solicitará seu ID de inquilino. A ID do inquilino em AppFabric é sua ID de inquilino do Azure Active Directory. Para encontrar sua ID de locatário do Azure Active Directory, consulte Como encontrar sua ID de locatário do Azure Active Directory na Documentação do Produto Azure no site da Microsoft.

Nome do locatário

Insira um nome que identifique essa conta do Microsoft 365 exclusiva. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará seu ID de cliente. O ID do cliente em AppFabric é o ID do aplicativo (cliente) Microsoft 365. Para encontrar sua ID (de cliente) do aplicativo no Microsoft 365, siga estas etapas:

1. Abra a página de visão geral do aplicativo OAuth que você usa com. AppFabric
2. A ID (de cliente) do aplicativo aparece em Fundamentos.
3. Insira o ID do aplicativo (cliente) do seu cliente OAuth no campo ID do cliente em. AppFabric

Segredo do cliente

AppFabric solicitará o segredo do seu cliente. Microsoft365 fornece esse valor somente quando você cria inicialmente o segredo do cliente para seu aplicativo OAuth. Para gerar um novo segredo do cliente, caso você não tenha um, use as seguintes etapas:

1. Para criar um segredo do cliente, siga as instruções na seção Adicionar um segredo de cliente do Guia do Desenvolvedor do Azure Active Directory.
2. Insira o conteúdo do campo Valor no campo Segredo do cliente em AppFabric.

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up do Microsoft 365 para aprovar a autorização. Para aprovar a AppFabric autorização, escolha permitir.

Miro

Miro é um espaço de trabalho on-line para inovação que permite que equipes distribuídas de qualquer tamanho criem a próxima grande novidade. A tela infinita da plataforma permite que as equipes conduzam workshops e reuniões envolventes, criem produtos, debatam ideias e muito mais. Miro, com sede conjunta em São Francisco e Amsterdã, atende a mais de 50 milhões de usuários em todo o mundo, incluindo 99% das empresas da Fortune 100. Miro foi fundada em 2011 e atualmente tem mais de 1.500 funcionários em 12 centros ao redor do mundo. Para saber mais, acesse Miro.

Miro inclui um conjunto completo de recursos colaborativos projetados para inovação, incluindo diagramação, wireframing, visualização de dados em tempo real, facilitação de workshops e suporte integrado para práticas ágeis, workshops e apresentações interativas. Miro anunciou recentemente a IA Miro, que amplia as capacidades de Miro, com mapeamento e diagramação orientados por IA, agrupamento e resumo e geração de conteúdo. Miro permite que as organizações reduzam o número de ferramentas autônomas, reduzindo a fragmentação e o custo das informações.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioMiro, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Miro
- Conectando-se AppFabric à sua Miro conta

AppFabric suporte para Miro

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doMiro.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Miro de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter um plano empresarial Miro. Para obter mais informações sobre os tipos de planos de Miro, consulte a página de Miropreços no site Miro.
- Você deve ter um usuário com o perfil de Administrador da empresa em sua conta do Miro. Para obter mais informações sobre funções, consulte a seção Funções em nível de empresa no Miro no site da Central de Ajuda do Miro.
- Você deve ter uma equipe de desenvolvedores corporativos em sua conta de Miro. Para obter informações sobre a criação de equipes de desenvolvedores, consulte Equipes de desenvolvedores corporativos no site da Central de Ajuda do Miro.

Considerações sobre limites de taxa

O Miro impõe limites de taxa na API do Miro. Para obter mais informações sobre os limites de taxas de API do Miro, consulte Limites de taxa no Guia do desenvolvedor do Miro no site do Miro. Se a combinação de seus aplicativos de Miro API existentes AppFabric e seus aplicativos excederem o limite, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Miro conta

Depois de criar seu pacote de aplicativos no AppFabric serviço, você deve autorizar AppFabric com. Miro Para encontrar as informações necessárias para autorizar Miro AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Miro uso do OAuth. Para criar um aplicativo OAuth no Miro, siga estas etapas:

1. Para criar um aplicativo OAuth, siga as instruções na seção Criação e instalação de aplicativos do artigo Equipes de desenvolvedores corporativos no site da Central de Ajuda do Miro.
2. Na caixa de diálogo de criação do aplicativo, marque a caixa de seleção Expirar token de autorização do usuário depois de selecionar uma equipe de desenvolvedores na organização corporativa.

   > **Note**
   >
   > Você deve fazer isso antes de criar o aplicativo, pois não é possível alterar essa opção depois de criar o aplicativo.

3. Na página do aplicativo, insira um URL com o seguinte formato na seção URI de redirecionamento para seção de OAuth 2.0.

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

   Nesse URL, <region>está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
4. Copie e salve seu ID e segredo do cliente para usar na autorização do AppFabric aplicativo.

Escopos necessários

Você deve adicionar os seguintes escopos na seção `Permissions` da página de seu aplicativo OAuth Miro:

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

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do inquilino AppFabric é seu ID Miro da equipe. Para obter informações sobre como encontrar seu ID de equipe do Miro, consulte a seção Perguntas frequentes de Sou um novo Miro administrador. Por onde começar? no site da MiroCentral de Ajuda.

Nome do locatário

Insira um nome que identifique essa organização exclusiva do Miro. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará seu ID de cliente. Para encontrar sua ID de cliente, siga estas etapas:

1. Navegue até as configurações do seu perfil no Miro.
2. Selecione a guia Seus aplicativos.
3. Selecione o aplicativo que você usa para se conectar AppFabric.
4. Insira o ID do cliente na seção Credenciais do aplicativo no campo ID do cliente em AppFabric.

Segredo do cliente

AppFabric solicitará o segredo do seu cliente. Para descobrir o segredo do cliente, siga estas etapas:

1. Navegue até as configurações do seu perfil no Miro.
2. Selecione a guia Seus aplicativos.
3. Selecione o aplicativo que você usa para se conectar AppFabric.
4. Insira o segredo do cliente na seção Credenciais do aplicativo no campo Segredo do cliente em AppFabric.

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up Miro para aprovar a autorização. Para aprovar a AppFabric autorização, escolha Permitir.

Okta

O Okta é a maior empresa de identidade do mundo. Como principal parceiro independente de Identidade, o Okta permite que todos utilizem qualquer tecnologia, em qualquer lugar, em qualquer dispositivo ou aplicativo, com segurança. As marcas mais renomadas confiam no Okta para fornecer acesso, autenticação e automação seguros. Priorizando a flexibilidade e a neutralidade nas Nuvens de identidade da força de trabalho e dos clientes do Okta, líderes de negócios e desenvolvedores podem se concentrar na inovação e acelerar a transformação digital, graças às

soluções personalizáveis e às mais de 7.000 integrações pré-construídas. O Okta está construindo um mundo onde a identidade pertence a você. Saiba mais em okta.com.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioOkta, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Okta
- Conectando-se AppFabric à sua Okta conta

AppFabric suporte para Okta

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doOkta.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Okta de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você pode usar AppFabric com qualquer tipo de Okta plano.
- Você deve ter um usuário com o perfil de Super Administrador em sua conta do Okta.
- O usuário que aprova a autorização do aplicativo também AppFabric deve ter a função de Superadministrador em sua Okta conta.

Considerações sobre limites de taxa

O Okta impõe limites de taxa na API do Okta. Para obter mais informações sobre os limites de taxas de API do Okta, consulte Limites de taxa no Guia do desenvolvedor do Okta no site do Okta. Se a combinação de seus aplicativos de Okta API existentes AppFabric e seus aplicativos Okta de API excederem os limites, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Okta conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Okta Para encontrar as informações necessárias para autorizar Okta AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Okta uso do OAuth. Para criar um aplicativo OAuth para se conectar AppFabric, siga as instruções em Criar integrações de aplicativos OIDC no site da Central de Ajuda. Okta A seguir estão as considerações de configuração para AppFabric:

1. Em Tipo de aplicativo, selecione Aplicativo web.
2. Para Tipo de concessão, escolha Código de autorização e Atualizar token.
3. Use um URL de redirecionamento com o seguinte formato como URI de redirecionamento de login e URI de redirecionamento de logout.

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

   Nesse URL, <region>está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
4. Você pode pular a configuração de Origens confiáveis.
5. Conceda acesso a todos em sua organização do Okta na configuração de Acesso controlado.

   > **Note**
   >
   > Se pular essa etapa durante a criação inicial do aplicativo OAuth, você poderá atribuir todos em sua organização como um grupo usando a guia Atribuições na página de configuração do aplicativo.
6. Você pode deixar todas as outras opções com seus valores padrão.

Escopos necessários

Você deve adicionar os seguintes escopos ao seu aplicativo OAuth do Okta:

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

Autorizações do aplicativo

ID de locatário

AppFabric solicitará um ID de inquilino. O ID do inquilino AppFabric é seu Okta domínio. Para obter mais informações sobre como encontrar seu domínio do Okta, consulte Encontre seu domínio do Okta no Guia do desenvolvedor do Okta no site do Okta.

Nome do locatário

Insira um nome que identifique essa organização exclusiva do Okta. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. Para encontrar sua ID de cliente no Okta, siga as etapas abaixo:

1. Navegue até o console do desenvolvedor do Okta.
2. Escolha a guia Aplicativos.
3. Escolha seu aplicativo e depois escolha a guia Geral.
4. Role até a seção Credenciais do cliente.
5. Insira o ID do cliente do seu cliente OAuth no campo ID do cliente em. AppFabric

Segredo do cliente

AppFabric solicitará um segredo do cliente. Para descobrir seu segredo do cliente no Okta, siga as etapas abaixo:

1. Navegue até o console do desenvolvedor do Okta.
2. Escolha a guia Aplicativos.
3. Escolha seu aplicativo e depois escolha a guia Geral.
4. Role até a seção Credenciais do cliente.

5. Insira o segredo do cliente do seu aplicativo OAuth no campo Segredo do cliente em. AppFabric

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up Okta para aprovar a autorização. Para aprovar a AppFabric autorização, escolha permitir. O usuário que aprova a autorização do Okta deve ter permissão de Super Administrador no Okta.

OneLogin by One Identity

O OneLogin by One Identity é uma solução moderna de gerenciamento de acesso baseada em nuvem que gerencia perfeitamente todas as identidades digitais de sua força de trabalho, clientes e parceiros. O OneLogin fornece autenticação única (SSO), autenticação multifator (MFA), autenticação adaptativa, MFA em nível de desktop, integração de diretórios com AD, LDAP, G Suite e outros diretórios externos, gerenciamento do ciclo de vida de identidade e muito mais. Com OneLogin isso, você pode proteger sua organização contra os ataques mais comuns, resultando em maior segurança, experiências de usuário simplificadas e conformidade com os requisitos regulatórios. Você pode usar a segurança AWS AppFabric para receber registros de auditoria e dados de usuáriosOneLogin, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um Amazon Simple Storage Service (Amazon S3) bucket ou Amazon Data Firehose Stream do Firehose.

Tópicos

- AppFabric suporte para OneLogin by One Identity
- Conectando-se AppFabric à sua OneLogin by One Identity conta

AppFabric suporte para OneLogin by One Identity

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doOneLogin by One Identity.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria OneLogin by One Identity de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter uma conta do OneLogin Avançada ou Profissional.
- Você deve ter um usuário com privilégios de administrador/administrador delegado.

Considerações sobre limites de taxa

O OneLogin by One Identity impõe limites de taxa na API do OneLogin. Para obter mais informações sobre os limites de taxa de API do OneLogin, consulte Obtenção de limite de taxa na Referência de API do OneLogin. Se a combinação de seus aplicativos de OneLogin API existentes AppFabric e seus aplicativos OneLogin de API excederem os limites, os registros de auditoria que aparecem AppFabric podem ser adiados. No entanto, o limite de taxa OneLogin pode ser aumentado. Para obter ajuda, entre em contato com seu gerente de conta do OneLogin by One Identity ou entre em contato com One Identity.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua OneLogin by One Identity conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. OneLogin by One Identity Para encontrar as informações necessárias para autorizar OneLogin AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao OneLogin by One Identity uso do OAuth. Para criar um aplicativo OAuth no OneLogin, siga estas etapas:

1. Navegue até a página de login do OneLogin e faça login.
2. No menu Desenvolvedores, escolha Credenciais de API.
3. Escolha Novas credenciais, insira um nome para sua nova credencial e escolha Ler tudo.
4. Escolha Salvar. O OneLogin criará um ID de cliente e um segredo do cliente.

Escopos necessários

Você deve adicionar os seguintes escopos ao seu aplicativo OAuth do OneLogin by One Identity:

- Leia tudo. Para obter mais informações sobre escopos e credenciais do cliente, consulte Trabalho com credenciais de API na Referência de API do OneLogin.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará um ID de inquilino. O ID do locatário em AppFabric é o subdomínio da sua instância. É possível encontrar sua ID de locatário na barra de endereços do navegador. Por exemplo, `subdomain` é a ID de locatário no seguinte URL `https://subdomain.onelogin.com`.

Nome do locatário

Insira um nome que identifique essa organização exclusiva do OneLogin by One Identity. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. Para encontrar sua ID de cliente no OneLogin by One Identity, siga as etapas abaixo:

1. Navegue até a página de login do OneLogin e faça login.
2. No menu Desenvolvedores, escolha Credenciais de API.
3. Escolha a credencial da API para obter o ID do cliente.

Segredo do cliente

AppFabric solicitará um segredo do cliente. Para descobrir seu segredo do cliente no OneLogin by One Identity, siga as etapas abaixo:

1. Navegue até a página de login do OneLogin e faça login.
2. No menu Desenvolvedores, escolha Credenciais de API.
3. Escolha a credencial da API para obter o segredo do cliente.

Autorização da aplicação do cliente

Em AppFabric, crie uma autorização de aplicativo usando seu ID e nome de inquilino e seu nome e ID de cliente. Escolha conectar para ativar a autorização.

PagerDuty

O PagerDuty é uma plataforma digital de gerenciamento de operações que ajuda as equipes a mitigar os problemas que afetam os clientes, transformando qualquer sinal em ação para que você possa resolver problemas com mais rapidez e operar com mais eficiência. Se integra com CloudWatch, GuardDuty, CloudTrail e Personal Health Dashboard. Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioPagerDuty, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para PagerDuty
- Conectando-se AppFabric à sua PagerDuty conta

AppFabric suporte para PagerDuty

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doPagerDuty.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria PagerDuty de destinos compatíveis, você deve atender aos seguintes requisitos:

- Para acessar os logs de auditoria, você deve ter um plano Business ou Operações Digitais do PagerDuty.
- Você deve ser administrador global ou proprietário da conta do PagerDuty.

Considerações sobre limites de taxa

O PagerDuty impõe limites de taxa na API do PagerDuty. Para obter mais informações sobre os limites de taxas de API do PagerDuty, consulte Limites de taxa da REST API na Plataforma de desenvolvimento do PagerDuty. Se a combinação de seus aplicativos de PagerDuty API existentes AppFabric e seus aplicativos PagerDuty de API excederem os limites, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua PagerDuty conta

A plataforma PagerDuty oferece suporte a chaves de acesso a APIs. Para gerar uma chave de acesso à API, siga as etapas adiante.

Criar uma chave de acesso à API

AppFabric se integra ao PagerDuty uso de uma chave de acesso à API para clientes públicos. Para criar uma chave de acesso à API no PagerDuty, siga as etapas adiante:

1. Navegue até a página de login do PagerDuty e faça login.
2. Escolha Integrações, Chaves de acesso a APIs.
3. Escolha Criar nova chave de API.
4. Insira uma descrição e selecione Chave de API somente para leitura.
5. Escolha Create Key (Criar chave).
6. Copie e salve a chave da API. Você precisará disso mais tarde AppFabric. Se você fechar a página antes de salvar a chave da API, deverá gerar uma nova chave da API e salvá-la. Essa chave deve ser dedicada AppFabric para evitar o compartilhamento do limite de taxa da PagerDuty API com suas outras integrações.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do locatário da sua conta do PagerDuty é o URL base da sua conta. É possível encontrar isso fazendo login no PagerDuty e copiando da barra de endereços do navegador da Web. O ID do locatário deve seguir um dos seguintes formatos:

- Para contas dos EUA, *subdomain*`.pagerduty.com`
- Para contas da UE, *subdomain*`.eu.pagerduty.com`

Nome do locatário

Insira um nome que identifique essa organização exclusiva do PagerDuty. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

Token de contas de serviço

AppFabric solicitará o token da sua conta de serviço. O token da conta de serviço AppFabric é a chave de acesso à API que você criouCriar uma chave de acesso à API.

Ping Identity

Na Ping Identity, acreditamos em tornar as experiências digitais seguras e perfeitas para todos os usuários, sem concessões. É por isso que mais da metade das empresas da Fortune 100 optam pela Ping Identity para proteger as interações digitais de seus usuários e, ao mesmo tempo, tornar as experiências tranquilas. Em 23 de agosto de 2023, a Ping Identity e a ForgeRock se reuniram para oferecer mais opções, maior experiência e uma solução de identidade mais completa para clientes e parceiros. Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioPing Identity, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Ping Identity
- Conectando-se AppFabric à sua Ping Identity conta

AppFabric suporte para Ping Identity

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doPing Identity.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Ping Identity de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter uma conta Essential, Plus ou Premium da Ping Identity. Para obter mais informações sobre como criar ou atualizar para o tipo de plano aplicável do Ping Identity, consulte definição de preços de todos os atributos do Ping Identity no site do Ping Identity.

- Você deve ter o perfil Somente leitura de dados de identidade em sua conta da Ping Identity. É possível adicionar perfis à sua conta concedendo perfis para sua aplicação. Para obter mais informações sobre perfis, consulte Perfis no site de suporte da Ping Identity.

Considerações sobre limites de taxa

A Ping Identity não publica limites de taxas. Você deve criar um caso de suporte ou entrar em contato com sua equipe de sucesso do cliente da Ping Identity. Se a combinação de seus aplicativos de Ping Identity API existentes AppFabric e seus aplicativos Ping Identity de API excederem os limites, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Ping Identity conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Ping Identity Para encontrar as informações necessárias para autorizar Ping Identity AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Ping Identity uso do OAuth. Para criar um aplicativo OAuth no Ping Identity, siga estas etapas:

1. Siga as instruções na seção Criar uma conexão de aplicação no guia PingOne para desenvolvedores no site Ping Identity.
2. Depois de criar a aplicação, personalize os tipos de concessão.
    a. Quando estiver conectado à aplicação, escolha a guia Configuração e clique no ícone de lápis para fazer alterações na configuração existente.
    b. Em Tipo de concessão, selecione Código de autorização. Mantenha a Aplicação de PKCE como OPCIONAL.
    c. Selecione Atualizar token e escolha suas durações de atualização.

3. Use um URL de redirecionamento com o formato a seguir em Redirecionar URL/URL de retorno de chamada.

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

   Nesse URL, <region>está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do inquilino em AppFabric é o nome da sua Ping Identity instância. É possível encontrar sua ID de locatário na barra de endereços do navegador. Por exemplo, *API_PATH*`/v1/environments/`*environmentID*. Onde *API_PATH* representa o domínio regional do servidor PingOne, como `api.pingone.com`, e *environmentID* representa o ID do ambiente indicado nas propriedades do ambiente da aplicação. Para obter mais informações sobre propriedades do ambiente, consulte Propriedades do ambiente no site Ping Identity.

Nome do locatário

Insira um nome que identifique essa organização exclusiva do Ping Identity. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. Para encontrar sua ID de cliente no Ping Identity, siga as etapas abaixo:

1. Faça login no console de administração do PingOne e escolha Aplicações.
2. Escolha a aplicação na lista.
3. Escolha a guia Visão geral e, em seguida, procure o valor do ID do cliente.

Segredo do cliente

AppFabric solicitará um segredo do cliente. Para descobrir seu segredo do cliente no Ping Identity, siga as etapas abaixo:

1. Faça login no console de administração do PingOne e escolha Aplicações.
2. Escolha a aplicação na lista.
3. Escolha a guia Visão geral e, em seguida, procure o valor do Segredo do cliente.

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up Ping Identity para aprovar a autorização. Para aprovar a AppFabric autorização, escolha permitir.

Salesforce

Salesforcefabrica software baseado em nuvem projetado para ajudar as empresas a encontrar mais clientes potenciais, fechar mais negócios e impressionar os clientes com um serviço incrível. Salesforce's O Customer 360 oferece um conjunto completo de produtos, une equipes de vendas, serviços, marketing, comércio e TI com uma visão única e compartilhada das informações do cliente, ajudando as organizações a desenvolver relacionamentos tanto com clientes quanto com funcionários. Você pode usar AWS AppFabric para receber registros de auditoria e dados do usuárioSalesforce, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Salesforce
- Conectando-se AppFabric à sua Salesforce conta

AppFabric suporte para Salesforce

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doSalesforce.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Salesforce de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter uma edição Performance, Enterprise ou Unlimited doSalesforce. Entre em contato Salesforce para fazer o upgrade para uma dessas edições.
- Se você deseja AppFabric transferir arquivos de registro de eventos por hora com um conjunto completo de eventos de registro deSalesforce, você deve se inscrever no Event Monitoring como parte do Shield Features ofSalesforce. Caso contrário, AppFabric transferirá eventos limitados (ou seja, login, logout InsecureExternalAssets, uso total da API, violação de CORS e eventos HostnameRedirects ELF) do arquivo de log diário Salesforce's padrão. Você pode verificar se sua Salesforce conta já está inscrita no Shield Features acessando Configuração > Gerenciador de eventos. Se você ver 19 ou mais eventos listados, sua conta está inscrita no Monitoramento de Eventos. Se você não tem monitoramento de eventos, pode comprar uma assinatura desse complemento entrando Salesforce em contato com.
- Você precisa optar pela geração do Arquivo de Registro de Eventos nas Salesforce configurações.
- Você deve usar o Perfil do Administrador do Sistema para criar um aplicativo OAuth e fazer login com as mesmas credenciais do. AppFabric

> **Note**
>
> O uso total da API, o registro de violação do CORS, os redirecionamentos de nome de host, os ativos externos inseguros, os eventos de login e logout estão disponíveis sem custo adicional nas edições suportadas do. Salesforce Entre em contato Salesforce para comprar os demais tipos de eventos. Para obter mais informações sobre os tipos de Salesforce eventos, consulte Tipos de eventos EventLogFile compatíveis no Salesforce site. AppFabric pode suportar até 100.000 eventos por tipo de evento por instância do arquivo de log (diariamente ou de hora em hora, dependendo da assinatura do complemento Event Monitoring). Um arquivo de log que exceda o limite pode fazer com que todo o arquivo de log seja excluído da ingestão.

Considerações sobre limites de taxa

O Salesforce impõe limites de taxa na API do Salesforce. Para obter mais informações sobre os limites de taxa da Salesforce API, consulte Limites e alocações de solicitações de API no Salesforce site. Se a combinação de seus aplicativos de Salesforce API existentes AppFabric e seus aplicativos de API excederem Salesforce's os limites, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Você pode ver um atraso de até 6 horas no arquivo de registro diário ou até 29 horas de atraso no arquivo de log de hora em hora para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Salesforce conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Salesforce Para encontrar as informações necessárias para autorizar Salesforce AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Salesforce uso do OAuth. Para criar um aplicativo OAuth no Salesforce, siga estas etapas:

1. Faça login na sua Salesforce conta.
2. Acesse a página de configuração conforme descrito na Salesforcedocumentação.
3. Pesquise o App Manager na busca rápida.
4. Escolha Novo aplicativo conectado.
5. Insira as informações necessárias nos campos do formulário.
6. Escolha Ativar configurações de OAuth.
7. Certifique-se de desativar as seguintes opções:
   - Exigir chave de prova para extensão de troca de código (PKCE) para fluxos de autorização compatíveis
   - Exigir segredo para o fluxo do servidor Web
   - Exigir segredo para Refresh Token Flow
8. Insira uma URL com o seguinte formato na caixa de texto URL de retorno de chamada e escolha Salvar alterações.

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

   Nesse URL, <region>está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da

Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

9. Preencha os escopos conforme necessário (descrito na Escopos necessários seção a seguir). Todos os outros campos podem ser deixados com seus valores padrão.
10. Escolha Salvar.
11. Conclua as etapas a seguir para verificar a política de token de atualização para o novo aplicativo OAuth:
    a. Na página Configuração, insira Aplicativos conectados na caixa de texto Busca rápida e escolha Gerenciar aplicativos conectados.
    b. Escolha Editar ao lado do aplicativo recém-criado.
    c. Certifique-se de que o token de atualização seja válido até que a opção revogada seja selecionada.
    d. Salve as alterações.
12. Conclua as etapas a seguir para verificar se os registros de auditoria estão sendo gerados:
    a. Na página Configuração, insira Arquivo de registro de eventos na caixa de texto Busca rápida e escolha Navegador de arquivos de registro de eventos.
    b. Confirme se os registros de eventos estão listados no Navegador de arquivos de registro de eventos.
13. Navegue até o aplicativo criado e escolha Exibir no menu suspenso.
14. Escolha Gerenciar detalhes do consumidor.

    Você será redirecionado para uma nova guia na qual precisará verificar sua identidade. Nessa guia, anote os valores da Chave do Consumidor e do Segredo do Consumidor. Você precisará deles mais tarde para fazer login.

Escopos necessários

Você deve adicionar os seguintes escopos ao seu aplicativo OAuth do Salesforce:

- Gerencie os dados do usuário por meio de APIs (`API`).
- Execute a solicitação a qualquer momento (`refresh_tokeneoffline_access`).

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do inquilino em AppFabric é o subdomínio do seu Salesforce Meu domínio. Você pode encontrar seu subdomínio Meu domínio na barra de endereço do seu navegador entre `https://` e. `.my.salesforce.com`

Para encontrar seu Salesforce Meu domínio, use as instruções a seguir na tela Salesforce inicial.

1. Acesse a página de configuração conforme descrito na Salesforcedocumentação.
2. Pesquise Configurações da empresa na busca rápida e escolha Meu domínio nos resultados.

Nome do locatário

Insira um nome que identifique essa Salesforce organização exclusiva. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. Para encontrar sua ID de cliente no Salesforce, siga as etapas abaixo:

1. Navegue até a página de configuração.
2. Escolha Configuração e, em seguida, selecione Gerenciador de aplicativos.
3. Escolha o aplicativo criado e escolha Exibir no menu suspenso.
4. Escolha Gerenciar detalhes do consumidor. Você será redirecionado para uma nova guia.
5. Verifique sua identidade e, em seguida, procure o valor da Chave do Consumidor.
6. Insira a Chave do Consumidor no campo ID do cliente em AppFabric.

Segredo do cliente

AppFabric solicitará o segredo do seu cliente. O segredo do cliente AppFabric é o segredo do consumidor emSalesforce. Para descobrir seu segredoSalesforce, use as seguintes etapas:

1. Navegue até a página de configuração.

2. Escolha Configuração e, em seguida, selecione Gerenciador de aplicativos.
3. Escolha o aplicativo criado e escolha Exibir no menu suspenso.
4. Escolha Gerenciar detalhes do consumidor. Você será redirecionado para uma nova guia.
5. Verifique sua identidade e, em seguida, procure o valor do Segredo do Consumidor.
6. Insira o Segredo do Consumidor no campo segredo do cliente em AppFabric.

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up Salesforce para aprovar a autorização. Na página de aprovação, certifique-se de usar a função de administrador do Salesforce sistema ou um Salesforce usuário que tenha permissões de usuário para visualizar arquivos de registro de eventos e API habilitadas para API ao autorizar. Escolha Permitir para aprovar a AppFabric autorização.

ServiceNow

ServiceNowé uma provedora líder de serviços baseados em nuvem que automatizam as operações corporativas de TI. ServiceNowO ITOM da oferece às empresas visibilidade e controle completos de todo o seu ambiente de TI, incluindo infraestrutura virtualizada e em nuvem. Ele simplifica o mapeamento, a entrega e a garantia do serviço, consolidando dados de infraestrutura e serviços de TI em um único sistema de registro. Além disso, automatiza e simplifica os principais processos, incluindo gerenciamento de eventos, incidentes, problemas, configurações e mudanças. Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioServiceNow, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para ServiceNow
- Considerações sobre o atraso de dados
- Conectando-se AppFabric à sua ServiceNow conta

AppFabric suporte para ServiceNow

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doServiceNow.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria ServiceNow de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você pode usar AppFabric com qualquer tipo de ServiceNow plano.
- Você deve ter um usuário com o perfil de Administrador em sua conta do ServiceNow.
- Você deve ter uma instância do ServiceNow.

Considerações sobre limites de taxa

O ServiceNow impõe limites de taxa na API do ServiceNow. Para obter mais informações sobre os limites de taxas de API do ServiceNow, consulte Limites de taxa de recepção API REST no site do ServiceNow. Se a combinação de seus aplicativos de ServiceNow API existentes AppFabric e seus aplicativos de API excederem os limites, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua ServiceNow conta

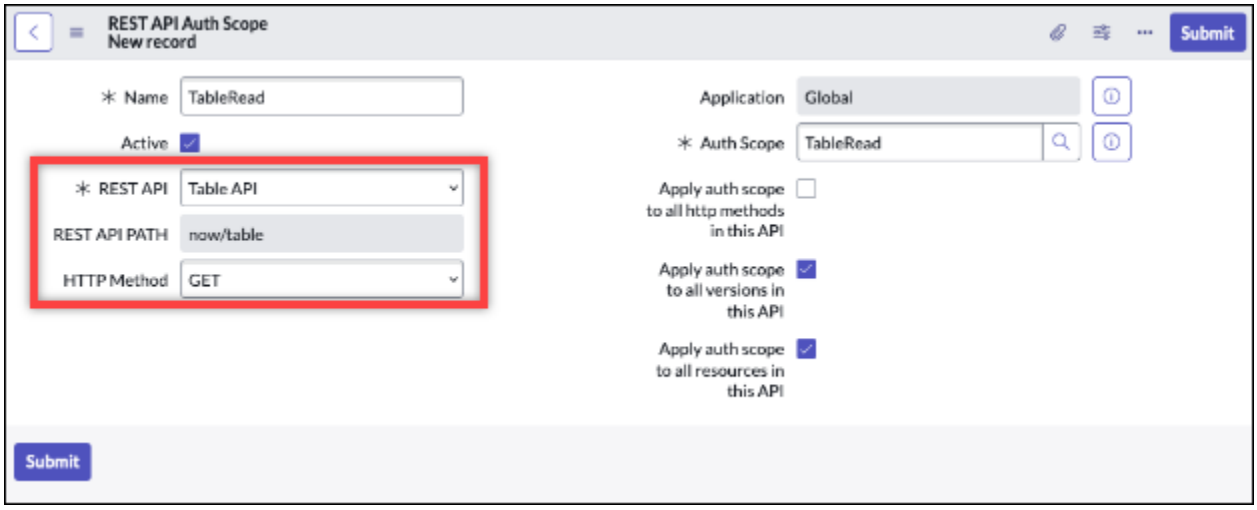
Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. ServiceNow Use as etapas a seguir para encontrar as informações necessárias para ServiceNow autorizar AppFabric.

Criar um aplicativo OAuth

O Now Platform é compatível com o OAuth 2.0 – Concessão de autorização para clientes públicos para gerar um token de acesso.

1. Registre seu aplicativo OAuth. Isso requer as três etapas a seguir. Para obter mais informações sobre como executar essas etapas, consulte Registre seu aplicativo com o ServiceNow no site do ServiceNow.

a. Registre o aplicativo e certifique-se de que o escopo de autenticação tenha acesso à API de tabela, com um PATH da API REST de agora/tabela e um método HTTP de GET, conforme mostrado no exemplo a seguir.



b. Gerar um código de autorização.

c. Gerar um token de portador usando o código de autorização.

2. Usar um URL de redirecionamento com o formato a seguir.

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

Nesse URL, <region>está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará um ID de inquilino. O ID do inquilino em AppFabric é o nome da sua instância. É possível encontrar sua ID de locatário na barra de endereços do navegador. Por exemplo, *example* é a ID de locatário no seguinte URL `https://example.service-now.com`.

Nome do locatário

Insira um nome que identifique essa ServiceNow organização exclusiva. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. Siga as etapas abaixo para encontrar sua ID de cliente no ServiceNow.

1. Navegue até o console ServiceNow.
2. Escolha OAuth do sistema e, depois, escolha a guia Registro do aplicativo.
3. Escolha o aplicativo.
4. Insira o ID do cliente do seu cliente OAuth no campo ID do cliente em. AppFabric

Segredo do cliente

AppFabric solicitará um segredo do cliente. Siga etapas abaixo para descobrir seu segredo de cliente no ServiceNow.

1. Navegue até o console ServiceNow.
2. Escolha OAuth do sistema e, depois, escolha a guia Registro do aplicativo.
3. Escolha o aplicativo.
4. Insira o segredo do cliente do seu aplicativo OAuth no campo Segredo do cliente em. AppFabric

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up ServiceNow para aprovar a autorização. Escolha Permitir para aprovar a AppFabric autorização.

Singularity Cloud

A Singularity Cloud plataforma protege sua empresa contra ameaças de todas as categorias, em todos os estágios. Sua inteligência artificial patenteada estende a segurança desde assinaturas e padrões conhecidos até os ataques mais sofisticados, como dia zero e ransomware.

Você pode usar AWS AppFabric para receber registros de auditoria e dados do usuárioSingularity Cloud, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar

os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

> **Note**
>
> Singularity Clouda documentação só pode ser acessada depois que você fizer login na sua Singularity Cloud conta. Portanto, não podemos vincular diretamente à Singularity Cloud documentação deste documento.

Tópicos

- AppFabric suporte para Singularity Cloud
- Conectando-se AppFabric à sua Singularity Cloud conta

AppFabric suporte para Singularity Cloud

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doSingularity Cloud.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Singularity Cloud de destinos compatíveis, você deve ter uma função de administrador em sua Singularity Cloud conta. Para obter mais informações sobre os limites de taxa da Singularity Cloud API, faça login na sua conta do Singularity Cloud, navegue pela seção de documentação e pesquise funções.

Considerações sobre limites de taxa

O Singularity Cloud impõe limites de taxa na API do Singularity Cloud. Para obter mais informações sobre os limites de taxa da Singularity Cloud API, faça login na sua conta do Singularity Cloud, navegue pela seção de documentação e pesquise os limites de taxa da API.

Considerações sobre o atraso de dados

Você pode ver um atraso de até 30 minutos em um evento de auditoria para ser entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Singularity Cloud conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Singularity Cloud Para encontrar as informações necessárias para autorizar Singularity Cloud AppFabric, use as etapas a seguir.

Crie um token de API para Singularity Cloud

Conclua o procedimento a seguir para criar um token de API associado a um usuário do serviço. O token da API não será vinculado a um usuário ou endereço de e-mail específico do console.

> **Note**
>
> Crie um novo usuário ou copie o usuário do serviço para obter um novo token de API antes ou depois da expiração do token de API do usuário do serviço.

1. Faça login na sua conta da Singularity Cloud.
2. Na barra de ferramentas Configurações, escolha Usuários e, em seguida, escolha Usuários do serviço.
3. Escolha Ações e, em seguida, selecione Criar novo usuário de serviço.
4. Na página Criar novo usuário do serviço, insira um nome, descrição e data de expiração para o usuário do serviço.
5. Escolha Próximo.
6. Na seção Selecionar escopo de acesso, selecione o escopo.
   - Selecione Conta para o nível de acesso.
   - Selecione a conta da qual você deseja obter registros de auditoria.
7. Escolha Create User.

   O token da API é gerado. Uma janela é aberta e mostra a sequência de caracteres do token com uma mensagem indicando que essa é a última vez que você pode ver o token.
8. (Opcional) Escolha Copiar token de API e armazene-o em um local seguro.
9. Escolha Fechar.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do inquilino AppFabric será o subdomínio do endereço do Sentinel One site em que você faz login no serviço. Por exemplo, se você fizer login na sua Singularity Cloud conta no `example-company-1.sentinelone.net` endereço, seu ID de inquilino será`example-company-1`.

Nome do locatário

Insira um nome que identifique essa Singularity Cloud organização exclusiva. AppFabric usa o nome do inquilino para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

Token de contas de serviço

Use o token que você gerou usando as etapas na Crie um token de API para Singularity Cloud seção deste guia. Se você perder ou não conseguir localizar o token, poderá gerar um novo seguindo as mesmas etapas novamente.

> **Note**
>
> Se um novo token de API for gerado no console do Singularity Cloud durante AppFabric a ingestão dos registros de auditoria, as ingestões serão interrompidas. Se isso acontecer, você precisará atualizar a autorização do aplicativo com um novo token de API para retomar a ingestão do registro de auditoria.

Slack

O Slack tem a missão de tornar a vida profissional das pessoas mais simples, mais agradável e mais produtiva. É a plataforma de produtividade para empresas clientes que melhora o desempenho ao capacitar todos com automação sem código, simplificando a pesquisa e o compartilhamento de conhecimento, além de manter as equipes conectadas e engajadas à medida que avançam no trabalho em conjunto. Como parte integrante do Salesforce, o Slack está profundamente incorporado ao Salesforce Customer 360, aumentando a produtividade das equipes de vendas, serviços e marketing. Para saber mais e começar a usar o Slack gratuitamente, visite slack.com.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioSlack, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF)

e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Slack
- Conectando-se AppFabric à sua Slack conta

AppFabric suporte para Slack

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doSlack.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Slack de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter um plano Enterprise Grid com Slack. Para obter mais informações, consulte Uma introdução ao Enterprise Grid do Slack no site do Slack.
- Você deve ter um usuário com o perfil de Proprietário da organização em sua conta do Slack. Para obter mais informações sobre perfis, consulte Tipos de perfis no Slack, disponível na Central de Ajuda do Slack, no site do Slack.

Considerações sobre limites de taxa

O Slack impõe limites de taxa na API do Slack. Para obter mais informações sobre os limites de taxas de API do Slack, consulte Limites de taxa no Guia de uso de API do Slack no site do Slack. Se a combinação de seus aplicativos de Slack API existentes AppFabric e seus aplicativos de API excederem o limite, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Slack conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Slack Para encontrar as informações necessárias para autorizar Slack AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Slack uso do OAuth. Há duas maneiras de criar um aplicativo OAuth: Usando um manifesto de aplicativo ou Do zero. Para criar um aplicativo OAuth no Slack, siga as etapas abaixo:

Using an app manifest

1. Navegue até a Interface do usuário de gerenciamento de aplicativos do Slack em seu navegador.
2. Selecione Create novo aplicativo.
3. Escolha A partir de um manifesto de aplicativo.
4. Escolha o espaço de trabalho para o qual você deseja AppFabric autorizar.
5. Na caixa Inserir manifesto do aplicativo abaixo, escolha JSON e substitua o JSON existente pelo que segue. <region>Substitua pelo apropriado Região da AWS (por exemplo, *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 e salve a ID e o segredo do cliente na página Informações básicas.
7. Para o escopo do `auditLogs:read`, você deve ativar a distribuição pública do seu aplicativo. Para mais informações, consulte Ativação da distribuição pública no site do Slack.

From scratch

1. Escolha Do zero na tela Criar um aplicativo.
2. Dê um nome ao seu aplicativo e escolha um espaço de trabalho.
3. Copie e salve a ID e o segredo do cliente na página Informações básicas.
4. Na página OAuth e permissões, escolha a opção Segurança avançada de tokens via rotação de tokens.
5. Adicione um URL com o seguinte formato na seção URLs de redirecionamento da página OAuth e permissões.

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

   Nesse URL, *<region>* está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.
6. Para o escopo do `auditLogs:read`, você deve ativar a distribuição pública do seu aplicativo. Para mais informações, consulte Ativação da distribuição pública no site do Slack.

Escopos necessários

> **Note**
>
> Esta seção só será aplicável se você optar por criar o aplicativo OAuth do zero. Ignore esta seção se você optar por usar o manifesto do aplicativo para criar uma autorização de aplicativo.

Você deve adicionar os seguintes escopos de token de usuário na página OAuth e permissões do seu aplicativo OAuth do Slack:

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

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do inquilino AppFabric é o ID do seu Slack espaço de trabalho. Para obter sua ID de locatário, siga as instruções em Localize seu URL do Slack na SlackCentral de Ajuda do site do Slack. O URL de seu espaço de trabalho do Slack tem um formato semelhante a `examplecorp.slack.com` ou `examplecorp.enterprise.slack.com`. A ID de locatário de que você precisa é `examplecorp` sem `.slack.com` ou `.enterprise.slack.com`.

Nome do locatário

Insira um nome que identifique o ID do seu Slack espaço de trabalho. AppFabricusa o nome do inquilino para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo

ID de cliente

AppFabric solicitará o ID do cliente do seu aplicativo Slack OAuth. Para encontrar a ID de cliente, siga as etapas abaixo:

1. Navegue até a Interface do usuário de gerenciamento de aplicativos do Slack em seu navegador.
2. Escolha o aplicativo OAuth com o qual você usa. AppFabric
3. Insira a ID do cliente da página Informações básicas no campo ID do cliente em AppFabric.

Segredo do cliente

AppFabric solicitará o segredo do cliente do seu aplicativo Slack OAuth. Para encontrar o segredo do cliente, siga as etapas abaixo:

1. Navegue até a interface do usuário de gerenciamento de aplicativos do Slack em seu navegador.
2. Escolha o aplicativo OAuth com o qual você usa. AppFabric
3. Insira o segredo do cliente da página Informações básicas no campo Segredo do cliente em AppFabric.

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up Slack para aprovar a autorização. Para aprovar a AppFabric autorização, escolha permitir.

Smartsheet

Smartsheet é uma plataforma de gerenciamento de trabalho que ajuda você a alinhar atividades, pessoas e tecnologia em toda a sua empresa. Smartsheet oferece um conjunto robusto de recursos de nível corporativo para capacitar todos a gerenciar projetos, automatizar fluxos de trabalho e criar rapidamente soluções em escala, criando um ambiente para a inovação e mantendo a segurança e a conformidade.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioSmartsheet, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Smartsheet
- Conectando-se AppFabric à sua Smartsheet conta

AppFabric suporte para Smartsheet

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doSmartsheet.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Smartsheet de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter uma conta Comercial, Empresarial ou Avançada do Smartsheet. Para obter mais informações sobre como criar ou atualizar sua conta Smartsheet, consulte definição de preços do Smartsheet ou Avançado do Smartsheet no site do Smartsheet.
- Você deve realizar o processo de registro do desenvolvedor do Smartsheet.

Considerações sobre limites de taxa

O Smartsheet impõe limites de taxa na API do Smartsheet. Para obter mais informações sobre os limites de taxa de API do Smartsheet, consulte Limitação de taxa na Referência de APIs do Smartsheet no site do Smartsheet.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Smartsheet conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Smartsheet Para encontrar as informações necessárias para autorizar Smartsheet AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Smartsheet uso do OAuth. Para criar um aplicativo OAuth no Smartsheet, siga as etapas abaixo:

1. Navegue até as ferramentas do desenvolvedor em sua conta do Smartsheet.
2. Escolha Criar novo aplicativo na tela de ferramentas do desenvolvedor.
3. Preencha todos os campos de entrada na tela Criar novo aplicativo.
4. Use qualquer valor exclusivo para o URL do aplicativo e Contato/suporte do aplicativo.
5. Usar um URL de redirecionamento com o formato a seguir quando o aplicativo redireciona o URL.

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

Nesse URL, *<region>* está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

6. Escolha Salvar.
7. Copie e salve a ID do cliente e o segredo do aplicativo.

Escopos necessários

Smartsheetnão exige que você adicione explicitamente escopos à sua configuração do OAuth. AppFabric solicitará os seguintes escopos na solicitação de autorização para sua Smartsheet conta:

- `READ_EVENTS`
- `READ_USERS`

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do inquilino AppFabric é o ID Smartsheet da sua conta.

Nome do locatário

AppFabric solicitará seu ID de inquilino. Insira qualquer valor que identifique sua conta do Smartsheet de forma exclusiva.

ID de cliente

AppFabric solicitará seu ID de cliente. O ID do cliente em AppFabric é o ID do cliente do seu Smartsheet aplicativo. Para encontrar sua ID do cliente do aplicativo no Smartsheet, siga etapas abaixo:

1. Navegue até as ferramentas do desenvolvedor em sua conta do Smartsheet.
2. Selecione o aplicativo OAuth que você usa para se conectar. AppFabric
3. Insira o ID do cliente do aplicativo na tela Perfil do aplicativo no campo ID do cliente em AppFabric.

Segredo do cliente

AppFabric solicitará o segredo do seu cliente. O segredo do cliente AppFabric é o segredo Smartsheet do seu aplicativo. Para descobrir o segredo do aplicativo no Smartsheet, siga as etapas abaixo:

1. Navegue até as ferramentas do desenvolvedor em sua conta do Smartsheet.
2. Selecione o aplicativo OAuth que você usa para se conectar. AppFabric
3. Insira o segredo do aplicativo na tela Perfil do aplicativo no campo Segredo do cliente em AppFabric.

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up Smartsheet para aprovar a autorização. Para aprovar a AppFabric autorização, escolha Permitir.

Terraform Cloud

HashiCorp Terraform Cloudé o produto de provisionamento multinuvem mais usado no mundo. O Terraform ecossistema tem mais de 3.000 provedores, 14.000 módulos e 250 milhões de downloads. Terraform Cloudé a maneira mais rápida de adotarTerraform, fornecendo tudo o que profissionais, equipes e empresas globais precisam para criar e colaborar na infraestrutura e gerenciar riscos de segurança, conformidade e restrições operacionais. Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioTerraform Cloud, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Terraform Cloud
- Conectando-se AppFabric à sua Terraform Cloud conta

AppFabric suporte para Terraform Cloud

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doTerraform Cloud.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Terraform Cloud de destinos compatíveis, você deve atender aos seguintes requisitos:

- Para acessar os registros de auditoria, você deve ter um plano Terraform Cloud Plus Edition e ser o proprietário da organização. Para obter mais informações sobre Terraform Cloud os planos, consulte os Terraformpreços no HashiCorp Terraform site.
- Os registros de auditoria TBD estão disponíveis para organizações que podem ser criadas a partir da Terraform Cloud conta.

Considerações sobre limites de taxa

O Terraform Cloud impõe limites de taxa na API do Terraform Cloud. Para obter mais informações sobre os limites de taxa de Terraform Cloud API, consulte Limitação de taxa de API na configuração geral de administração de Terraform Cloud desenvolvedores no Terraform Cloud site. Se a combinação de seus aplicativos de Terraform Cloud API existentes AppFabric e seus aplicativos Terraform Cloud de API excederem os limites, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Terraform Cloud conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Terraform Cloud Para encontrar as informações necessárias para autorizar Terraform Cloud AppFabric, use as etapas a seguir.

Crie um token de API da organização

AppFabric se integra ao Terraform Cloud uso de um token de API da organização. Para obter mais informações sobre os tokens da API da Terraform Cloud organização, consulte Tokens da API da organização. Para criar uma organização, siga as instruções em Creating Organizations. Para criar um token de API da organizaçãoTerraform Cloud, use as etapas a seguir.

1. Navegue até a Terraform Cloud página de login e faça login.
2. Escolha Organização, Configurações no painel do lado esquerdo e, em seguida, escolha Tokens de API.
3. Em Tokens da organização, escolha Criar um token da organização e, em seguida, escolha Gerar token.
4. (Opcional) Insira a data ou a hora de expiração do token ou crie um token que nunca expire.
5. Copie e salve o token. Você precisará disso mais tarde AppFabric. Se você fechar a página antes de salvar o token, deverá revogar o token antigo e criar um novo.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará um ID de inquilino. O ID do inquilino Terraform Cloud da sua conta é o URL da organização atual da sua conta. Você pode encontrar isso fazendo login na sua Terraform Cloud organização e copiando a URL atual da organização. O ID do locatário deve seguir um dos seguintes formatos:

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

Nome do locatário

Insira um nome que identifique essa organização exclusiva do Terraform Cloud. AppFabric usa o nome do inquilino para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

Token de contas de serviço

AppFabric solicitará o token da sua conta de serviço. O token da conta de serviço AppFabric é o token da API da organização em que você criouCrie um token de API da organização.

Webex by Cisco

A Cisco é líder mundial em tecnologia que impulsiona a Internet. A Cisco inspira novas possibilidades ao repensar seus aplicativos, proteger seus dados, transformar sua infraestrutura e capacitar suas equipes visando um futuro global e inclusivo.

Sobre o Webex by Cisco

O Webex é o principal fornecedor de soluções de colaboração baseadas em nuvem que incluem videoconferências, chamadas, mensagens, eventos, soluções de experiência do cliente, como centro de atendimento ao cliente e dispositivos de colaboração personalizados. O foco do Webex voltado para proporcionar experiências de colaboração inclusivas estimula a inovação, que utiliza IA e Machine Learning para eliminar os obstáculos da geografia, do idioma, da personalidade e da familiaridade com a tecnologia. Suas soluções são reforçadas pela segurança e privacidade desde o design. O Webex trabalha com os principais aplicativos de negócios e produtividade do mundo, fornecidos por meio de um único aplicativo e interface. Saiba mais em webex.com.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioWebex, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Webex
- Conectando-se AppFabric à sua Webex conta

AppFabric suporte para Webex

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doWebex.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Webex de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter um plano Collaboration Flex, Meet Plan, Call Plan ou superior. Para obter mais informações sobre como criar ou atualizar para o tipo de plano aplicável do Webex, consulte definição de preços de todos os atributos do Webex no site do Webex.
- Sua conta deve ter a licença Pro Pack para acessar os eventos de auditoria de segurança fornecidos por uma das AuditLog APIs da Cisco.
- Você deve ter um usuário com o perfil Administrador organizacional > Administrador completo.
- A configuração de Perfis de administrador para seu Administrador completo deve ter a opção Diretor de conformidade habilitada.

Considerações sobre limites de taxa

O Webex impõe limites de taxa na API do Webex. Para obter mais informações sobre os limites de taxas de API do Webex, consulte Limites de taxa no Guia do desenvolvedor do Webex no site do Webex. Se a combinação de seus aplicativos de Webex API existentes AppFabric e seus aplicativos de API excederem o limite, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Webex conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Webex Para encontrar as informações necessárias para autorizar Webex AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Webex uso do OAuth. Para criar um aplicativo OAuth no Webex, siga as etapas abaixo:

1. Siga as instruções na seção Registro da sua integração na página Integrações e autorização do Guia do desenvolvedor do Webex.
2. Usar um URL de redirecionamento com o formato a seguir.

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

   Nesse URL, *<region>* está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Escopos necessários

Você deve adicionar os seguintes escopos ao seu aplicativo OAuth do Webex:

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

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. A ID do inquilino AppFabric é a ID Webex da sua organização. Para obter informações sobre como encontrar a ID do Webex da sua organização, consulte Pesquisar a ID da sua organização no CiscoWebex Control Hub no site da Central de Ajuda do Webex.

Nome do locatário

Insira um nome que identifique essa Webex instância exclusiva. AppFabricusa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará seu ID de Webex cliente. Para encontrar sua ID de cliente do Webex, siga as etapas abaixo:

1. Faça login em sua conta do Webex em https://developer.webex.com.
2. Escolha seu avatar no canto superior direito.
3. Escolha Meus aplicativos Webex.
4. Escolha o aplicativo OAuth2 para o qual você usa. AppFabric
5. Insira a ID do cliente nesta página no campo ID do cliente em AppFabric.

Segredo do cliente

AppFabric solicitará o segredo Webex do seu cliente. Webexsó apresenta o segredo do seu cliente uma vez quando você cria seu aplicativo OAuth pela primeira vez. Para gerar um novo segredo do cliente se você não salvou o segredo inicial do cliente, siga as etapas abaixo:

1. Faça login em sua conta do Webex em https://developer.webex.com.
2. Escolha seu avatar no canto superior direito.

3. Escolha Meus aplicativos Webex.
4. Escolha o aplicativo OAuth2 para o qual você usa. AppFabric
5. Nesta página, gere um novo segredo do cliente.
6. Insira o novo segredo do cliente no campo Segredo do cliente em AppFabric.

Aprovar autorização

Depois de criar a autorização do aplicativo, AppFabric você receberá uma janela pop-up Webex para aprovar a autorização. Para aprovar a AppFabric autorização, escolha aceitar.

Zendesk

A Zendesk iniciou a revolução da experiência do cliente em 2007, permitindo que qualquer empresa em todo o mundo disponibilizasse seu atendimento ao cliente on-line. Hoje, a Zendesk é patrona de um ótimo serviço em todos os lugares, para todos, e potencializa bilhões de conversas, conectando mais de 100.000 marcas a centenas de milhões de clientes por telefone, bate-papo, e-mail, mensagens, canais sociais, comunidades, sites de avaliação e centrais de ajuda. Os produtos Zendesk são feitos com amor para serem amados. A empresa foi concebida em Copenhague, Dinamarca, construída e cultivada na Califórnia, EUA, e hoje emprega mais de 6.000 pessoas em todo o mundo.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioZendesk, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Zendesk
- Conectando-se AppFabric à sua Zendesk conta

AppFabric suporte para Zendesk

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doZendesk.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Zendesk de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter uma conta Zendesk Suite Enterprise ou Enterprise Plus, ou uma conta Zendesk Support Enterprise. Para obter mais informações sobre como criar ou atualizar para uma conta Zendesk Enterprise, consulte Como verificar seu tipo de plano do Zendesk no site Zendesk.
- Você deve ter um usuário com o perfil de Administrador em sua conta do Zendesk. Para obter mais informações sobre funções, consulte Compreendendo as funções de usuário de suporte do Zendesk no site Zendesk.

Considerações sobre limites de taxa

O Zendesk impõe limites de taxa na API do Zendesk. Para obter mais informações sobre os limites de taxas de API do Zendesk, consulte Limites de taxa no Guia do desenvolvedor do Zendesk no site do Zendesk. Se a combinação de seus aplicativos de Zendesk API existentes AppFabric e seus aplicativos de API excederem o limite, os registros de auditoria que aparecem AppFabric podem ser adiados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de até 30 minutos para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados. No entanto, isso pode ser personalizado ao nível da conta. Para obter ajuda, entre em contato com AWS Support.

Conectando-se AppFabric à sua Zendesk conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Zendesk Para encontrar as informações necessárias para autorizar Zendesk AppFabric, use as etapas a seguir.

Criar um aplicativo OAuth

AppFabric se integra ao Zendesk uso do OAuth. No Zendesk, você deve criar um aplicativo OAuth com as seguintes configurações:

1. Siga as instruções na seção Registrando seu aplicativo no Zendesk do artigo Como usar a autenticação OAuth com seu aplicativo no site de suporte do Zendesk.
2. Usar um URL de redirecionamento com o formato a seguir.

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

Nesse URL, *<region>* está o código Região da AWS no qual você configurou seu pacote de AppFabric aplicativos. Por exemplo, o código para a região Leste dos EUA (Norte da Virgínia) é `us-east-1`. Para essa região, o URL de redirecionamento é `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`.

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do locatário em AppFabric é seu Zendesk subdomínio. Para obter mais informações sobre como encontrar seu subdomínio do Zendesk, consulte Onde posso encontrar meu subdomínio do Zendesk no site do suporte de Zendesk.

Nome do locatário

Insira um nome que identifique essa organização exclusiva do Zendesk. AppFabric usa o nome do inquilino para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará um ID de cliente. O ID do cliente em AppFabric é o identificador exclusivo Zendesk da sua API. Para encontrar seu identificador exclusivo do Zendesk, use as seguintes etapas:

1. Navegue até a Central de administração em sua conta do Zendesk.
2. Escolha Aplicativos e integrações.
3. Escolha APIs, APIs do Zendesk.
4. Escolha a guia Clientes OAuth.
5. Escolha o aplicativo OAuth para o qual você criou. AppFabric
6. Insira o identificador exclusivo do seu cliente OAuth no campo ID do cliente em. AppFabric

Segredo do cliente

AppFabric solicitará um segredo do cliente. O segredo do cliente AppFabric é seu token Zendesk secreto. Zendeskapresenta seu token secreto somente uma vez quando você cria seu aplicativo

Zendesk OAuth pela primeira vez. Para gerar um novo token do segredo se você não salvou o token do segredo inicial, siga estas etapas:

1. Navegue até a Central de administração em sua conta do Zendesk.
2. Escolha Aplicativos e integrações.
3. Escolha APIs, APIs do Zendesk.
4. Escolha a guia Clientes OAuth.
5. Escolha o aplicativo OAuth para o qual você criou. AppFabric
6. Escolha o botão Regenerar ao lado do campo Token secreto.
7. Insira o novo token secreto no campo Segredo do cliente em AppFabric.

Aprovar autorização

Depois de criar a autorização do aplicativo em AppFabric, você receberá uma janela pop-up Zendesk para aprovar a autorização. Para aprovar a AppFabric autorização, escolha Permitir.

Zoom

Zoomé uma plataforma de colaboração all-in-one inteligente que torna a conexão mais fácil, mais imersiva e mais dinâmica para empresas e indivíduos. Zooma tecnologia coloca as pessoas no centro, permitindo conexões significativas, facilitando a colaboração moderna e impulsionando a inovação humana por meio de soluções como bate-papo em equipe, telefone, reuniões, contact center omnicanal na nuvem, gravações inteligentes, quadro branco e muito mais, em uma única oferta.

Você pode usar AWS AppFabric para fins de segurança receber registros de auditoria e dados do usuárioZoom, normalizar os dados no formato Open Cybersecurity Schema Framework (OCSF) e enviar os dados para um bucket do Amazon Simple Storage Service (Amazon S3) ou para um stream do Amazon Data Firehose.

Tópicos

- AppFabric suporte para Zoom
- Conectando-se AppFabric à sua Zoom conta

AppFabric suporte para Zoom

AppFabric suporta o recebimento de informações do usuário e registros de auditoria doZoom.

Pré-requisitos

Para usar AppFabric para transferir registros de auditoria Zoom de destinos compatíveis, você deve atender aos seguintes requisitos:

- Você deve ter um plano Zoom Pro, Business, Education ou Enterprise.
- Sua função de Zoom administrador deve ter permissão para criar aplicativos server-to-server OAuth. Para obter informações sobre como habilitar aplicativos server-to-server OAuth, consulte a seção Habilitar permissões da página OAuth de servidor para servidor no Guia do desenvolvedor no site. Zoom Zoom
- Sua função de administrador do Zoom deve ter permissão para visualizar os logs de atividades do administrador e fazer login/sair da atividade de auditoria. Para obter mais informações sobre como habilitar a permissão para visualizar atividades de auditoria, consulte Como usar o gerenciamento de funções e Como usar logs de atividades administrativas no site de suporte do Zoom.

Considerações sobre limites de taxa

O Zoom impõe limites de taxa na API do Zoom. Para obter mais informações sobre os limites de taxas de API do Zoom, consulte Limites de taxa no Guia do desenvolvedor do Zoom. Se a combinação de seus Zoom aplicativos existentes AppFabric e seus aplicativos excederem o limite, os registros de auditoria que aparecem AppFabric podem ser atrasados.

Considerações sobre o atraso de dados

Poderá ocorrer um atraso de aproximadamente 24 horas para que um evento de auditoria seja entregue ao seu destino. Isso se deve ao atraso nos eventos de auditoria disponibilizados pelo aplicativo, bem como às precauções tomadas para reduzir a perda de dados.

Conectando-se AppFabric à sua Zoom conta

Depois de criar seu pacote de aplicativos dentro do AppFabric serviço, você deve autorizar AppFabric com. Zoom Para encontrar as informações necessárias para autorizar Zoom AppFabric, use as etapas a seguir.

Crie um aplicativo server-to-server OAuth

AppFabric usa server-to-server OAuth com credenciais de aplicativo para integração com. Zoom Para criar um aplicativo server-to-server OAuth emZoom, siga as instruções em Criar um aplicativo OAuth de servidor para servidor no Guia do desenvolvedor. Zoom AppFabric não oferece suporte a Zoom webhooks e você pode pular a seção para adicionar assinaturas de webhooks.

Escopos necessários

Você deve adicionar os seguintes escopos ao seu aplicativo Zoom server-to-server OAuth:

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

Autorizações do aplicativo

ID de locatário

AppFabric solicitará seu ID de inquilino. O ID do inquilino em AppFabric é o ID da Zoom conta. Para encontrar sua ID de conta do Zoom, siga estas etapas:

1. Navegue até o marketplace do Zoom.
2. Escolha Gerenciar.
3. Escolha o aplicativo server-to-server OAuth para o qual você usa. AppFabric
4. Insira o ID da conta na página Credenciais do aplicativo no campo ID do locatário em. AppFabric

Nome do locatário

Insira um nome que identifique essa organização exclusiva do Zoom. AppFabric usa o nome do locatário para rotular as autorizações do aplicativo e todas as ingestões criadas a partir da autorização do aplicativo.

ID de cliente

AppFabric solicitará seu ID de cliente. Para encontrar sua ID de cliente do Zoom, siga estas etapas:

1. Navegue até o marketplace do Zoom.
2. Escolha Gerenciar.
3. Escolha o aplicativo server-to-server OAuth para o qual você usa. AppFabric
4. Insira a ID do cliente na página Credenciais do aplicativo no campo ID do cliente em AppFabric.

Segredo do cliente

AppFabric solicitará o segredo do seu cliente. Para descobrir o segredo do cliente Zoom, siga estas etapas:

1. Navegue até o marketplace do Zoom.
2. Escolha Gerenciar.
3. Escolha o aplicativo server-to-server OAuth para o qual você usa. AppFabric
4. Insira o segredo do cliente na página Credenciais do aplicativo no campo Segredo do cliente em AppFabric.

Entrega do log de auditoria

O Zoom disponibiliza logs de auditoria acessando a API a cada 24 horas. Ao visualizar registros de auditoria com AppFabric, os dados que você vê Zoom são das atividades do dia anterior.

Ferramentas e serviços de segurança compatíveis

AWS AppFabric for security suporta a integração com as seguintes ferramentas e serviços de segurança. Escolha o nome de um serviço para obter mais informações sobre como configurar a segurança AppFabric para se conectar a ele.

Tópicos

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

Barracuda XDR

A Barracuda Networks é uma parceira confiável e fornecedora líder de soluções de segurança que priorizam a nuvem, protegendo emails, redes, dados e aplicações com soluções inovadoras que

crescem e se adaptam à jornada dos negócios. O Barracuda XDR é uma solução aberta e estendida de detecção e resposta que combina tecnologias sofisticadas com uma equipe de analistas de segurança em nosso centro de operações de segurança (SOC). A plataforma Barracuda XDR analisa bilhões de eventos brutos diariamente de mais de 40 fontes de dados integradas e, junto com as extensas regras de detecção de ameaças mapeadas na estrutura MITRE ATT&CK®, ela pode detectar ameaças mais rapidamente e reduzir o tempo de resposta.

AWS AppFabric considerações sobre a ingestão de registros de auditoria

As seções a seguir descrevem o esquema AppFabric de saída, os formatos de saída e os destinos de saída com Barracuda XDR os quais usar.

Esquema e formato

Barracuda XDRsuporta o seguinte esquema e formatos de AppFabric saída:

- OCSF - JSON: AppFabric normaliza os dados usando o Open Cybersecurity Schema Framework (OCSF) e gera os dados no formato JSON.

Locais de saída

O Barracuda XDR oferece suporte ao recebimento de logs de auditoria do Amazon Security Lake. Para enviar dados de AppFabric paraBarracuda XDR, siga as instruções abaixo:

1. Enviar dados para o Amazon Security Lake: configure AppFabric para enviar dados para o Amazon Security Lake por meio de um Amazon Data Firehose. Para ter mais informações, consulte Amazon Security Lake.
2. Enviar dados para o Barracuda XDR: configure o Barracuda XDR para receber logs de auditoria do Amazon Security Lake. Para obter mais informações, consulte Configuração e uso do Amazon Security Lake.

Dynatrace

O Dynatrace® Platform combina observabilidade ampla e profunda e segurança contínua de aplicativos em tempo de execução com AIOps avançados para fornecer respostas e automação inteligente a partir de dados. Isso permite que os inovadores modernizem e automatizem as operações em nuvem, forneçam software com mais rapidez e segurança e garantam experiências digitais perfeitas.

AWS AppFabric considerações sobre a ingestão de registros de auditoria

As seções a seguir descrevem o esquema AppFabric de saída, os formatos de saída e os destinos de saída a serem usados com o. Dynatrace Platform

Esquema e formato

O Dynatrace Platform suporta o seguinte esquema e formatos de AppFabric saída:

- OCSF - JSON: AppFabric normaliza os dados usando o Open Cybersecurity Schema Framework (OCSF) e gera os dados no formato JSON.

Locais de saída

O Dynatrace Platform suporta o recebimento de registros de auditoria dos seguintes locais AppFabric de saída.

- Amazon Simple Storage Service (Amazon S3)
  - Para configurar o Dynatrace Platform para receber dados do bucket Amazon S3 que contém seus registros de auditoria, siga as instruções no projeto S3 Log Forwarder da Dynatrace em. GitHub

Logz.io

Logz.io ajuda empresas nativas de nuvem a monitorar e proteger seus ambientes por meio da plataforma Logz.ioOpen 360, transformando a observabilidade e a segurança de uma carga de alto custo e baixo valor em uma ferramenta econômica e de alto valor que possibilita melhores resultados comerciais.

Logz.ioO Cloud SIEM aborda diretamente os principais desafios de segurança atuais, da sobrecarga de dados à lacuna onipresente de habilidades cibernéticas, por meio de consultas rápidas, detecção multidimensional e conteúdo de segurança profundamente personalizável para ajudar a monitorar e investigar em toda a extensão do seu ambiente de nuvem, sem degradação do desempenho, independentemente dos volumes de dados.

A solução Logz.io foi criada especificamente para fornecer análise e investigação avançadas de ameaças com menos complexidade e custo. Os clientes contam com o apoio de analistas de segurança dedicados, conteúdo de ameaças como serviço e recursos baseados em IA

desenvolvidos especificamente para ajudar a reduzir dados ruidosos e se concentrar nas informações que permitem que sua equipe priorize rapidamente as ameaças do mundo real.

AWS AppFabric considerações sobre a ingestão de registros de auditoria

As seções a seguir descrevem o esquema AppFabric de saída, os formatos de saída e os destinos de saída com Logz.io os quais usar.

Esquema e formato

Logz.iosuporta o seguinte esquema e formatos de AppFabric saída:

- Raw - JSON
  - AppFabric gera dados no esquema original usado pelo aplicativo de origem no formato JSON.
- OCSF - JSON
  - AppFabric normaliza os dados usando o Open Cybersecurity Schema Framework (OCSF) e gera os dados no formato JSON.

Locais de saída

Logz.iosuporta os seguintes locais AppFabric de saída:

- Amazon Data Firehose
  - Para configurar seu stream de entrega do Firehose para que ele envie dados paraLogz.io, siga as instruções em Choose Logz.io for Your Destination no Amazon Data Firehose Developer Guide.
- Amazon Simple Storage Service (Amazon S3)
  - Para configurar o Logz.io para receber dados do bucket do Amazon S3 que contém seus logs de auditoria, siga as instruções em Configurar um bucket do Amazon S3 no site Logz.io.

Netskope

A Netskope, líder global em segurança cibernética, está redefinindo a segurança na nuvem, nos dados e na rede para ajudar as organizações a aplicar princípios de confiança zero para proteger os dados. Rápida e fácil de usar, a plataforma Netskope fornece acesso otimizado e segurança de confiança zero para pessoas, dispositivos e dados em qualquer lugar. A Netskope ajuda os clientes a reduzir riscos, acelerar o desempenho e obter visibilidade incomparável de qualquer atividade na nuvem, na web e em aplicativos privados. Milhares de clientes, incluindo mais de 25 empresas

da Fortune 100, confiam em Netskope nossa poderosa NewEdge rede para lidar com ameaças em evolução, novos riscos, mudanças tecnológicas, mudanças organizacionais e de rede e novos requisitos regulatórios. Saiba como Netskope ajuda os clientes a se prepararem para qualquer coisa em sua jornada de SASE, visite netskope.com.

AWS AppFabric considerações sobre a ingestão de registros de auditoria

As seções a seguir descrevem o esquema AppFabric de saída, os formatos de saída e os destinos de saída com Netskope os quais usar.

Esquema e formato

Netskopesuporta o seguinte esquema e formatos de AppFabric saída:

- Raw - JSON
  - AppFabric gera dados no esquema original usado pelo aplicativo de origem no formato JSON.
- OCSF - JSON
  - AppFabric normaliza os dados usando o Open Cybersecurity Schema Framework (OCSF) e gera os dados no formato JSON.

Locais de saída

Netskopesuporta o seguinte local AppFabric de saída:

- Amazon Simple Storage Service (Amazon S3)
  - Para configurar o Netskope para receber dados do bucket do Amazon S3 que contém seus logs de auditoria, siga as instruções em Proteção de dados para Amazon Web Services S3 no site Netskope.

NetWitness

A NetWitness é uma desenvolvedora líder de software de detecção e resposta estendidas (XDR). Sua base global de clientes altamente preocupados com a segurança confia no NetWitness XDR para se defender contra adversários sofisticados e agressivos. Com a plataforma mais completa, integrada e madura do setor para detectar, investigar e responder a ataques digitais, o NetWitness XDR é a base unificadora de um SOC moderno e eficaz.

Devido à sua arquitetura altamente modular, o NetWitness XDR detecta ameaças onde quer que elas ocorram — na nuvem, on-premises, com funcionários móveis e remotos, ou em qualquer lugar

intermediário. O NetWitness Platform XDR oferece visibilidade completa combinada com inteligência de ameaças aplicada e análise do comportamento do usuário para detectar ameaças, priorizar atividades, investigar e automatizar a resposta. Tudo isso capacita os analistas de segurança com uma eficiência melhor e mais rápida para manter as operações de segurança bem à frente das ameaças que afetam os negócios.

AWS AppFabric considerações sobre a ingestão de registros de auditoria

As seções a seguir descrevem o esquema AppFabric de saída, os formatos de saída e os destinos de saída com NetWitness os quais usar.

Esquema e formato

NetWitness suporta o seguinte esquema e formatos de AppFabric saída:

- Raw - JSON
  - AppFabric gera dados no esquema original usado pelo aplicativo de origem no formato JSON.
- OCSF - JSON
  - AppFabric normaliza os dados usando o Open Cybersecurity Schema Framework (OCSF) e gera os dados no formato JSON.

Locais de saída

NetWitnesssuporta o seguinte local AppFabric de saída:

- Amazon Simple Storage Service (Amazon S3)
  - Para configurar o NetWitness para receber dados do bucket do Amazon S3 que contém seus logs de auditoria, siga as instruções no Guia de configuração do log de fonte de eventos do S3 Universal Connector na página de Integrações de plataformas do NetWitness no site NetWitness.

Amazon QuickSight

A Amazon QuickSight capacita organizações orientadas por dados com inteligência de negócios (BI) unificada em hiperescala. Com QuickSight, todos os usuários podem atender a diferentes necessidades analíticas a partir da mesma fonte confiável por meio de painéis interativos modernos, relatórios paginados, análises incorporadas e consultas em linguagem natural. Você pode analisar os dados do log de AWS AppFabric QuickSight auditoria escolhendo seu bucket do Amazon Simple

Storage Service (Amazon S3) onde AppFabric seus registros de segurança são armazenados como sua fonte.

AppFabric considerações sobre a ingestão de registros de auditoria

As seções a seguir descrevem o esquema AppFabric de saída, os formatos de saída e os destinos de saída a serem usados com a Amazon QuickSight.

Esquema e formatos

QuickSight suporta o seguinte esquema e formatos de AppFabric saída:

- Raw - JSON
  - AppFabric gera dados no esquema original usado pelo aplicativo de origem no formato JSON.
- OCSF - JSON
  - AppFabric normaliza os dados usando o Open Cybersecurity Schema Framework (OCSF) e gera os dados no formato JSON.

Locais de saída

QuickSight suporta os seguintes locais AppFabric de saída:

- Amazon S3
  - Você pode ingerir dados do Amazon S3 QuickSight diretamente criando um conjunto de dados usando arquivos do Amazon S3. Para verificar se seu conjunto de arquivos de destino não excede as cotas da fonte de QuickSight dados, consulte Cotas da fonte de dados no Guia QuickSight do usuário da Amazon.
  - Se seu conjunto de arquivos exceder as QuickSight cotas de uma fonte de dados do Amazon S3, você poderá ingerir seus dados no Amazon S3 usando o Amazon Athena e tabelas. AWS Glue Usar o Athena em seu QuickSight conjunto de dados acarretará custos adicionais. Para obter informações sobre preços do Athena, consulte a página de preços do Athena.

    Para usar o Athena:

    1. Siga as instruções em Como usar AWS Glue para se conectar às fontes de dados no Amazon S3 no Guia do usuário do Athena.
    2. Siga as instruções em Criação de um conjunto de dados usando dados do Athena no Guia do usuário da QuickSight Amazon.

Rapid7

Rapid7, Inc. tem a missão de criar um mundo digital mais seguro, tornando a segurança cibernética mais simples e acessível. Rapid7capacita os profissionais de segurança a gerenciar uma superfície de ataque moderna por meio de best-in-class tecnologia, pesquisas de ponta e ampla experiência estratégica. Rapid7As soluções de segurança abrangentes da ajudam mais de 10.000 clientes globais a unir o gerenciamento de riscos na nuvem e a detecção de ameaças para reduzir as superfícies de ataque e eliminar ameaças com velocidade e precisão.

AWS AppFabric considerações sobre a ingestão de registros de auditoria

As seções a seguir descrevem o esquema AppFabric de saída, o formato de saída e os destinos de saída a serem usados comRapid7.

Esquema e formato

Rapid7suporta o seguinte esquema e formatos de AppFabric saída:

- Raw - JSON
  - AppFabric gera dados no esquema original usado pelo aplicativo de origem no formato JSON.
- OCSF - JSON
  - AppFabric normaliza os dados usando o Open Cybersecurity Schema Framework (OCSF) e gera os dados no formato JSON.

Locais de saída

Rapid7suporta o seguinte local AppFabric de saída:

- Amazon Simple Storage Service (Amazon S3)
  - Para configurar o Rapid7 para receber dados do bucket do Amazon S3 que contém seus logs de auditoria, siga as instruções na postagem do blog Como monitorar sua atividade no Amazon S3 com o InsightIDR no site do blog Rapid7.

Amazon Security Lake

O Amazon Security Lake centraliza automaticamente dados de segurança de AWS ambientes, provedores de software como serviço (SaaS), locais e fontes na nuvem em um data lake criado especificamente e armazenado em seu. Conta da AWS Com o Security Lake, você pode obter uma compreensão mais completa dos seus dados de segurança em toda a organização. O Security Lake

adotou o Open Cybersecurity Schema Framework (OCSF), um esquema de eventos de segurança de código aberto. Com o suporte do OCSF, o serviço normaliza e combina dados de segurança de AWS uma ampla variedade de fontes de dados de segurança corporativa.

AppFabric considerações sobre a ingestão de registros de auditoria

Você pode obter seus registros de auditoria de SaaS no Amazon Security Lake Conta da AWS adicionando uma fonte personalizada ao Security Lake. As seções a seguir descrevem o esquema AppFabric de saída, o formato de saída e os destinos de saída a serem usados com o Security Lake.

Esquema e formato

O Security Lake suporta o seguinte esquema e formato de AppFabric saída:

- OCSF - JSON
  - AppFabric normaliza os dados usando o Open Cybersecurity Schema Framework (OCSF) e gera os dados no formato JSON.

Locais de saída

O Security Lake oferece suporte AppFabric como uma fonte personalizada usando um stream de entrega do Amazon Data Firehose como local de saída da AppFabric ingestão. Para configurar a AWS Glue tabela e o stream de entrega do Firehose e configurar uma fonte personalizada no Security Lake, use os procedimentos a seguir.

Crie uma AWS Glue tabela

1. Navegue até o Amazon Simple Storage Service (Amazon S3) e crie um bucket com um nome de sua escolha.
2. Navegue até o AWS Glue console.
3. Para Catálogo de dados, vá para a seção Tabelas e escolha Adicionar tabela.
4. Insira um nome de sua escolha para essa tabela.
5. Selecione o bucket do Amazon S3 que você criou na etapa 1.
6. Para o formato de dados, selecione JSON e escolha Avançar.
7. Na página Escolher ou definir esquema, escolha Editar esquema como JSON.
8. Insira o esquema a seguir e conclua o processo de criação da AWS Glue tabela.

```
[
```

```
    {
        "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>"
    }
]
```

Criar uma fonte personalizada no Security Lake

1. Navegue até o console do Amazon Security Lake.
2. Selecione Fontes personalizadas no painel de navegação.
3. Escolha Criar fonte personalizada.
4. Insira um nome para a fonte personalizada e selecione uma classe de evento do OCSF aplicável.

> **Note**
>
> AppFabric usa classes de eventos de Alteração de Conta, Autenticação, Gerenciamento de Acesso de Usuários, Gerenciamento de Grupos, Atividade de Recursos da Web e Atividade de Acesso a Recursos da Web.

5. Para Conta da AWS ID e ID externa, insira sua Conta da AWS ID. Selecione Criar.
6. Salve a localização do Amazon S3 da fonte personalizada. Você o usará para configurar um stream de entrega do Amazon Data Firehose.

Crie um stream de entrega no Firehose

1. Navegue até o console do Amazon Data Firehose.
2. Escolha Criar stream de entrega.
3. Para Fonte, selecione PUT direto.
4. Para Destino, escolha S3.

5. Na seção Transformar e converter registros, escolha Habilitar conversão de formato de registro e escolha Apache Parquet como formato de saída.
6. Para AWS Glue tabela, escolha a AWS Glue tabela que você criou no procedimento anterior e escolha a versão mais recente.
7. Para Configurações de destino, escolha o bucket do Amazon S3 que você criou com a fonte personalizada do Security Lake.
8. Para Particionamento dinâmico, escolha Ativado.
9. Para Análise embutida para JSON, escolha Ativado.
   - Para Nome, insira `eventDayValue`.
   - Para Expressão JQ, insira `(.time/1000)|strftime("%Y%m%d")`.
10. Para o Prefixo do bucket do S3, insira o valor seguinte.

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

    <region><account_id>Substitua e por seu Conta da AWS ID Região da AWS e.
11. Para o Prefixo de saída de erro do bucket do S3, insira o valor seguinte.

    ```
    ext/AppFabric/error/
    ```
12. Para a Duração da nova tentativa, selecione 300.
13. Para o Tamanho do buffer, selecione 128 MiB.
14. Para o Intervalo de buffer, selecione 60s.
15. Conclua o processo de criação do stream de entrega do Firehose.

Crie AppFabric ingestões

Para enviar dados para o Amazon Security Lake, você deve criar uma ingestão no AppFabric console que use o stream de entrega do Firehose que você criou anteriormente como local de saída. Para obter mais informações sobre como configurar AppFabric ingestões para usar o Firehose como um local de saída, consulte Criar um local de saída.

Singularity Cloud

A Singularity Cloud plataforma protege sua empresa contra ameaças de todas as categorias, em todos os estágios. Sua IA (Inteligência Artificial) patenteada estende a segurança desde assinaturas e padrões conhecidos até os ataques mais sofisticados, como dia zero e ransomware.

AWS AppFabric considerações sobre a ingestão de registros de auditoria

As seções a seguir descrevem o esquema AppFabric de saída, os formatos de saída e os destinos de saída com Singularity Cloud os quais usar.

Esquema e formato

Singularity Cloudsuporta o seguinte esquema e formatos de AppFabric saída:

OCSF - JSON: AppFabric normaliza os dados usando o Open Cybersecurity Schema Framework (OCSF) e gera os dados no formato JSON.

Locais de saída

Singularity Cloudsuporta o recebimento de registros de auditoria dos seguintes locais AppFabric de saída.

- Amazon Simple Storage Service (Amazon S3)
  - Para configurar Singularity Cloud para receber dados do bucket do Amazon S3 que contém seus registros de auditoria, siga as instruções na Singularity Cloud’s documentação.

Splunk

A Splunk ajuda a tornar as organizações mais resilientes. As principais organizações usam a plataforma unificada de segurança e observabilidade de Splunk para manter seus sistemas digitais seguros e confiáveis. As organizações confiam em Splunk para evitar que problemas de segurança, infraestrutura e aplicativos se tornem incidentes graves, absorvam os choques das interrupções digitais e acelerem a transformação digital.

AWS AppFabric considerações sobre a ingestão de registros de auditoria

As seções a seguir descrevem o esquema AppFabric de saída, os formatos de saída e os destinos de saída com Splunk os quais usar.

Esquema e formato

O Splunk suporta os seguintes esquemas e formatos de AppFabric saída:

- Raw - JSON
  - AppFabric gera dados no esquema original usado pelo aplicativo de origem no formato JSON.
- OCSF - JSON
  - AppFabric normaliza os dados usando o Open Cybersecurity Schema Framework (OCSF) e gera os dados no formato JSON.
- OCSF - Parquet
  - AppFabric normaliza os dados usando o Open Cybersecurity Schema Framework (OCSF) e gera os dados no formato. Apache Parquet

Locais de saída

Splunksuporta os seguintes locais AppFabric de saída:

- Amazon Data Firehose
  - Para configurar Splunk para receber registros de auditoria do stream do Firehose que contém seus registros de auditoria, siga as instruções em SplunkAdd-on for Amazon Data Firehose no site. Splunk
- Amazon Simple Storage Service (Amazon S3)
  - Para configurar o Splunk para receber dados do bucket do Amazon S3 que contém seus logs de auditoria, siga as instruções em Configurar entradas de S3 baseadas em SQS para o add-on Splunk para o AWS no site Splunk.

Excluir AWS AppFabric para recursos de segurança

Se você não quiser continuar usando AWS AppFabric por motivos de segurança, certifique-se de excluir os dados nos locais de saída que você criou durante a configuração e seus recursos de segurança AppFabric para evitar cobranças adicionais. Para limpar seus AppFabric recursos, você deve excluir os recursos na ordem inversa em que os criou para cada aplicativo de software como serviço (SaaS): Destinos de ingestão > Ingestões > Autorização de aplicativos > Pacotes de aplicativos

Depois de excluir sua autorização final do aplicativo, você pode excluir o pacote de aplicativos.

Tópicos

- Excluir um destino de ingestão
- Excluir uma ingestão
- Exclua uma autorização de aplicativo.
- Excluir um pacote de aplicativos

Excluir um destino de ingestão

Se você selecionar um local de saída ao criar uma ingestão, AppFabric por segurança, criará destinos de ingestão em seu nome. Use as seguintes etapas para excluir um destino de ingestão:

1. Abra o AppFabric console em https://console.aws.amazon.com/appfabric/.
2. Na página de Introdução, expanda o menu à esquerda.
3. Escolha Ingestões.
4. Escolha uma autorização de aplicativo.
5. Selecione o botão de opções ao lado do destino que você deseja excluir e escolha Excluir.
6. Escolha Excluir na caixa de diário de destino de exclusão para confirmar.
7. Repita as etapas acima para todos os seus destinos.

Excluir uma ingestão

Use as seguintes etapas para excluir uma ingestão:

1. Na página de Introdução, expanda o menu à esquerda.
2. Escolha Ingestões.
3. Selecione o botão de opção que está ao lado da autorização do seu aplicativo.
4. Escolha o menu suspenso Ações.
5. Escolha Excluir.
6. Escolha Excluir na caixa de diário de destino de exclusão para confirmar.

Exclua uma autorização de aplicativo.

Use as seguintes etapas para excluir uma autorização de aplicativos:

1. Na página de Introdução, expanda o menu à esquerda.
2. Escolha Autorizações de aplicativo.
3. Selecione o botão de opção que está ao lado da autorização do seu aplicativo que deseja excluir.
4. Escolha o menu suspenso Ações.
5. Escolha Excluir.
6. Escolha Excluir na caixa de diário de destino de exclusão para confirmar.

Excluir um pacote de aplicativos

Use as etapas a seguir para excluir seu pacote de aplicativos.

1. Na página de Introdução, expanda o menu à esquerda.
2. Escolha o pacote de aplicativos.
3. Escolha o botão Delete (Excluir) .
4. Digite `delete` para confirmar, e então escolha Excluir.

O que AWS AppFabric significa produtividade?

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

> **Note**
>
> Desenvolvido pelo Amazon Bedrock: AWS implementa a detecção automática de abusos. Como AWS AppFabric a produtividade é construída no Amazon Bedrock, os usuários herdam os controles implementados no Amazon Bedrock para garantir a segurança e o uso responsável da IA.

AWS AppFabric for productivity (versão prévia) ajuda a reimaginar a produtividade do usuário final em aplicativos de terceiros, gerando insights e ações com contexto de vários aplicativos. Os desenvolvedores de aplicações reconhecem que acessar os dados do usuário de outras aplicações é importante para criar uma experiência de aplicação mais produtiva, mas eles não querem criar e gerenciar integrações com cada aplicação. Com o objetivo AppFabric de produtividade, os

desenvolvedores de aplicativos obtêm acesso a APIs generativas baseadas em IA que geram informações e ações de dados entre aplicativos para que possam fornecer experiências mais ricas ao usuário final por meio de assistentes de IA generativos novos ou existentes. AppFabric para produtividade, integra dados de vários aplicativos, eliminando a necessidade de os desenvolvedores criarem ou manterem point-to-point integrações. Os desenvolvedores de aplicativos podem incorporar AppFabric a produtividade diretamente na interface do usuário do aplicativo, mantendo uma experiência consistente para os usuários finais e, ao mesmo tempo, revelando o contexto relevante de outros aplicativos.

AppFabric para produtividade, conecta dados de aplicativos comumente usadosAsana, como,Atlassian Jira Suite,Google Workspace,Microsoft 365,Miro, SlackSmartsheet, e muito mais. AppFabric para produtividade, os desenvolvedores de aplicativos oferecem aos desenvolvedores de aplicativos uma maneira mais fácil de criar experiências de aplicativos mais personalizadas que melhoram a adoção, a satisfação e a fidelidade dos usuários. Enquanto isso, os usuários finais se beneficiam do acesso às informações de que precisam em suas aplicações, sem interromper o fluxo de trabalho.

Tópicos

- Benefícios
- Casos de uso
- Acesso AppFabric para produtividade
- Introdução à AppFabric produtividade (versão prévia) para desenvolvedores de aplicativos
- Introdução à AppFabric produtividade (versão prévia) para usuários finais
- AppFabric APIs de produtividade
- Processamento de dados

Benefícios

Com AppFabric o objetivo de produtividade, os desenvolvedores de aplicativos obtêm acesso a APIs que geram informações e ações de dados entre aplicativos para que possam fornecer experiências mais ricas ao usuário final por meio de assistentes de IA generativos novos ou existentes.

- Fonte única de dados de usuários entre aplicativos: AppFabric para produtividade, integra dados de vários aplicativos, eliminando a necessidade de os desenvolvedores criarem ou manterem point-to-point integrações. Os dados SaaS da aplicação são processados para uso em outras aplicações, normalizando automaticamente tipos de dados diferentes em um formato

compreensível por qualquer aplicação, permitindo que os desenvolvedores de aplicações incorporem mais dados que, na verdade, melhorem a produtividade dos usuários finais.

- Controle total da experiência do usuário: os desenvolvedores AppFabric incorporam a produtividade diretamente na interface do usuário do aplicativo, mantendo o controle total da experiência do usuário e fornecendo insights personalizados e ações recomendadas aos usuários finais com o contexto de todos os aplicativos. Isso torna AppFabric a produtividade disponível no aplicativo SaaS preferido dos usuários finais e pode ser acessado no aplicativo que eles preferem para concluir suas tarefas. Os usuários finais passam menos tempo alternando entre aplicações, e podem permanecer no fluxo de seu trabalho.
- Acelere o tempo de lançamento no mercado: em uma única chamada de API, os desenvolvedores de aplicativos podem receber insights em nível de usuário sobre os dados de um usuário que são gerados sem precisar ajustar um modelo, escrever um prompt personalizado ou criar integrações em vários aplicativos. AppFabric abstrai essa complexidade para permitir que os desenvolvedores de aplicativos criem, incorporem ou enriqueçam os recursos de IA generativa com mais rapidez. Isso permite que os desenvolvedores de aplicações se concentrem em seus recursos nas tarefas mais importantes.
- Referências de artefatos para aumentar a confiança do usuário: como parte do resultado, AppFabric para fins de produtividade, apresentarão artefatos relevantes ou arquivos de origem usados para gerar insights para criar a confiança do usuário final nas saídas do LLM.
- Permissões de usuário simplificadas: os artefatos do usuário usados para gerar insights são baseados no que o usuário tem acesso. AppFabric para produtividade, usa a permissão e o controle de acesso de um ISV como a fonte da verdade.

Casos de uso

Os desenvolvedores de aplicativos podem usar a produtividade AppFabric para reimaginar a produtividade em seus aplicativos. AppFabric for productivity oferece duas APIs focadas nos seguintes casos de uso para ajudar seus usuários finais a serem mais produtivos:

- Priorize seu dia
  - A API de informações acionáveis ajuda os usuários a gerenciar melhor seu dia, exibindo informações oportunas de todas as aplicações, incluindo emails, calendário, mensagens, tarefas e muito mais. Além disso, os usuários podem executar ações entre aplicações, como criar emails, agendar reuniões e criar itens de ação a partir da aplicação preferida. Por exemplo, um funcionário que tenha tido um escalonamento de clientes durante a noite não só verá um resumo das conversas noturnas, mas também poderá ver uma ação recomendada para agendar

uma reunião com o gerente de contas do cliente. As ações são previamente preenchidas com campos obrigatórios (como nome e proprietário da tarefa ou remetente/destinatário do email), com a capacidade de editar o conteúdo previamente preenchido antes de executar a ação.

- Prepare-se para as próximas reuniões
  - A API de preparação de reuniões ajuda os usuários a se prepararem melhor para as reuniões, resumindo o objetivo da reunião e revelando artefatos relevantes entre aplicações, como emails, mensagens e muito mais. Os usuários podem se preparar rapidamente para as reuniões agora e não perder tempo alternando entre aplicações para localizar conteúdo.

Acesso AppFabric para produtividade

AppFabric para produtividade está atualmente lançado como uma prévia e está disponível no Leste dos EUA (Norte da Virgínia) Região da AWS. Para obter mais informações sobre Regiões da AWS, consulte AWS AppFabric endpoints e cotas no. Referência geral da AWS

Em cada região, você pode acessar AppFabric a produtividade de qualquer uma das seguintes formas:

- Como um desenvolvedor de aplicações
  - Introdução à AppFabric produtividade (versão prévia) para desenvolvedores de aplicativos
- Como um usuário final
  - Introdução à AppFabric produtividade (versão prévia) para usuários finais

Introdução à AppFabric produtividade (versão prévia) para desenvolvedores de aplicativos

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Esta seção ajuda os desenvolvedores de aplicativos a integrarem seus aplicativos AWS AppFabric para fins de produtividade (pré-visualização). AWS AppFabric para produtividade, permite que os desenvolvedores criem experiências de aplicativos mais ricas para seus usuários, gerando informações e ações baseadas em IA a partir de e-mails, eventos do calendário, tarefas, mensagens e muito mais em vários aplicativos. Para obter uma lista dos aplicativos compatíveis, consulte Aplicativos AWS AppFabric compatíveis.

AppFabric para produtividade oferece aos desenvolvedores de aplicativos acesso para criar e experimentar em um ambiente seguro e controlado. Ao começar a usar AppFabric para fins de produtividade, você cria um AppClient e registra um único usuário de teste. Essa abordagem foi projetada para ajudá-lo a entender e testar o fluxo de autenticação e comunicação entre seu aplicativo AppFabric e. Depois de testar com um único usuário, você pode enviar sua inscrição AppFabric para verificação antes de expandir o acesso a outros usuários (consulteEtapa 5. Solicitação AppFabric para verificar sua inscrição). AppFabric verificará as informações do aplicativo antes de permitir uma ampla adoção para ajudar a proteger os desenvolvedores de aplicativos, os usuários finais e seus dados, abrindo caminho para expandir a adoção pelos usuários de forma responsável.

Tópicos

- Pré-requisitos
- Etapa 1. Crie um AppFabric para produtividade AppClient
- Etapa 2. Autentique e autorize sua aplicação
- Etapa 3. Adicione a URL AppFabric do portal do usuário ao seu aplicativo
- Etapa 4. Use AppFabric para revelar informações e ações entre aplicativos
- Etapa 5. Solicitação AppFabric para verificar sua inscrição
- Gerenciando AppFabric a produtividade AppClients
- Solução de problemas

Pré-requisitos

Antes de começar, você precisa criar um Conta da AWS. Para ter mais informações, consulte Inscreva-se para um Conta da AWS. Você também precisa criar pelo menos um usuário com acesso à política do `"appfabric:CreateAppClient"` IAM listada abaixo, que permite que o usuário registre seu aplicativo com AppFabric. Para obter mais informações sobre a concessão de permissões AppFabric para os recursos de produtividade, consulteAppFabric exemplos de políticas de IAM para produtividade. Embora ter um usuário administrativo seja benéfico, isso não é obrigatório para a configuração inicial. Para ter mais informações, consulte Criar um usuário com acesso administrativo.

AppFabric para produtividade é somente no Leste dos EUA (Norte da Virgínia) durante a pré-visualização. Certifique-se de estar nessa região antes de iniciar as etapas abaixo.

```
{
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Etapa 1. Crie um AppFabric para produtividade AppClient

Antes de começar a AppFabric buscar insights de produtividade em seu aplicativo, você precisa criar um AppFabric AppClient. An AppClient é essencialmente sua porta de entrada AppFabric para produtividade, funcionando como um cliente de aplicativo OAuth seguro, permitindo a comunicação segura entre seu aplicativo e. AppFabric Ao criar um AppClient, você receberá um AppClient ID, um identificador exclusivo crucial para garantir que ele AppFabric saiba que está funcionando com seu aplicativo e com o seu Conta da AWS.

AppFabric para produtividade oferece aos desenvolvedores de aplicativos acesso para criar e experimentar em um ambiente seguro e controlado. Ao começar a usar AppFabric para fins de produtividade, você cria um AppClient e registra um único usuário de teste. Essa abordagem foi projetada para ajudá-lo a entender e testar o fluxo de autenticação e comunicação entre seu aplicativo AppFabric e. Depois de testar com um único usuário, você pode enviar sua inscrição AppFabric para verificação antes de expandir o acesso a outros usuários (consulteEtapa 5. Solicitação AppFabric para verificar sua inscrição). AppFabric verificará as informações do aplicativo antes de permitir uma ampla adoção para ajudar a proteger os desenvolvedores de aplicativos, os usuários finais e seus dados, abrindo caminho para expandir a adoção pelos usuários de forma responsável.

Para criar um AppClient, use a operação de AWS AppFabric `CreateAppClient` API. Se precisar atualizar o AppClient after, você pode usar a operação da `UpdateAppClient` API para alterar somente os redirectURLs. Se você precisar alterar qualquer um dos outros parâmetros associados ao seu, AppClient como AppName ou description, exclua o AppClient e crie um novo. Para ter mais informações, consulte CreateAppClient.

Você pode registrar seu aplicativo com AWS serviços usando a `CreateAppClient` API usando várias linguagens de programação, incluindo Python, Node.js, Java, C#, Go e Rust. Para obter mais

informações, consulte Solicitação de exemplos de assinaturas no Guia do usuário do IAM. Você precisa usar suas credenciais de assinatura de conta versão 4 para realizar essa operação de API. Para obter mais informações sobre a assinatura versão 4, consulte Solicitações de AWS API de assinatura no Guia do usuário do IAM.

Campos de solicitação

- `appName`- O nome do aplicativo que será exibido aos usuários na página de consentimento do portal do AppFabric usuário. A página de consentimento solicita permissão aos usuários finais para exibir AppFabric insights dentro do seu aplicativo. Para obter detalhes sobre a página de consentimento, consulte Etapa 2. Forneça consentimento para que a aplicação exiba informações.
- `description`: uma descrição da aplicação.
- `redirectUrls`: o URI para o qual redirecionar os usuários finais após a autorização. É possível adicionar até 5 redirectUrls. Por exemplo, `https://localhost:8080`.
- `starterUserEmails`: um endereço de email do usuário que terá acesso para receber as informações até que a aplicação seja verificada. Só é permitido um endereço de email. Por exemplo, `anyuser@example.com`.
- `customerManagedKeyIdentifier` (opcional): o ARN da chave gerenciada pelo cliente (gerada pelo KMS) a ser usada para criptografar os dados. Se não for especificada, a chave AWS AppFabric gerenciada será usada. Para ter mais informações sobre Chaves pertencentes à AWS e chaves gerenciadas pelo cliente, consulte Chaves de clientes e chaves AWS no Guia do desenvolvedor AWS Key Management Service .

Campos de resposta

- `appClientArn`- O nome de recurso da Amazon (ARN) que inclui o AppClient ID. Por exemplo, o AppClient ID é `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `verificationStatus`- O status da AppClient verificação.
  - `pending_verification`- A verificação do ainda AppClient está em andamento com AppFabric. Até que AppClient seja verificado, somente um usuário (especificado em`starterUserEmails`) pode usar AppClient o. O usuário verá uma notificação no portal do AppFabric usuário, introduzida emEtapa 3. Adicione a URL AppFabric do portal do usuário ao seu aplicativo, indicando que o aplicativo não foi verificado.
  - `verified`- O processo de verificação foi concluído com sucesso AppFabric e agora AppClient está totalmente verificado.

- `rejected`- O processo de verificação do AppClient foi rejeitado por AppFabric. Eles AppClient não podem ser usados por usuários adicionais até que o processo de verificação seja reiniciado e concluído com êxito.

```
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>"
}'
```

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

```
{
    "appClientConfigSummary": {
        "appClientArn": "arn:aws:appfabric:<region>:<account>:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "verificationStatus": "pending_verification"
    }
}
```

Etapa 2. Autentique e autorize sua aplicação

Permita que seu aplicativo integre AppFabric insights com segurança estabelecendo um fluxo de autorização do OAuth 2.0. Primeiro, você precisa criar um código de autorização que verifique a identidade da sua aplicação. Para ter mais informações, consulte Autorizar. Em seguida, você trocará esse código de autorização por um token de acesso, que concede ao seu aplicativo as permissões para buscar e exibir AppFabric insights dentro do seu aplicativo. Para ter mais informações, consulte Token.

Para obter mais informações sobre como conceder permissão para autorizar uma aplicação, consulte Permitir acesso para autorizar aplicações.

1. Para criar um código de autorização, use a operação AWS AppFabric `oauth2/authorize` da API.

   Campos de solicitação

   - `app_client_id`(obrigatório) - O AppClient ID do Conta da AWS criado na Etapa 1. Crie um AppClient. Por exemplo, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
   - `redirect_uri` (obrigatório): o URI para o qual redirecionar os usuários finais após a autorização que você usou na Etapa 1. Crie um AppClient. Por exemplo, `https://localhost:8080`.
   - `state` (obrigatório): um valor exclusivo para manter o estado entre a solicitação e o retorno de chamada. Por exemplo, `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. Após a autenticação, você irá para o URI especificado com um código de autorização retornado como parâmetro de consulta. Por exemplo, onde `code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`.

   ```
   https://localhost:8080/?code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-
   sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-
   oampc&state=a8904edc-890c-1005-1996-29a757272a44
   ```

3. Troque esse código de autorização por um token de acesso usando a operação AppFabric `oauth2/token` da API.

   Esse token é usado para solicitações de API e é inicialmente válido `starterUserEmails` até que AppClient seja verificado. Depois de AppClient verificado, esse token pode ser usado por qualquer usuário. Você precisa usar suas credenciais de assinatura de conta versão 4 para realizar essa operação de API. Para obter mais informações sobre a assinatura versão 4, consulte Solicitações de AWS API de assinatura no Guia do usuário do IAM.

Campos de solicitação

- `code` (obrigatório): o código de autorização que você recebeu após a autenticação na última etapa. Por exemplo, `mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`.
- `app_client_id`(obrigatório) - O AppClient ID do Conta da AWS criado na Etapa 1. Crie um AppClient. Por exemplo, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `grant_type` (obrigatório): o valor deve ser `authorization_code`.
- `redirect_uri` (obrigatório): o URI para o qual redirecionar os usuários após a autorização que você usou na Etapa 1. Crie um AppClient. Esse deve ser o mesmo URI de redirecionamento usado para criar um código de autorização. Por exemplo, `https://localhost:8080`.

Campos de resposta

- `expires_in`: quanto tempo falta para o token expirar. O tempo de expiração padrão é de 12 horas.
- `refresh_token`: o token de atualização recebido da solicitação inicial do token.
- `token`: o token recebido da solicitação inicial do token.
- `token_type`: o valor será `Bearer`.
- `appfabric_user_id`- O ID AppFabric do usuário. Isso é retornado somente para solicitações que usem o tipo de concessão `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\"
```

```
}"
```

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

```
{
    "expires_in": 43200,
    "refresh_token": "apkaeibaerjr2example",
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "<userId>"
}
```

Etapa 3. Adicione a URL AppFabric do portal do usuário ao seu aplicativo

Os usuários finais precisam se AppFabric autorizar a acessar dados de seus aplicativos que são usados para gerar insights. AppFabric elimina a complexidade de os desenvolvedores de aplicativos controlarem esse processo criando um portal de usuário dedicado (uma tela pop-up) para que os usuários finais autorizem seus aplicativos. Quando os usuários estiverem prontos AppFabric para aumentar a produtividade, eles serão direcionados ao portal do usuário, que permite conectar e gerenciar aplicativos usados para gerar insights e ações entre aplicativos. Quando conectados, os usuários podem conectar aplicativos AppFabric para aumentar a produtividade e depois voltar ao seu aplicativo para explorar os insights e as ações. Para integrar seu aplicativo AppFabric para fins de produtividade, você precisa adicionar um AppFabric URL específico ao seu aplicativo. Essa etapa é crucial para permitir que os usuários acessem o portal AppFabric do usuário diretamente do seu aplicativo.

1. Navegue até as configurações da sua aplicação e localize a seção para adicionar URLs de redirecionamento.
2. Depois de encontrar a área apropriada, adicione o seguinte AppFabric URL como URL de redirecionamento para seu aplicativo:

```
https://userportal.appfabric.<region>.amazonaws.com/eup_login
```

Depois de adicionar a URL, seu aplicativo será configurado para direcionar os usuários ao portal do AppFabric usuário. Aqui, os usuários podem fazer login, conectar e gerenciar seus aplicativos usados AppFabric para gerar insights de produtividade.

Etapa 4. Use AppFabric para revelar informações e ações entre aplicativos

Depois que os usuários conectarem seus aplicativos, você poderá trazer os insights do usuário para melhorar sua produtividade, ajudando a reduzir a troca de aplicativos e contextos. AppFabric só gera insights para um usuário com base no que o usuário tem permissão para acessar. AppFabric armazena dados do usuário em uma Conta da AWS propriedade de AppFabric. Para obter informações sobre como AppFabric usa seus dados, consulteProcessamento de dados.

É possível usar as seguintes APIs baseadas em IA para gerar e exibir informações e ações em nível de usuário em suas aplicações:

- `ListActionableInsights`: para obter mais informações, consulte Informações acionáveis abaixo.
- `ListMeetingInsights`: para obter mais informações, consulte Preparação da reunião mais adiante neste guia.

Informações acionáveis (**`ListActionableInsights`**)

A API `ListActionableInsights` ajuda os usuários a gerenciar melhor seu dia, revelando informações oportunas baseadas nas atividades de todas as aplicações, incluindo emails, calendário, mensagens, tarefas e muito mais. As informações retornadas também mostrarão links incorporados para artefatos usados para gerar a informação, ajudando os usuários a visualizar rapidamente quais dados foram usados para gerar a informação. Além disso, a API pode retornar ações sugeridas com base na informação e permitir que os usuários executem ações entre aplicações de dentro da sua aplicação. Especificamente, a API se integra a plataformas como Asana, Google Workspace, Microsoft 365 e Smartsheet para permitir que os usuários enviem emails, criem eventos de calendário e criem tarefas. Os grandes modelo de linguagem (LLM) podem preencher previamente detalhes dentro de uma ação recomendada (como corpo do email ou nome da tarefa), que os usuários podem personalizar antes da execução, simplificando a tomada de decisões e aumentando a produtividade. Semelhante à experiência dos usuários finais de autorizar aplicativos, AppFabric usa o mesmo portal dedicado para que os usuários visualizem, editem e executem ações entre aplicativos. Para executar ações, AppFabric exige que os ISVs redirecionem os usuários para um portal AppFabric do usuário onde eles possam ver os detalhes das ações e executá-las. Cada ação gerada por AppFabric tem um URL exclusivo. Esse URL está disponível na resposta da resposta da API `ListActionableInsights`.

Abaixo há um resumo das ações entre aplicações com suporte e em quais aplicações:

- Enviar email (Google Workspace, Microsoft 365)
- Criar evento do calendário (Google Workspace, Microsoft 365)
- Criar tarefa (Asana, Smartsheet)

Campos de solicitação

- `nextToken` (opcional): o token de paginação para obter o próximo conjunto de informações.
- `includeActionExecutionStatus`: um filtro que aceita uma lista de status de execução da ação. As ações são filtradas com base nos valores de status passados. Valores possíveis: `NOT_EXECUTED` | `EXECUTED`

Cabeçalho da solicitação

- O cabeçalho da autorização precisa ser passado com o valor `Bearer Token` .

Campos de resposta

- `insightId`: o id exclusivo da informação gerada.
- `insightContent`: retorna um resumo da informação e links incorporados aos artefatos usados para gerar a informação. Observação: isso seria um conteúdo HTML contendo links incorporados (tags <a>).
- `insightTitle`: o título da informação gerada.
- `createdAt`: quando a informação foi gerada.
- `actions`: uma lista de ações recomendadas para a informação gerada. Objeto de ação:
  - `actionId`: o id exclusivo da ação gerada.
  - `actionIconUrl`: o URL do ícone da aplicação no qual a ação é sugerida para ser executada.
  - `actionTitle`: o título da ação gerada.
  - `actionUrl`- O URL exclusivo para o usuário final visualizar e executar a ação no portal AppFabric do usuário. Observação: para executar ações, os aplicativos ISV redirecionarão os usuários para o portal AppFabric do usuário (tela pop-up) usando essa URL.
  - `actionExecutionStatus`: uma enumeração que indica o status da ação. Os valores possíveis são: `EXECUTED` | `NOT_EXECUTED`

- `nextToken` (opcional): o token de paginação para obter o próximo conjunto de informações. É um campo opcional que, se retornado nulo, significa que não há mais informações a serem carregadas.

Para ter mais informações, consulte ActionableInsights.

```
curl -v --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/actionableInsights" \
  --header "Authorization: Bearer <token>"
```

Se a ação for bem-sucedida, o serviço retornará uma resposta 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
}
```

Preparação da reunião (**`ListMeetingInsights`**)

A API `ListMeetingInsights` ajuda os usuários a se prepararem melhor para as reuniões vindouras, resumindo o objetivo da reunião e revelando artefatos relevantes entre aplicações, como emails, mensagens e muito mais. Os usuários podem se preparar rapidamente para as reuniões agora e não perder tempo alternando entre aplicações para localizar conteúdo.

Campos de solicitação

- `nextToken` (opcional): o token de paginação para obter o próximo conjunto de informações.

Cabeçalho da solicitação

- O cabeçalho da autorização precisa ser passado com o valor `Bearer Token`.

Campos de resposta

- `insightId`: o id exclusivo da informação gerada.
- `insightContent`: a descrição da informação, destacando os detalhes em um formato de string. Por exemplo, por que essa informação é importante.
- `insightTitle`: o título da informação gerada.
- `createdAt`: quando a informação foi gerada.

- `calendarEvent`: o evento ou reunião importante do calendário em que o usuário deve se concentrar. Objeto Calendar Event:
  - `startTime`: a hora de início do evento.
  - `endTime`: a hora de término do evento.
  - `eventUrl`: o URL do evento do calendário na aplicação do ISV.
- `resources`: a lista contendo os outros recursos relacionados à geração da informação. Objeto de recurso:
  - `appName`: o nome da aplicação à qual o recurso pertence.
  - `resourceTitle`: o título do recurso.
  - `resourceType`: o tipo do recurso. Os valores possíveis são: `EMAIL` | `EVENT` | `MESSAGE` | `TASK`
  - `resourceUrl`: o URL do recurso na aplicação.
  - `appIconUrl`: o URL da imagem da aplicação à qual o recurso pertence.
- `nextToken` (opcional): o token de paginação para obter o próximo conjunto de informações. É um campo opcional que, se retornado nulo, significa que não há mais informações a serem carregadas.

Para ter mais informações, consulte MeetingInsights.

```
curl --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/meetingContexts" \
  --header "Authorization: Bearer <token>"
```

Se a ação for bem-sucedida, o serviço retornará uma resposta 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
}
```

Forneça comentários sobre suas informações ou ações

Use a operação AppFabric `PutFeedback` da API para fornecer feedback sobre as informações e ações geradas. Você pode incorporar esse recurso em seus aplicativos para fornecer uma forma de enviar uma avaliação de feedback (de 1 a 5, em que quanto maior a classificação, melhor) para um determinado InsightId ou ActionId.

Campos de solicitação

- `id`: o identificador do objeto para o qual o comentário está sendo enviado. Isso pode ser o InsightId ou ActionId o.
- `feedbackFor`: o tipo de recurso para o qual o comentário está sendo enviado. Valores possíveis: `ACTIONABLE_INSIGHT` | `MEETING_INSIGHT` | `ACTION`
- `feedbackRating`: classificação do comentário de 1 a 5. Quanto maior a classificação, melhor.

Campos de resposta

- Não há campos de resposta.

Para ter mais informações, 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
}'
```

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 201 com um corpo HTTP vazio.

Etapa 5. Solicitação AppFabric para verificar sua inscrição

Até agora, você atualizou a interface do usuário do seu aplicativo para incorporar informações e ações AppFabric entre aplicativos e recebeu insights para um único usuário. Depois de ficar satisfeito com o teste e quiser estender sua experiência AppFabric aprimorada para mais usuários, você pode enviar sua inscrição AppFabric para análise e verificação. AppFabric verificará as informações do aplicativo antes de permitir uma ampla adoção para ajudar a proteger os desenvolvedores de aplicativos, os usuários finais e seus dados, abrindo caminho para expandir a adoção pelos usuários de forma responsável.

Inicie o processo de verificação

Comece o processo de verificação enviando um email para appfabric-appverification@amazon.com e solicitando que sua aplicação seja verificada.

No email, inclua os detalhes a seguir:

- Seu Conta da AWS ID
- O nome da aplicação para a qual você está buscando verificação
- Seu AppClient ID
- Suas informações de contato

Além disso, forneça as seguintes informações, se disponíveis, para nos ajudar a avaliar a prioridade e o impacto:

- Um número estimado de usuários aos quais você planeja conceder acesso
- Sua data de lançamento prevista

> **Note**
>
> Se você tiver um Conta da AWS gerente ou gerente de desenvolvimento de AWS parceiros, copie-os em seu e-mail. Incluir esses contatos pode ajudar a agilizar o processo de verificação.

Critérios de verificação

Antes de usar esse processo de verificação, verifique se ele atende aos critérios a seguir.

- Você deve usar um válido Conta da AWS para usar AppFabric para produtividade

Além disso, você deve atender a pelo menos um destes critérios:

- Sua organização é AWS parceira AWS Partner Network com pelo menos um nível “AWS Selecionar”. Para obter mais informações, consulte Níveis de serviços de parceiros da AWS.
- Sua organização deveria ter gasto pelo menos $10.000 em AppFabric serviços nos últimos três anos.
- Sua aplicação deve estar listada no AWS Marketplace. Para obter mais informações, consulte o AWS Marketplace.

Aguarde a atualização do status da verificação

Depois que sua inscrição for analisada, responderemos por e-mail e o status de sua inscrição AppClient mudará de `pending_verification` para`verified`. Se a aplicação for rejeitada, você precisará reiniciar o processo de verificação.

Gerenciando AppFabric a produtividade AppClients

> O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Você pode gerenciar sua produtividade AppFabric para garantir AppClients a operação e a manutenção sem problemas dos processos de autenticação e autorização.

Obtenha detalhes de um AppClient

Use a operação AppFabric `GetAppClient` da API para ver detalhes sobre sua AppClient, incluindo verificar o AppClient status. Para ter mais informações, consulte GetAppClient.

Para obter detalhes de um AppClient, você deve ter, no mínimo, as permissões da política `"appfabric:GetAppClient"` do IAM. Para ter mais informações, consulte Permita o acesso para obter detalhes de AppClients.

Campos de solicitação

- `appClientId`- O AppClient ID.

Campos de resposta

- `appName`- O nome do aplicativo que será exibido aos usuários na página de consentimento do portal do AppFabric usuário.
- `customerManagedKeyIdentifier` (opcional): o ARN da chave gerenciada pelo cliente (gerada pelo KMS) a ser usada para criptografar os dados. Se não for especificado, a chave AWS AppFabric gerenciada será usada.
- `description`: uma descrição da aplicação.
- `redirectUrls`: o URI para o qual redirecionar os usuários finais após a autorização. É possível adicionar até 5 redirectUrls. Por exemplo, `https://localhost:8080`.
- `starterUserEmails`: um endereço de email do usuário que terá acesso para receber as informações até que a aplicação seja verificada. Só é permitido um endereço de email. Por exemplo, `anyuser@example.com`.
- `verificationStatus`- O status da AppClient verificação.
  - `pending_verification`- A verificação do ainda AppClient está em andamento com AppFabric. Até que AppClient seja verificado, somente um usuário (especificado em`starterUserEmails`) pode usar AppClient o.
  - `verified`- O processo de verificação foi concluído com sucesso AppFabric e agora AppClient está totalmente verificado.
  - `rejected`- O processo de verificação do AppClient foi rejeitado por AppFabric. Eles AppClient não podem ser usados por usuários adicionais até que o processo de verificação seja reiniciado e concluído com êxito.

```
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
```

Se a ação for bem-sucedida, o serviço retornará uma resposta 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

Use a operação de AppFabric `ListAppClients` API para ver uma lista de seus AppClients. AppFabric só permite um AppClient por Conta da AWS. Isso está sujeito a alterações no futuro. Para ter mais informações, consulte ListAppClients.

Para listar AppClients, você deve ter, no mínimo, as permissões da política `"appfabric:ListAppClients"` do IAM. Para ter mais informações, consulte Permitir acesso à lista AppClients.

Campos de solicitação

- Não há campos obrigatórios.

Campos de resposta

- `appClientARN`- O nome de recurso da Amazon (ARN) que inclui o AppClient ID. Por exemplo, o AppClient ID é`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `verificationStatus`- O status da AppClient verificação.
  - `pending_verification`- A verificação do ainda AppClient está em andamento com AppFabric. Até que AppClient seja verificado, somente um usuário (especificado em`starterUserEmails`) pode usar AppClient o.

- `verified`- O processo de verificação foi concluído com sucesso AppFabric e agora AppClient está totalmente verificado.
- `rejected`- O processo de verificação do AppClient foi rejeitado por AppFabric. Eles AppClient não podem ser usados por usuários adicionais até que o processo de verificação seja reiniciado e concluído com êxito.

```
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
```

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

```
200 OK

{
    "appClientList": [
        {
            "appClientArn": "arn:aws:appfabric:<region>:111122223333:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "verificationStatus": "pending_verification"
        }
    ]
}
```

Atualizar um AppClient

Use a operação da AppFabric `UpdateAppClient` API para atualizar os redirectUrls mapeados para o seu. AppClient Se precisar alterar qualquer outro parâmetro, como AppName starterUserEmails, ou outro, exclua o AppClient e crie um novo. Para ter mais informações, consulte UpdateAppClient.

Para atualizar um AppClient, você deve ter, no mínimo, as permissões da política `"appfabric:UpdateAppClient"` do IAM. Para ter mais informações, consulte Permitir acesso à atualização AppClients.

Campos de solicitação

- `appClientId`(obrigatório) - O AppClient ID com o qual você está atualizando os RedirectUrls.
- `redirectUrls` (obrigatório): a lista atualizada dos redirectUrls. É possível adicionar até 5 redirectUrls.

Campos de resposta

- `appName`- O nome do aplicativo que será exibido aos usuários na página de consentimento do portal do AppFabric usuário.
- `customerManagedKeyIdentifier` (opcional): o ARN da chave gerenciada pelo cliente (gerada pelo KMS) a ser usada para criptografar os dados. Se não for especificado, a chave AWS AppFabric gerenciada será usada.
- `description`: uma descrição da aplicação.
- `redirectUrls`: o URI para o qual redirecionar os usuários finais após a autorização. Por exemplo, `https://localhost:8080`.
- `starterUserEmails`: um endereço de email do usuário que terá acesso para receber as informações até que a aplicação seja verificada. Só é permitido um endereço de email. Por exemplo, `anyuser@example.com`.
- `verificationStatus`- O status da AppClient verificação.
  - `pending_verification`- A verificação do ainda AppClient está em andamento com AppFabric. Até que AppClient seja verificado, somente um usuário (especificado em`starterUserEmails`) pode usar AppClient o.
  - `verified`- O processo de verificação foi concluído com sucesso AppFabric e agora AppClient está totalmente verificado.
  - `rejected`- O processo de verificação do AppClient foi rejeitado por AppFabric. Eles AppClient não podem ser usados por usuários adicionais até que o processo de verificação seja reiniciado e concluído com êxito.

```
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"]
}'
```

Se a ação for bem-sucedida, o serviço retornará uma resposta 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"
        }
    }
}
```

Excluir um AppClient

Use a operação AppFabric API `DeleteAppClient` para excluir as AppClients que você não precisa mais. Para ter mais informações, consulte DeleteAppClient.

Para excluir um AppClient, você deve ter, no mínimo, as permissões da política `"appfabric:DeleteAppClient"` do IAM. Para ter mais informações, consulte Permitir acesso para excluir AppClients.

Campos de solicitação

- `appClientId`- O AppClient ID.

Campos de resposta

- Não há campos de resposta.

```
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
```

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 204 com um corpo HTTP vazio.

Atualizar tokens para usuários finais

Os tokens que você AppClient adquire para os usuários finais podem ser atualizados no vencimento. Isso pode ser feito usando a API Token com o grant_type `refresh_token`. O `refresh_token` a ser usado é retornado como parte da resposta da API do token quando o grant_type for `authorization_code`. O tempo de expiração padrão é de 12 horas. Para chamar a API de atualização, você precisa ter a permissão da política do IAM `"appfabric:Token"`. Para obter mais informações, consulte Token e Permitir acesso à atualização AppClients.

Campos de solicitação

- `refresh_token` (obrigatório): o token de atualização recebido da solicitação `/token` inicial.
- `app_client_id`(obrigatório) - O ID do AppClient recurso criado para Conta da AWS o.
- `grant_type` (obrigatório): isso deve ser `refresh_token`.

Campos de resposta

- `expires_in`: quanto tempo falta para o token expirar. O tempo de expiração padrão é de 12 horas.
- `refresh_token`: o token de atualização recebido da solicitação inicial do token.
- `token`: o token recebido da solicitação inicial do token.
- `token_type`: o valor será `Bearer`.
- `appfabric_user_id`- O ID AppFabric do usuário. Isso é retornado somente para solicitações que usem o tipo de concessão `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\"
}"
```

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

```
200 OK

{
    "expires_in": 43200,
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "${UserID}"
}
```

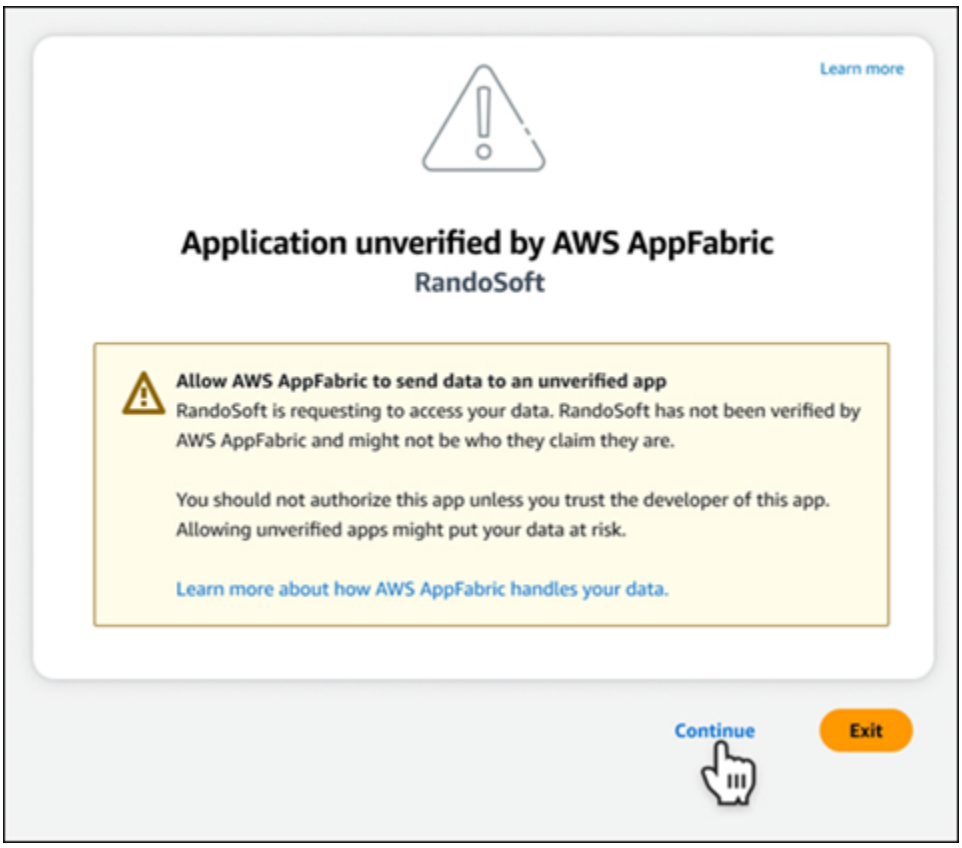
Solução de problemas

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Esta seção descreve erros comuns e soluções de problemas AppFabric para aumentar a produtividade.

Aplicação não verificada

Os desenvolvedores de aplicativos que usam a produtividade AppFabric para enriquecer suas experiências de aplicativos passarão por um processo de verificação antes de lançar seus recursos para os usuários finais. Todas as aplicações começam como não verificadas e mudam para verificadas somente quando o processo de verificação é concluído. Isso significa que o que `starterUserEmails` você usou ao criar um AppClient verá essa mensagem.



Erros do **`CreateAppClient`**

ServiceQuotaExceededException

Se você receber a seguinte exceção ao criar um AppClient, você excedeu o número AppClients que pode ser criado por Conta da AWS. O limite é 1. Código de status 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
```

Erros do **`GetAppClient`**

ResourceNotFoundException

Se você receber a seguinte exceção ao obter detalhes de um AppClient, verifique se inseriu o AppClient identificador correto. Esse erro significa que o especificado não AppClient foi encontrado.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
```

```
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Erros do **`DeleteAppClient`**

ConflictException

Se você receber a exceção a seguir ao excluir uma AppClient, outra solicitação de exclusão está em andamento. Espere até que seja concluída e tente novamente. Código de Status HTTP: 409

```
ConflictException
Another delete request is in progress. Wait until it completes then try again.
HTTP Status Code: 409
```

ResourceNotFoundException

Se você receber a seguinte exceção ao excluir um AppClient, verifique se inseriu o AppClient identificador correto. Esse erro significa que o especificado não AppClient foi encontrado.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Erros do **`UpdateAppClient`**

ResourceNotFoundException

Se você receber a seguinte exceção ao atualizar um AppClient, verifique se inseriu o AppClient identificador correto. Esse erro significa que o especificado não AppClient foi encontrado.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Erros do **`Authorize`**

ValidationException

Você poderá receber a exceção a seguir se algum dos parâmetros da API não atender às restrições definidas nas especificações da API.

```
ValidationException
HTTP Status Code: 400
```

Razão 1: quando o AppClient ID não é especificado

O `app_client_id` está ausente nos parâmetros da solicitação. Crie o AppClient se ainda não tiver sido criado ou use o existente `app_client_id` e tente novamente. Para encontrar o AppClient ID, use a operação ListAppClientda API.

Motivo 2: Quando AppFabric não tem acesso à chave gerenciada pelo cliente

```
Message: AppFabric couldn't access the customer managed key configured for AppClient.
```

AppFabric atualmente não consegue acessar as chaves gerenciadas pelo cliente, provavelmente devido a mudanças recentes em suas permissões. Verifique se a chave especificada existe e garanta que AppFabric as permissões de acesso apropriadas sejam concedidas.

Motivo 3: O URL de redirecionamento especificado não é válido

```
Message: Redirect url invalid
```

Certifique-se de que o URL de redirecionamento em sua solicitação esteja correto. Ele deve corresponder a um dos URLs de redirecionamento especificados quando você criou ou atualizou o. AppClient Para ver a lista de URLs de redirecionamento permitidos, use a operação da GetAppClientAPI.

Erros do **`Token`**

TokenException

Você poderá receber a exceção a seguir por alguns motivos.

```
TokenException
HTTP Status Code: 400
```

Motivo 1: quando um email inválido é especificado

```
Message: Invalid Email used
```

Verifique se o endereço de e-mail que você está usando corresponde ao listado para o `starterUserEmails` atributo quando você criou AppClient o. Se os emails não corresponderem, mude para o endereço de email correspondente e tente novamente. Para ver o e-mail usado, use a operação GetAppClientda API.

Motivo 2: Para grant_type como refresh_token quando o token não for especificado.

```
Message: refresh_token must be non-null for Refresh Token Grant-type
```

O token de atualização especificado na solicitação é nulo ou está vazio. Especifique um `refresh_token` ativo recebido na resposta de chamada da API Token.

ThrottlingException

Você poderá receber a exceção a seguir se a API estiver sendo chamada a uma taxa maior do que a cota permitida.

```
ThrottlingException
HTTP Status Code: 429
```

Erros **`ListActionableInsights`**, **`ListMeetingInsights`** e **`PutFeedback`**

ValidationException

Você poderá receber a exceção a seguir se algum dos parâmetros da API não atender às restrições definidas nas especificações da API.

```
ValidationException
HTTP Status Code: 400
```

ThrottlingException

Você poderá receber a exceção a seguir se a API estiver sendo chamada a uma taxa maior do que a cota permitida.

```
ThrottlingException
```

```
HTTP Status Code: 429
```

Introdução à AppFabric produtividade (versão prévia) para usuários finais

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Esta seção é destinada aos usuários finais de aplicativos SaaS que desejam aumentar a produtividade (versão prévia) AWS AppFabric para melhorar o gerenciamento de tarefas e a eficiência do fluxo de trabalho. Siga estas etapas para conectar seus aplicativos e AppFabric autorizar a revelar insights entre aplicativos e ajudá-lo a concluir ações (como enviar um e-mail ou agendar uma reunião) a partir de seus aplicativos preferidos. Você pode conectar aplicações como Asana, Atlassian Jira Suite, Google Workspace, Microsoft 365, Miro, Slack, Smartsheet e muito mais. Depois de autorizar AppFabric o acesso ao seu conteúdo, AppFabric traz insights e ações entre aplicativos diretamente para seus aplicativos preferidos, ajudando você a trabalhar com mais eficiência e a permanecer dentro dos fluxos de trabalho atuais.

AppFabric para produtividade, usa IA generativa que é alimentada pelo Amazon Bedrock. AppFabric gerará insights e ações somente após receber sua permissão explícita. Você autoriza cada aplicativo individual a manter o controle total de qual conteúdo é usado. AppFabric não usará seus dados para treinar ou melhorar os grandes modelos de linguagem subjacentes usados para gerar insights. Para obter mais informações, consulte Perguntas frequentes do Amazon Bedrock.

Tópicos

- Pré-requisitos
- Etapa 1. Faça login em AppFabric
- Etapa 2. Forneça consentimento para que a aplicação exiba informações
- Etapa 3. Conecte suas aplicações para gerar informações e ações
- Etapa 4. Comece a ver informações e execute ações entre aplicações em sua aplicação
- Atenção, administradores de TI e segurança: gerenciando o acesso aos recursos AppFabric de produtividade (versão prévia)
- Solução de problemas

Pré-requisitos

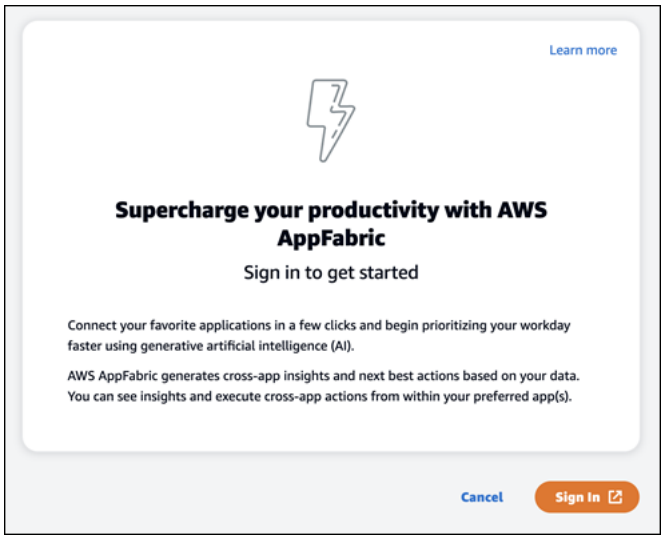
Antes de iniciar, verifique se você possui:

- Credenciais para entrar AppFabric: Para começar a usar AppFabric para fins de produtividade, você precisará de credenciais de login federadas (nome de usuário e senha) para um dos seguintes provedores:Asana,,, ou. Google Workspace Microsoft 365 Slack Fazer login nos AppFabric ajuda a identificá-lo como usuário em cada aplicativo que você habilita AppFabric para produtividade. Depois de fazer login, você poderá conectar suas aplicações para começar a gerar informações.
- Credenciais para conectar suas aplicações: informações e ações entre aplicações são geradas somente com base nas aplicações que você autorizar. Você precisará de credenciais de login (nome de usuário e senha) para cada uma das aplicações que desejar autorizar. As aplicações com suporte incluem Asana, Atlassian Jira Suite, Google Workspace, Microsoft 365, Miro, Slack e Smartsheet.

Etapa 1. Faça login em AppFabric

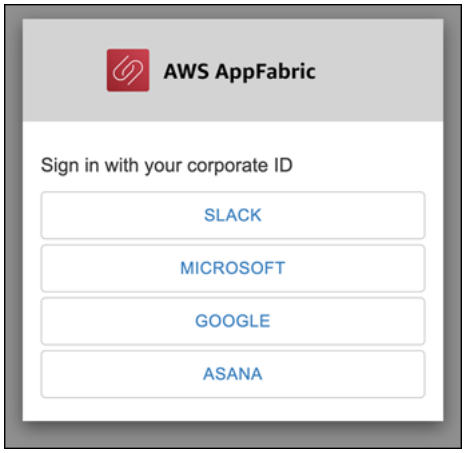
Conecte aplicativos AppFabric para trazer seu conteúdo e insights diretamente para seus aplicativos preferidos.

1. Cada aplicativo será usado AppFabric para produtividade de maneiras diferentes para proporcionar experiências de aplicativo mais ricas. Devido a isso, cada aplicativo terá um ponto de entrada diferente para acessar a AppFabric página inicial de produtividade abaixo. A página inicial define o contexto sobre o processo a ser ativado AppFabric e primeiro solicita que você faça login. Cada aplicativo que você deseja ativar AppFabric chegará a essa tela.

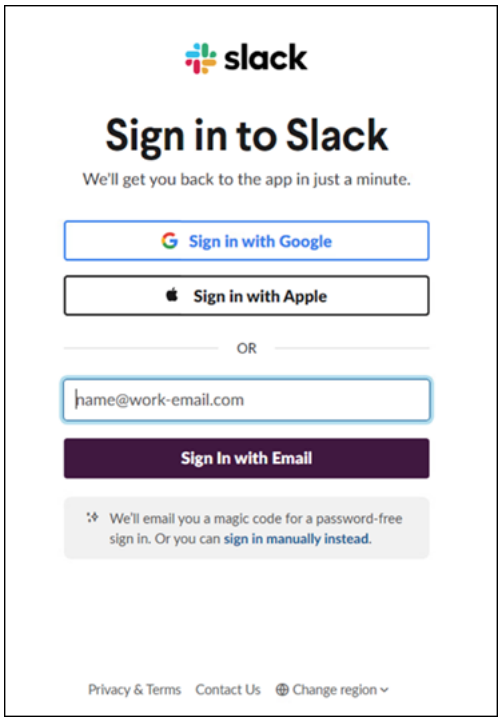


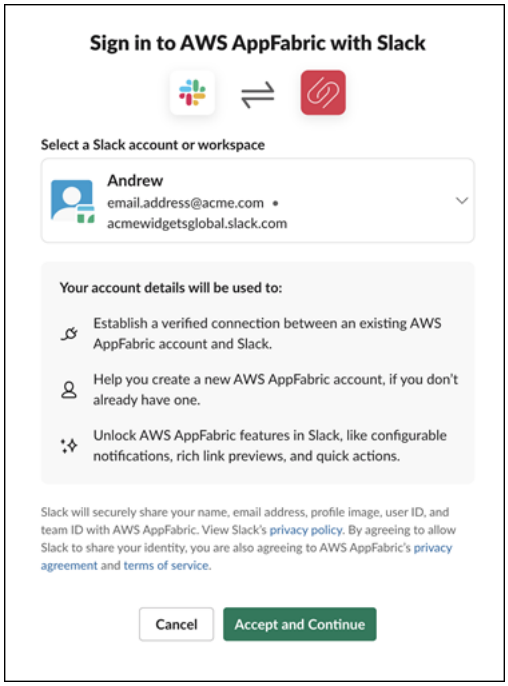
2. Faça login com suas credenciais de um destes provedores: Asana, Google Workspace, Microsoft 365 ou Slack. Para obter a melhor experiência, recomendamos fazer login usando o mesmo provedor para cada aplicativo AppFabric ativado. Por exemplo, se você escolher as

credenciais do Google Workspace no App1, recomendamos escolher Google Workspace no App2, bem como todas as outras vezes em que precisar fazer login novamente. Se você fizer login com um provedor diferente, precisará reiniciar o processo de conexão das aplicações.



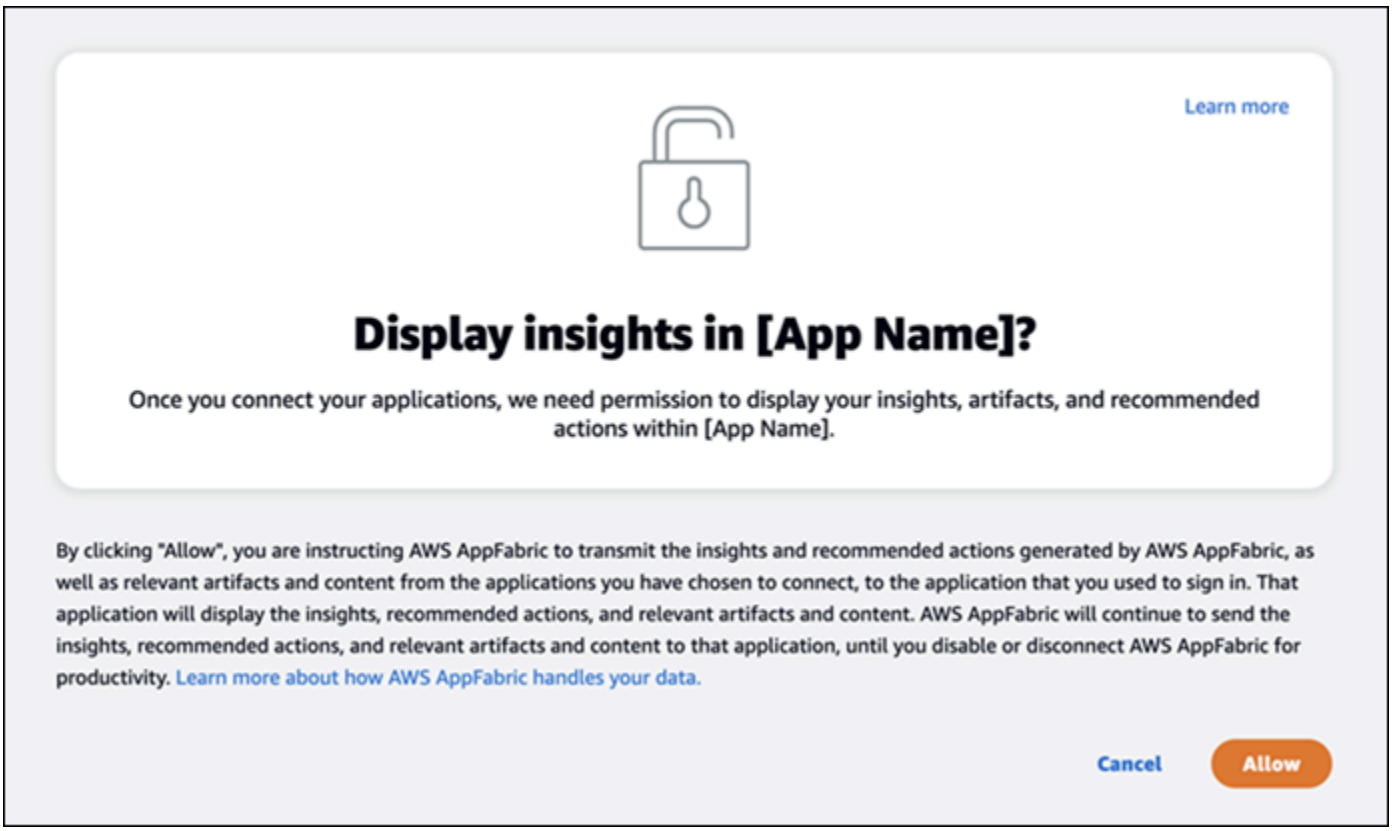
3. Se solicitado, insira suas credenciais de login e aceite o login AppFabric desse provedor.





Etapa 2. Forneça consentimento para que a aplicação exiba informações

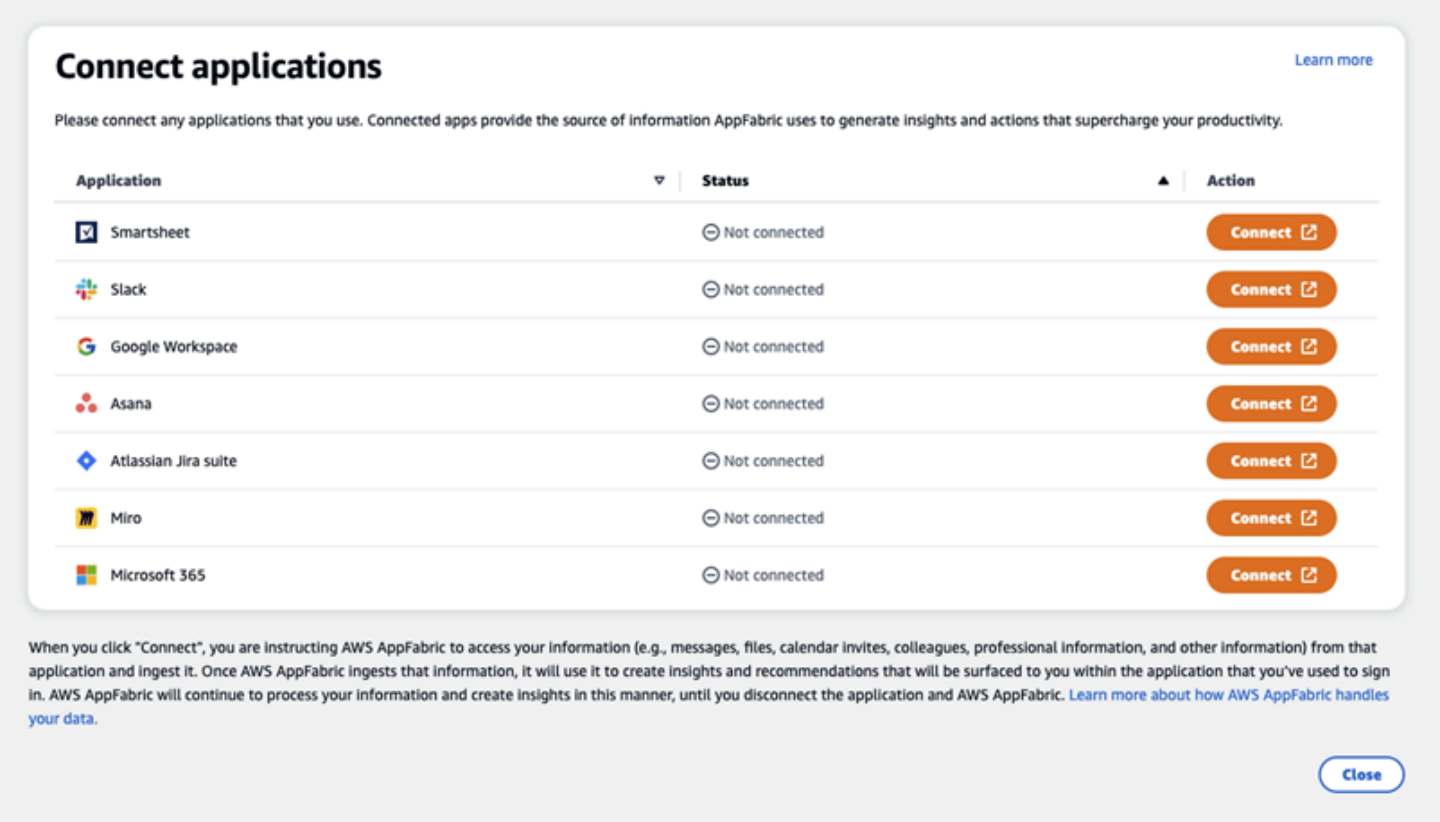
Depois de fazer login, AppFabric será exibida uma página de consentimento perguntando se você permite AppFabric a exibição de informações e ações entre aplicativos dentro do aplicativo em que você está ativando AppFabric a produtividade. Por exemplo, você permite AppFabric pegar seus Google Workspace e-mails e eventos do calendário e exibi-los emAsana. Você só precisa concluir essa etapa de consentimento uma vez por aplicativo AppFabric ativado.



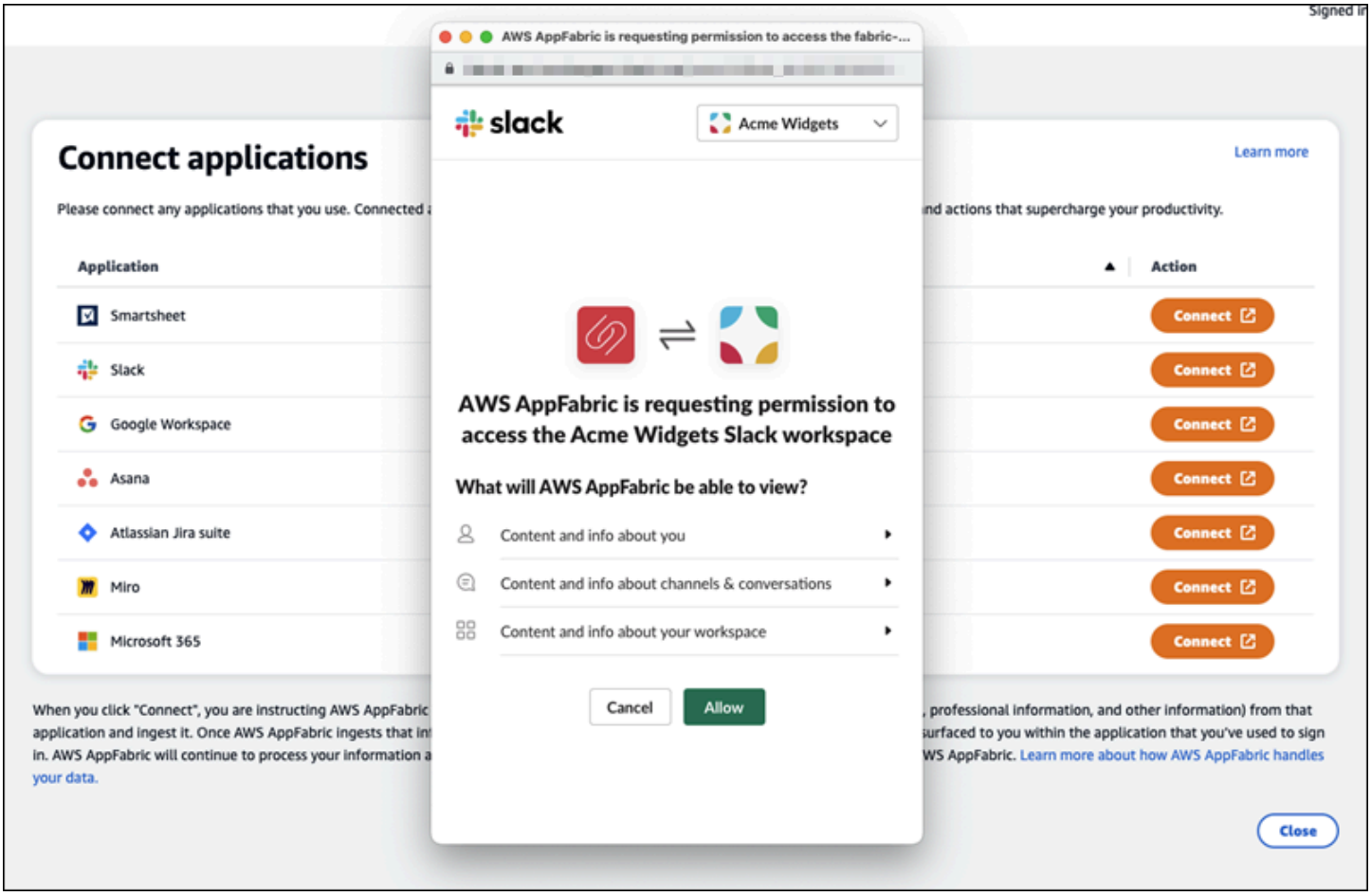
Etapa 3. Conecte suas aplicações para gerar informações e ações

Depois de concluir a página de consentimento, você será direcionado para a página Conectar aplicações, onde poderá conectar, desconectar ou reconectar aplicações individuais que, em última análise, são usadas para gerar suas informações e ações entre aplicações. Na maioria dos casos, depois de fazer login e fornecer consentimento, você continuará usando esta página para gerenciar suas aplicações conectadas.

Para conectar uma aplicação, escolha o botão Conectar ao lado de qualquer aplicação que você usar.



Você precisará fornecer suas credenciais de login para o aplicativo e AppFabric permitir o acesso aos seus dados para gerar insights e concluir ações.

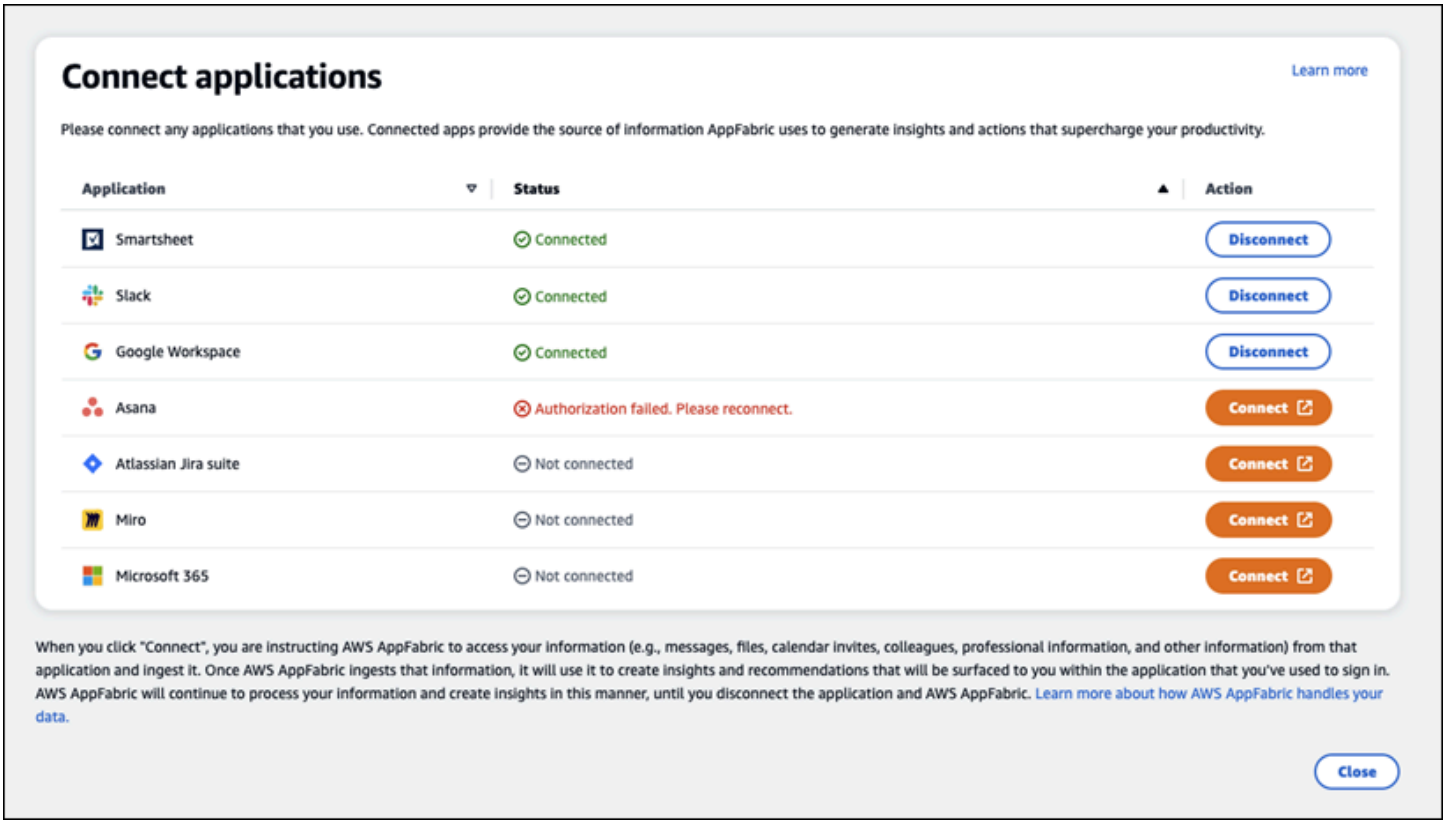


Depois de conectar uma aplicação com êxito, o status dessa aplicação mudará de “Não conectada” para “Conectada”. Lembrete: você precisa concluir essa etapa de autorização para cada aplicação que desejar que seja usada para gerar informações e ações.

Depois de conectar uma aplicação, ela não ficará conectada para sempre. Você precisará reconectar as aplicações periodicamente. Fazemos isso para garantir que ainda tenhamos sua permissão para gerar informações.

Os possíveis status das aplicações são:

- Conectado - AppFabric está autorizado e está gerando insights usando seus dados desse aplicativo.
- Não conectado - AppFabric não está gerando insights usando dados desse aplicativo. Você pode se conectar para começar a gerar informações.
- Falha na autorização. Reconecte. - Pode haver uma falha na autorização com uma aplicação específica. Se necessário, insira suas credenciais de login para acessar o repositório.



A configuração está concluída e você pode retornar à sua aplicação. Pode levar pelo menos algumas horas para começar a ver informações em suas aplicações.

Conforme necessário, você pode voltar para esta página para gerenciar suas aplicações conectadas. Se você optar por desconectar um aplicativo, AppFabric deixará de usar dados desse aplicativo ou de coletar novos dados para gerar novos insights. Os dados de aplicações desconectadas serão excluídos automaticamente em 7 dias se você optar por não reconectar a aplicação nesse período.

Etapa 4. Comece a ver informações e execute ações entre aplicações em sua aplicação

Depois de conectar seus aplicativos AppFabric, você terá acesso a informações valiosas e a capacidade de realizar ações entre aplicativos diretamente do seu aplicativo preferido. Observação: essa funcionalidade não é garantida em cada aplicativo e depende inteiramente AppFabric de quais recursos de produtividade o desenvolvedor do aplicativo escolheu ativar.

Informações entre aplicações

AppFabric para produtividade oferece dois tipos de insights:

- Insights acionáveis: AppFabric analisa informações de seus e-mails, eventos do calendário, tarefas e mensagens em seus aplicativos conectados e gera insights importantes que podem ser importantes para você priorizar. Além disso, AppFabric pode gerar ações recomendadas (como enviar e-mail, agendar reuniões e criar tarefas) que você pode editar e executar enquanto permanece em seu aplicativo preferido. Por exemplo, você pode receber uma informação dizendo que há uma escalação de clientes a ser resolvida e uma próxima ação sugerida para agendar uma reunião com seu cliente.
- Informações sobre a preparação de reuniões: esse recurso ajuda você a se preparar melhor para as próximas reuniões. AppFabric analisará suas próximas reuniões e gerará um resumo conciso sobre o objetivo da reunião. Além disso, ele exibirá artefatos relevantes (como emails, mensagens e tarefas) de suas aplicações conectadas que serão úteis para ajudá-lo a se preparar com eficiência para a reunião sem precisar alternar entre aplicações para encontrar conteúdo.

Ações entre aplicações

Para determinados insights, também AppFabric pode gerar ações recomendadas, como enviar um e-mail, agendar uma reunião ou criar uma tarefa. Ao gerar ações, AppFabric pode pré-preencher determinados campos com base no conteúdo e no contexto de seus aplicativos conectados. Por exemplo, AppFabric pode gerar uma resposta de e-mail sugerida ou um nome de tarefa com base no insight. Ao clicar em uma ação sugerida, você será direcionado para uma interface de usuário AppFabric própria, na qual poderá editar o conteúdo pré-preenchido antes de executar a ação. AppFabric não executará ações sem a análise e a entrada do usuário primeiro, pois a IA generativa e os modelos de linguagem grande (LLM) subjacentes podem alucinar de tempos em tempos.

> **Note**
>
> Você tem a responsabilidade de validar e confirmar os resultados do AppFabric LLM. AppFabric não garante a precisão ou a qualidade de suas saídas LLM. Para obter mais informações, consulte Política de IA responsável da AWS.

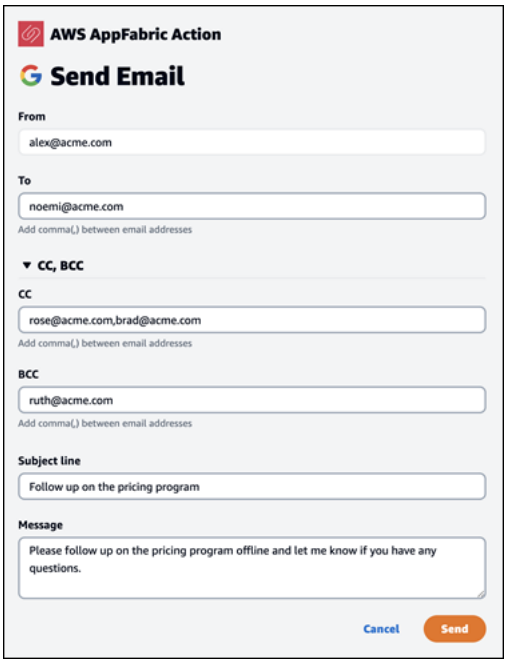
Criar emails (Google Workspace, Microsoft 365)

AppFabric permite que você edite e envie um e-mail de dentro do seu aplicativo preferido. Oferecemos suporte a campos básicos de e-mail, incluindo De, Para, Cc/Bcc, Linha de assunto do e-mail e Corpo da mensagem do e-mail. AppFabric pode gerar conteúdo nesses campos para ajudá-lo

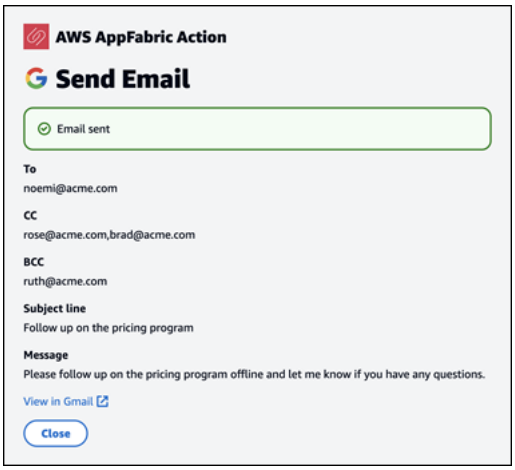
a reduzir o tempo de conclusão da tarefa. Depois de terminar de editar o email, escolha Enviar para enviar o email.

Os campos a seguir são obrigatórios para enviar um email:

- Pelo menos um dos emails do destinatário (Para, CC e BCC) é obrigatório e deve ser um endereço de email válido.
- Campos de linha de assunto e mensagem.



Depois que o email for enviado, você verá uma confirmação de que o email foi enviado. Além disso, você verá um link para ver o email na aplicação designada. Você pode usar esse link para navegar rapidamente até a aplicação e verificar se o email foi enviado.

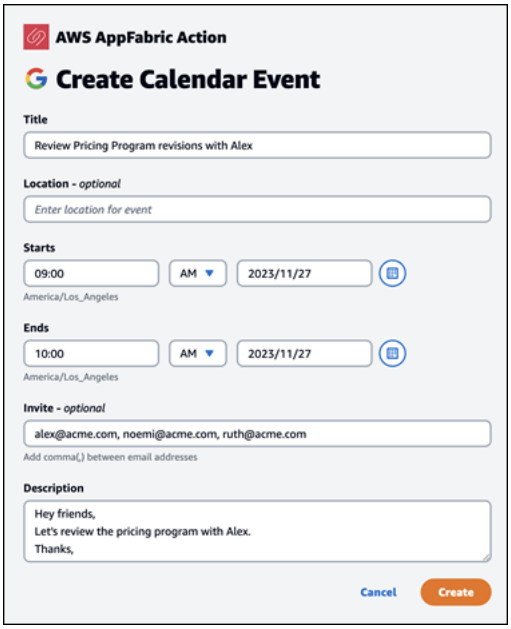


Criar evento de calendário (Google Workspace, Microsoft 365)

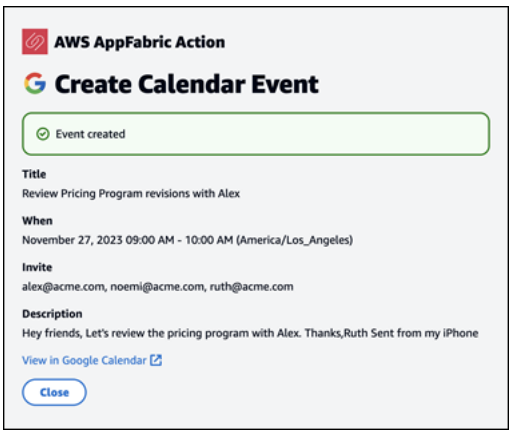
AppFabric permite que você edite e crie um evento de calendário a partir do seu aplicativo preferido. Oferecemos suporte aos campos básicos de eventos do calendário, incluindo título do evento, local, hora e data de início/término, lista de convidados e detalhes do evento. AppFabric pode gerar conteúdo nesses campos para ajudá-lo a reduzir o tempo de conclusão da tarefa. Depois de terminar de editar o evento do calendário, escolha Criar para criar o evento.

Os campos a seguir são obrigatórios para criar um evento de calendário:

- Campos Título, Início, Fim e Descrição.
- A hora e a data de início não devem ser anteriores à hora e data de término.
- O campo de convite é opcional, mas requer endereços de email válidos, se fornecidos.



Depois que o evento do calendário for enviado, você verá uma confirmação de que o evento foi criado. Além disso, você verá um link para ver o evento na aplicação designada. Você pode usar esse link para navegar rapidamente até a aplicação e verificar se o evento foi criado.

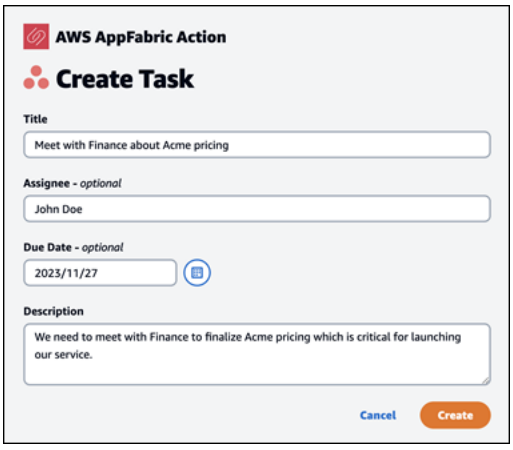


Criar tarefas (Asana)

AppFabric permite que você edite e crie uma tarefa de dentro Asana do seu aplicativo preferido. Oferecemos suporte a campos básicos de tarefas, como nome da tarefa, proprietário da tarefa, data de vencimento e descrição da tarefa. AppFabric pode gerar conteúdo nesses campos para ajudá-lo a reduzir o tempo de criação da tarefa. Depois de terminar de editar a tarefa, escolha Criar para criar a tarefa. As tarefas são criadas no espaço de trabalho, projeto ou tarefa aplicável do Asana, conforme sugerido pelo LLM.

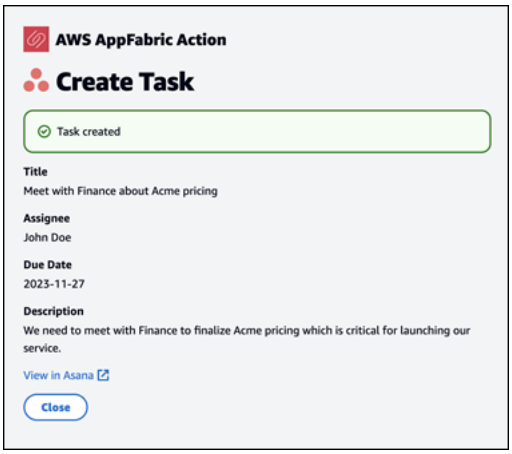
Os campos a seguir são obrigatórios para criar uma tarefa do Asana:

- Campos Título e Descrição.
- O destinatário deve ser um endereço de email válido se modificado.



Depois que a tarefa for criada, você verá uma confirmação de que a tarefa foi criada no Asana. Além disso, você verá um link para visualizar a tarefa no Asana. É possível usar esse link para

navegar rapidamente até a aplicação para verificar se a tarefa foi criada ou movê-la para o espaço de trabalho, projeto ou tarefa do Asana apropriados.

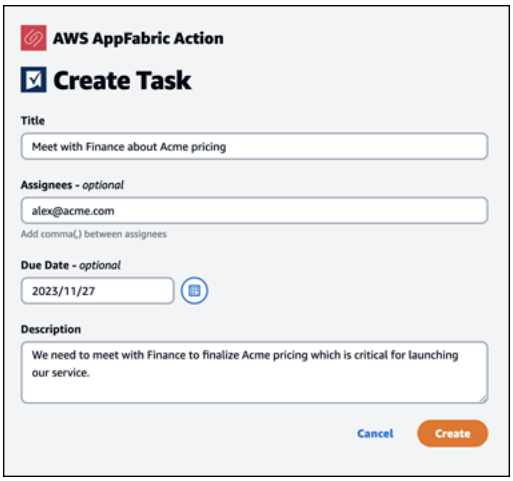


Criar tarefas (Smartsheet)

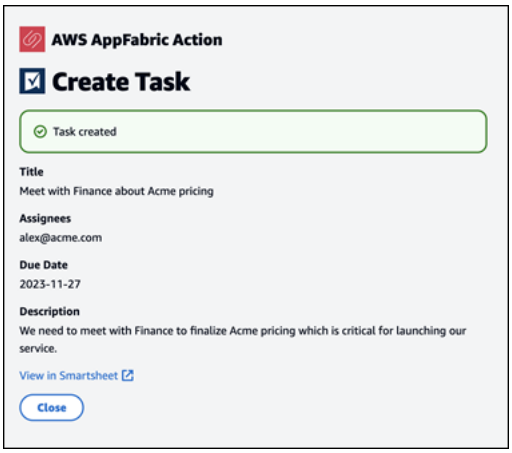
AppFabric permite que você edite e crie uma tarefa de dentro Smartsheet do seu aplicativo preferido. Oferecemos suporte a campos básicos de tarefas, como nome da tarefa, proprietário da tarefa, data de vencimento e descrição da tarefa. AppFabric pode gerar conteúdo nesses campos para ajudá-lo a reduzir o tempo de criação da tarefa. Depois de terminar de editar a tarefa, escolha Criar para criar a tarefa. Para Smartsheet tarefas, AppFabric criará uma nova Smartsheet planilha privada e preencherá todas as tarefas criadas. Isso é feito para ajudar a centralizar as ações AppFabric geradas em um único local de forma estruturada.

Os campos a seguir são obrigatórios para criar uma tarefa do Smartsheet:

- Campos Título e Descrição.
- O destinatário deve ter um endereço de email válido, se fornecido.



Depois que a tarefa for criada, você verá uma confirmação de que a tarefa foi criada no Smartsheet. Além disso, você verá um link para visualizar a tarefa no Smartsheet. É possível usar esse link para navegar rapidamente até a aplicação para visualizar a tarefa na planilha do Smartsheet criada. Todas as tarefas futuras do Smartsheet serão preenchidas nessa planilha. Se a planilha for excluída, AppFabric criará uma nova.



Atenção, administradores de TI e segurança: gerenciando o acesso aos recursos AppFabric de produtividade (versão prévia)

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

O portal do usuário AppFabric para produtividade está acessível publicamente a todos os usuários de aplicativos SaaS que se integraram aos recursos AppFabric de produtividade (versão prévia). Se você é um administrador de TI e deseja gerenciar o acesso a esses recursos de IA generativa em sua organização, considere estas opções:

- Restringir o login do provedor de identidades (IdP): você pode bloquear o acesso ao login por meio do seu provedor de identidades para controlar o acesso do usuário aos recursos de IA generativa.
- Desativar o OAuth para aplicações específicas: implemente restrições downstream desativando o OAuth. Essa ação impede que os usuários conectem aplicações que exijam autenticação OAuth ao espaço de trabalho da empresa.

Solução de problemas

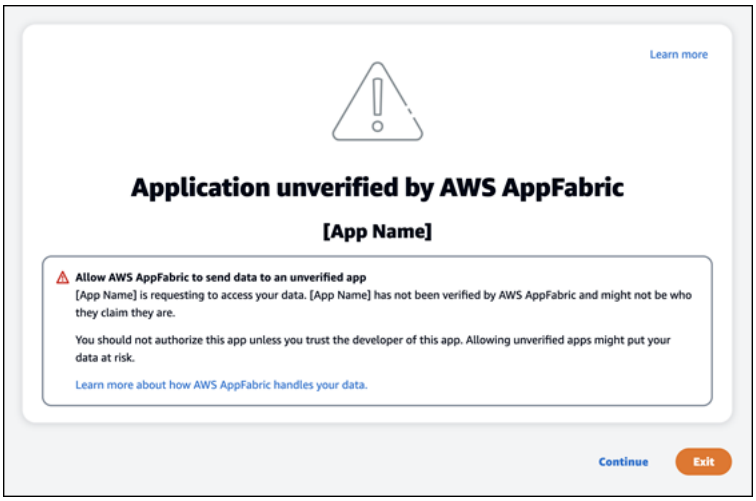
O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Esta seção descreve erros comuns e soluções de problemas AppFabric para aumentar a produtividade.

Aplicação não verificada

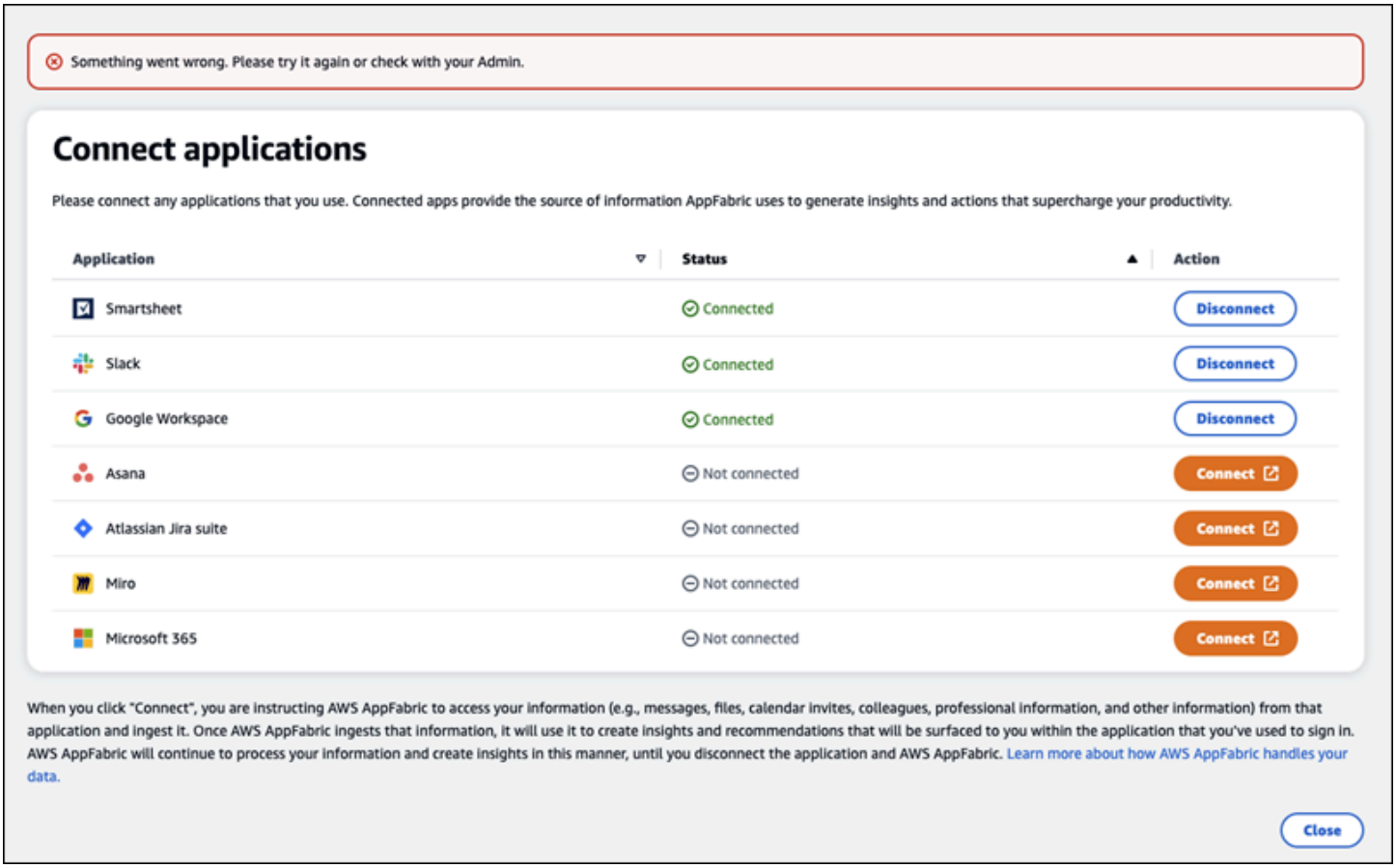
Os aplicativos que usam a produtividade AppFabric para enriquecer suas experiências de aplicativos passarão por um processo de verificação antes de lançarem seus recursos para os usuários finais. Se você encontrar um banner “não verificado” ao tentar fazer login AppFabric, isso significa que o aplicativo não passou pelo processo de verificação que confirma a identidade AppFabric do desenvolvedor do aplicativo e a precisão das informações de registro do aplicativo. Todas as aplicações começam como não verificadas e mudam para verificadas somente quando o processo de verificação é concluído.

Tenha cuidado ao usar uma aplicação não verificada. Se você não tiver certeza sobre os desenvolvedores da aplicação, espere até que a aplicação atinja o status de verificada antes de continuar.



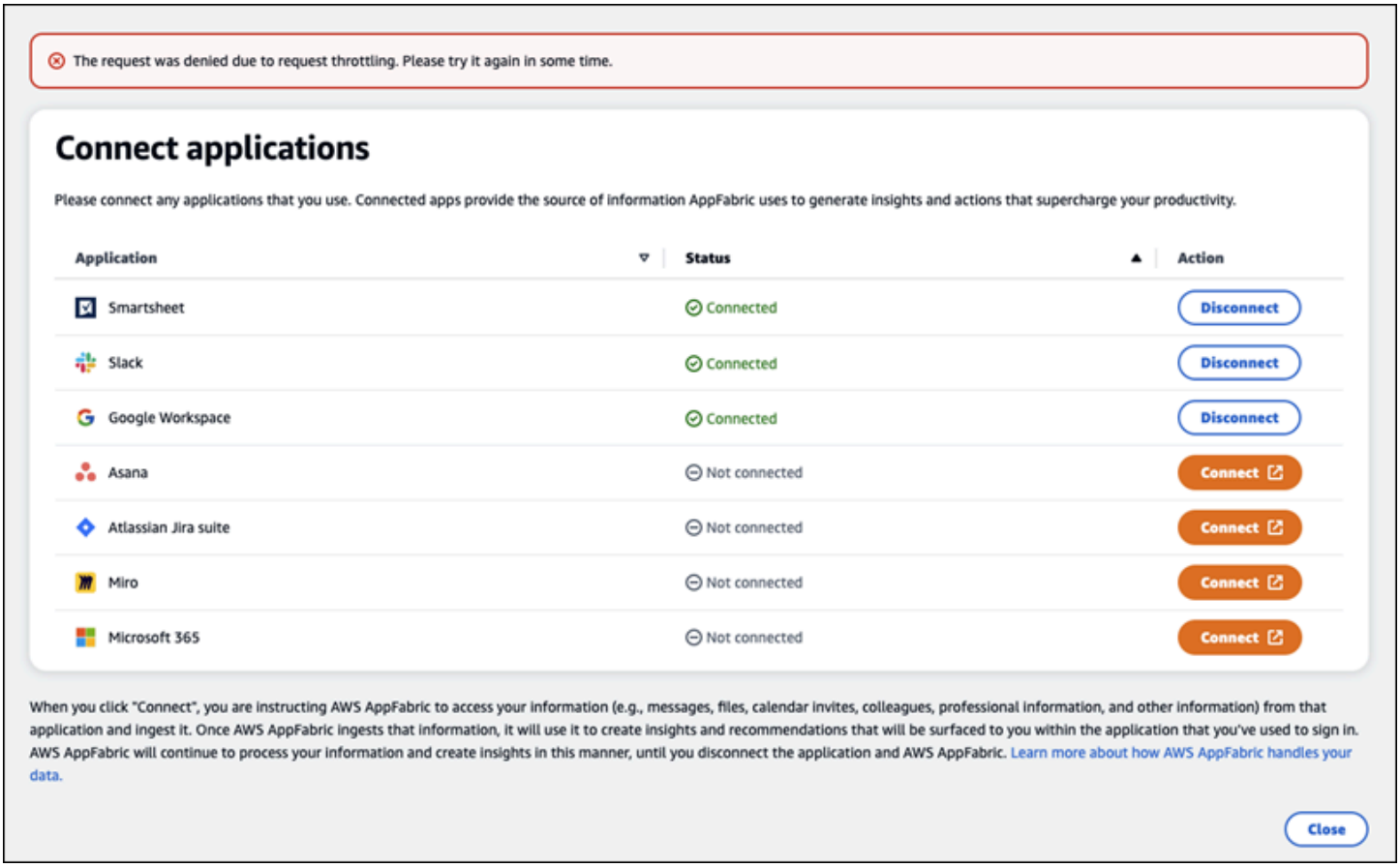
Algo deu errado. Tente novamente ou verifique com seu administrador (**`InternalServerException`**)

Você pode receber essa mensagem quando o portal AppFabric do usuário não consegue listar os aplicativos ou desconecta um aplicativo devido a um erro, exceção ou falha desconhecidos. Tente novamente mais tarde.



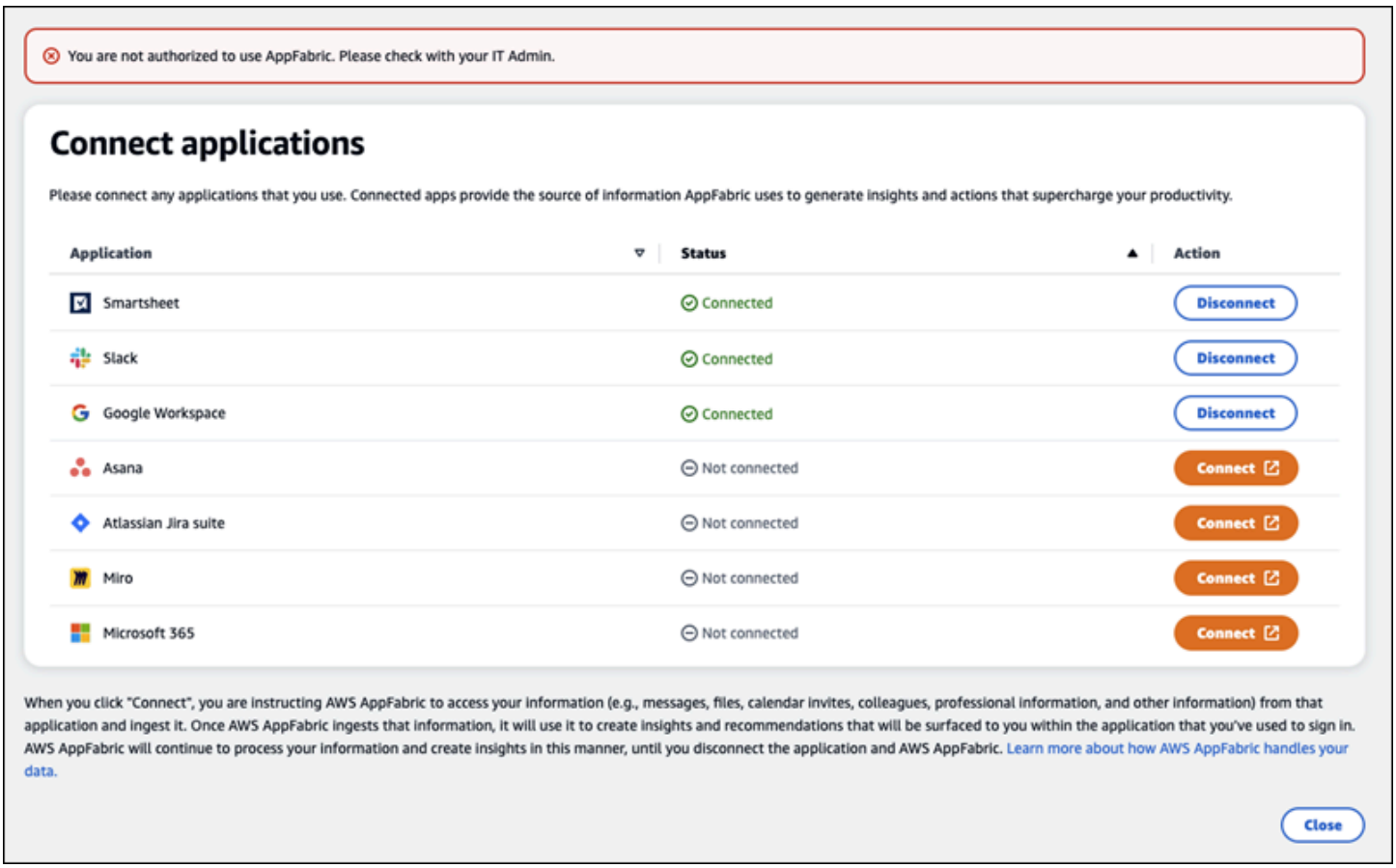
A solicitação foi negada devido ao controle de utilização da solicitação. Por favor, tente novamente daqui a algum tempo (**`ThrottlingException`**)

Você pode receber essa mensagem quando o portal AppFabric do usuário não consegue listar os aplicativos ou desconecta um aplicativo devido a um problema de limitação. Tente novamente mais tarde.



Você não está autorizado a usar AppFabric. Por favor, faça login AppFabric novamente (**`AccessDeniedException`**)

Você pode receber essa mensagem quando o portal AppFabric do usuário não consegue listar os aplicativos ou desconecta um aplicativo devido a uma exceção de acesso negado. Faça login AppFabric novamente.



AppFabric APIs de produtividade

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Esta seção fornece as operações de API, os tipos de dados e os erros comuns dos recursos de AWS AppFabric produtividade.

> **Note**
>
> Para todas as outras AppFabric APIs, consulte a Referência da AWS AppFabric API.

Tópicos

- Ações
- Tipos de dados
- Erros comuns

Ações

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

As ações a seguir são compatíveis com os recursos de AppFabric produtividade.

Para todas as outras ações de AppFabric API, consulte as Ações de AWS AppFabric API.

Tópicos

- Autorizar
- CreateAppClient
- DeleteAppClient
- GetAppClient
- ListActionableInsights
- ListAppClients
- ListMeetingInsights
- PutFeedback
- Token
- UpdateAppClient

Autorizar

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Autoriza um AppClient.

Tópicos

- Corpo da solicitação

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

Parâmetro	Descrição
app_client_id	O ID do a AppClient ser autorizado.
redirect_uri	O URI para o qual redirecionar os usuários finais após a autorização.
estado	Um valor exclusivo para manter o estado entre a solicitação e o retorno de chamada.

CreateAppClient

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Cria um AppClient.

Tópicos

- Corpo da solicitação
- Elementos de resposta

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

Parâmetro	Descrição
appName	O nome do app. Tipo: sequência Restrições de tamanho: tamanho mínimo 1. Comprimento máximo de 255. Obrigatório: Sim
clientToken	Especifica um identificador exclusivo que diferencia maiúsculas e minúsculas fornecido para garantir a idempotência da solicitaç

Parâmetro	Descrição
	ão. Isso permite que você repita a solicitação com segurança sem executar acidentalmente a mesma operação pela segunda vez. Passar o mesmo valor para uma chamada posterior para uma operação exige que você também passe o mesmo valor para todos os outros parâmetros. Recomendamos que você use um tipo de valor UUID. Se você não fornecer esse valor, AWS gerará um valor aleatório para você. Se você repetir a operação com o mesmo `ClientToken` , mas com parâmetros diferentes, a nova tentativa falhará com um erro `IdempotentParameterMismatch` . Tipo: string Padrão: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obrigatório: não

Parâmetro	Descrição
customerManagedKeyIdentificador	O ARN do chave gerenciada pelo cliente gerado por. AWS Key Management Service A chave é usada para criptografar os dados. Se nenhuma chave for especificada, um Chave gerenciada pela AWS será usado. Um mapa dos pares de chave-valor para a tag ou tags a atribuir ao recurso. Para obter mais informações sobre Chaves pertencentes à AWS chaves gerenciadas pelo cliente, consulte Chaves e AWS chaves do cliente no Guia do AWS Key Management Service desenvolvedor. Tipo: sequência Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.011. Padrão: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obrigatório: não
descrição	Uma descrição para a aplicação. Tipo: string Obrigatório: Sim
iconUrl	O URL do ícone ou logotipo do AppClient. Tipo: sequência Obrigatório: não

Parâmetro	Descrição
redirectUrls	O URI para o qual redirecionar os usuários finais após a autorização. É possível adicionar até 5 redirectUrls. Por exemplo, `https://localhost:8080` . Tipo: Matriz de strings Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens. Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 2.048. Padrão: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` Exigido: Sim
starterUserEmails	Endereços de e-mail iniciais para usuários que têm permissão para receber insights até que sejam verificados. AppClient Tipo: matriz de strings Membros da matriz: número fixo de 1 item. Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 320. Padrão: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Exigido: Sim

Parâmetro	Descrição
tags	Um mapa dos pares de chave-valor para a tag ou tags a atribuir ao recurso. Tipo: matriz de objetos Tag Membros da Matriz: número mínimo de 0 itens. Número máximo de 50 itens. Obrigatório: não

Elementos de resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 201.

Os dados a seguir são retornados no formato JSON pelo serviço.

Parâmetro	Descrição
appClientSummary	Contém um resumo do AppClient. Tipo: objeto AppClientSummary

DeleteAppClient

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Exclui um cliente de aplicação.

Tópicos

- Corpo da solicitação
- Elementos de resposta

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

Parâmetro	Descrição
appClientIdentifier	O Amazon Resource Name (ARN) ou o Universal Unique Identifier (UUID) do a AppClient ser usado para a solicitação. Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.011. Padrão: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Exigido: Sim

Elementos de resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 204 com um corpo HTTP vazio.

GetAppClient

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Retorna informações sobre um AppClient.

Tópicos

- Corpo da solicitação
- Elementos de resposta

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

Parâmetro	Descrição
appClientIdentifier	O Amazon Resource Name (ARN) ou o Universal Unique Identifier (UUID) do a AppClient ser usado para a solicitação.

Parâmetro	Descrição
	Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.011. Padrão: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Exigido: Sim

Elementos de resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Parâmetro	Descrição
appClient	Contém informações sobre um AppClient. Tipo: objeto AppClient

ListActionableInsights

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Lista as mensagens de email, tarefas e outras atualizações acionáveis mais importantes.

Tópicos

- Corpo da solicitação
- Elementos de resposta

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

Parâmetro	Descrição
nextToken	Se o `nextToken` for retornado, haverá mais resultados disponíveis. O valor de `nextToken` é um token de paginação exclusivo para cada página. Faça a chamada novamente usando o token retornado para recuperar a próxima página. Mantenha todos os outros argumentos inalterados. Cada token de paginação expira após 24 horas. Usar um token de paginação expirado retornará um erro HTTP 400. InvalidToken

Elementos de resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 201.

Os dados a seguir são retornados no formato JSON pelo serviço.

Parâmetro	Descrição
ActionableInsightsList	Lista as informações acionáveis, incluindo título, descrição , ações e timestamp de criação. Para ter mais informações, consulte ActionableInsights.
nextToken	Se o `nextToken` for retornado, haverá mais resultados disponíveis. O valor de `nextToken` é um token de paginação exclusivo para cada página. Faça a chamada novamente usando o token retornado para recuperar a próxima página. Mantenha todos os outros argumentos inalterados. Cada token de paginação expira após 24 horas. Usar um token de paginação expirado retornará um erro HTTP 400. InvalidToken Tipo: sequência

ListAppClients

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Retorna uma lista de todos AppClients.

Tópicos

- Corpo da solicitação
- Elementos de resposta

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

Parâmetro	Descrição
maxResults	O número máximo de resultados a serem retornados por chamada. É possível usar `nextToken` para obter páginas de resultados adicionais. Esse é apenas um limite superior. O número real de resultados retornados por chamada pode ser menor que o máximo especificado. Faixa válida: valor mínimo de 1. Valor máximo de 100.
nextToken	Se o `nextToken` for retornado, haverá mais resultados disponíveis. O valor de `nextToken` é um token de paginação exclusivo para cada página. Faça a chamada novamente usando o token retornado para recuperar a próxima página. Mantenha todos os outros argumentos inalterados. Cada token de paginação expira após 24 horas. Usar um token de paginação expirado retornará um erro HTTP 400. InvalidToken

Elementos de resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Parâmetro	Descrição
appClientList	Contém uma lista de AppClient resultados. Tipo: matriz de objetos AppClientSummary
nextToken	Se o `nextToken` for retornado, haverá mais resultados disponíveis. O valor de `nextToken` é um token de paginação exclusivo para cada página. Faça a chamada novamente usando o token retornado para recuperar a próxima página. Mantenha todos os outros argumentos inalterados. Cada token de paginação expira após 24 horas. Usar um token de paginação expirado retornará um erro HTTP 400. InvalidToken Tipo: sequência

ListMeetingInsights

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Lista os eventos acionáveis mais importantes do calendário.

Tópicos

- Corpo da solicitação
- Elementos de resposta

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

Parâmetro	Descrição
nextToken	Se o `nextToken` for retornado, haverá mais resultados disponíveis. O valor de `nextToken` é um token de paginação exclusivo para cada página. Faça a chamada novamente usando o token retornado para recuperar a próxima página.

Parâmetro	Descrição
	Mantenha todos os outros argumentos inalterados. Cada token de paginação expira após 24 horas. Usar um token de paginação expirado retornará um erro HTTP 400. InvalidToken

Elementos de resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 201.

Os dados a seguir são retornados no formato JSON pelo serviço.

Parâmetro	Descrição
MeetingInsightList	Lista as informações acionáveis da reunião. Para ter mais informações, consulte MeetingInsights.
nextToken	Se o `nextToken` for retornado, haverá mais resultados disponíveis. O valor de `nextToken` é um token de paginação exclusivo para cada página. Faça a chamada novamente usando o token retornado para recuperar a próxima página. Mantenha todos os outros argumentos inalterados. Cada token de paginação expira após 24 horas. Usar um token de paginação expirado retornará um erro HTTP 400. InvalidToken Tipo: sequência

PutFeedback

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Permite que os usuários enviem comentários sobre determinada informação ou ação.

Tópicos

- Corpo da solicitação
- Elementos de resposta

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

Parâmetro	Descrição
id	O ID do objeto para o qual o comentário está sendo enviado. Isso pode ser o InsightId ou ActionId o.
feedbackFor	O tipo de informação para o qual o comentário está sendo enviado. Valores possíveis: `ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION`
feedbackRating	Classificação do comentário de 1 a 5. Quanto maior a classificação, melhor.

Elementos de resposta

Se a ação tiver êxito, o serviço enviará de volta uma resposta HTTP 201 com um corpo HTTP vazio.

Token

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Contém informações que permitem AppClients trocar um código de autorização por um token de acesso.

Tópicos

- Corpo da solicitação
- Elementos de resposta

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

Parâmetro	Descrição
Código	O código de autorização recebido do endpoint de autorização. Tipo: sequência Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 2.048. Obrigatório: não
grant_type	O tipo de concessão do token. Deve ser `authorization_code` ou `refresh_token` . Tipo: string Obrigatório: Sim
app_client_id	O ID da AppClient. Tipo: string Padrão: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Exigido: Sim
redirect_uri	A URI de redirecionamento passada para o endpoint de autorização. Tipo: sequência Obrigatório: não
refresh_token	O token de atualização recebido da solicitação inicial do token. Tipo: sequência Restrições de tamanho: tamanho mínimo 1. O tamanho máximo é 4.096.

Parâmetro	Descrição
	Obrigatório: não

Elementos de resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Parâmetro	Descrição
appfabric_user_id	O ID do usuário para o token. Isso é retornado somente para solicitações que usem o tipo de concessão `authorization_code` . Tipo: sequência
expires_in	O número de segundos até a expiração do token. Tipo: longo
refresh_token	O token de atualização a ser usado em uma solicitação subsequente. Tipo: sequência Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 2.048.
token	O token de acesso. Tipo: sequência Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 2.048.
token_type	O tipo de token. Tipo: sequência

UpdateAppClient

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Atualiza um AppClient.

Tópicos

- Corpo da solicitação
- Elementos de resposta

Corpo da solicitação

A solicitação aceita os dados a seguir no formato JSON.

Parâmetro	Descrição
appClientIdentifier	O Amazon Resource Name (ARN) ou o Universal Unique Identifier (UUID) do a AppClient ser usado para a solicitação. Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.011. Padrão: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Exigido: Sim
redirectUrls	O URI para o qual redirecionar os usuários finais após a autorização. É possível adicionar até 5 redirectUrls. Por exemplo, `https://localhost:8080` . Tipo: Matriz de strings Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens. Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 2.048.

Parâmetro	Descrição
	Padrão: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

Elementos de resposta

Se a ação for bem-sucedida, o serviço retornará uma resposta HTTP 200.

Os dados a seguir são retornados no formato JSON pelo serviço.

Parâmetro	Descrição
appClient	Contém informações sobre um AppClient. Tipo: objeto AppClient

Tipos de dados

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

A AppFabric API contém vários tipos de dados que várias ações usam. Esta seção descreve detalhadamente os tipos de dados dos recursos de AppFabric produtividade.

Para todos os outros tipos de dados AppFabric da API, consulte os Tipos de dados AWS AppFabric da API.

> **Important**
>
> A ordem de cada elemento em uma estrutura de tipo de dados não é garantida. As aplicações não devem presumir uma ordem específica.

Tópicos

- ActionableInsights
- AppClient

- AppClientSummary
- MeetingInsights
- VerificationDetails

ActionableInsights

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Contém um resumo das ações importantes e adequadas para um usuário com base em emails, convites de calendário, mensagens e tarefas do portfólio de aplicações. Os usuários podem ver informações proativas dentre todas as aplicações para ajudá-los a orientar melhor seu dia. Essas informações fornecem uma justificativa sobre por que um usuário deve se preocupar com o resumo da informação junto com referências, como links incorporados, a aplicações e artefatos individuais que geraram a informação.

Parâmetro	Descrição
insightId	O id exclusivo da informação gerada.
insightContent	Retorna um resumo da informação e links incorporados aos artefatos usados para gerar a informação. Isso seria um conteúdo HTML contendo links incorporados (tags `<a>`).
insightTitle	O título da informação gerada.
createdAt	Quando a informação foi gerada.
actions	Uma lista de ações recomendadas para a informação gerada. O objeto de ação contém os seguintes parâmetros: • `actionId`: o id exclusivo da ação gerada. • `actionIconUrl` : o URL do ícone da aplicação no qual a ação é sugerida para ser executada. • `actionTitle` : o título da ação gerada.

Parâmetro	Descrição
	• `actionUrl` — O URL exclusivo para o usuário final visualizar e executar a ação no portal AppFabric do usuário. Para executar ações, os aplicativos ISV redirecionarão os usuários para o portal AppFabric do usuário (tela pop-up) usando essa URL. • `actionExecutionStatus` : uma enumeração que indica o status da ação. Os valores possíveis são: `EXECUTED | NOT_EXECUTED`

AppClient

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Contém informações sobre um AppClient.

Parâmetro	Descrição
appName	O nome da aplicação. Tipo: string Obrigatório: Sim
arn	O nome de recurso da Amazon (ARN) do. AppClient Tipo: sequência Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.011. Padrão: `arn:.+` Exigido: Sim

Parâmetro	Descrição
descrição	Uma descrição da aplicação. Tipo: string Obrigatório: Sim
iconUrl	O URL do ícone ou logotipo do AppClient. Tipo: sequência Obrigatório: não
redirectUrls	Os URLs de redirecionamento permitidos para o. AppClient Tipo: Matriz de strings Membros da Matriz: número mínimo de 1 item. Número máximo de 5 itens. Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 2.048. Padrão: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` Exigido: Sim
starterUserEmails	Endereços de e-mail iniciais para usuários que têm permissão para receber insights até que sejam verificados. AppClient Tipo: matriz de strings Membros da matriz: número fixo de 1 item. Restrições de tamanho: tamanho mínimo 0. Tamanho máximo de 320. Padrão: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Exigido: Sim

Parâmetro	Descrição
verificationDetails	Contém o status e o motivo da AppClient verificação. Tipo: objeto VerificationDetails Obrigatório: Sim
customerManagedKeyArn	O nome de recurso da Amazon (ARN) do chave gerenciada pelo cliente gerado por AWS Key Management Service para o. AppClient Tipo: sequência Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.011. Padrão: `arn:.+` Obrigatório: não
appClientId	O ID da AppClient. Destinado a ser usado em fluxos o-auth para o cliente do aplicativo. Tipo: string Padrão: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obrigatório: não

AppClientSummary

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Contém informações sobre um AppClient.

Parâmetro	Descrição
arn	O nome de recurso da Amazon (ARN) do. AppClient Tipo: sequência Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.011. Padrão: `arn:.+` Exigido: Sim
verificationStatus	O status da AppClient verificação. Tipo: sequências Valores Válidos: `pending_verification | verified | rejected` Obrigatório: Sim
appClientId	O ID da AppClient. Destinado a ser usado em fluxos o-auth para o cliente do aplicativo. Tipo: string Padrão: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Obrigatório: não

MeetingInsights

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Contém um resumo das três principais reuniões, juntamente com o objetivo da reunião, artefatos relacionados entre aplicações e atividades de tarefas, emails, mensagens e eventos do calendário.

Parâmetro	Descrição
insightId	O id exclusivo da informação gerada.
insightContent	A descrição da informação, destacando os detalhes em um formato de string. Por exemplo, por que essa informação é importante.
insightTitle	O título da informação gerada.
createdAt	Quando a informação foi gerada.
calendarEvent	O evento ou reunião importante do calendário em que o usuário deve se concentrar. Objeto Calendar Event: • `startTime` : a hora de início do evento. • `endTime`: a hora de término do evento. • `eventUrl`: o URL do evento do calendário na aplicação do ISV.
recursos	A lista contendo os outros recursos relacionados à geração da informação. Objeto de recurso: • `appName`: o nome da aplicação à qual o recurso pertence. • `resourceTitle` : o título do recurso. • `resourceType` : o tipo do recurso. Os valores possíveis são: `EMAIL | EVENT | MESSAGE | TASK` • `resourceUrl` : o URL do recurso na aplicação. • `appIconUrl` : o URL da imagem da aplicação à qual o recurso pertence.

Parâmetro	Descrição
nextToken	O token de paginação para obter o próximo conjunto de informações. É um campo opcional que, se retornado nulo, significa que não há mais informações a serem carregadas.

VerificationDetails

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Contém o status e o motivo da AppClient verificação.

Parâmetro	Descrição
verificationStatus	O status da AppClient verificação. Tipo: sequências Valores Válidos: `pending_verification | verified | rejected` Obrigatório: Sim
statusReason	O motivo do status da AppClient verificação. Tipo: sequência Restrições de tamanho: tamanho mínimo 1. Tamanho máximo de 1.024. Obrigatório: não

Erros comuns

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Esta seção lista os erros comuns às ações da API para os recursos de AWS AppFabric produtividade.

Para ver todos os outros erros AppFabric comuns da API, consulte Solução de problemas "Erros comuns da AWS AppFabric API" na Referência da AWS AppFabric API.

Nome de exceção	Descrição
TokenException	A solicitação do token não é válida. Código de Status HTTP: 400

Processamento de dados

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

AppFabric adota medidas para armazenar o conteúdo do usuário individualmente, em um bucket do Amazon S3 gerenciado por AppFabric e separadamente; o que ajuda a garantir a geração de insights específicos do usuário. Usamos salvaguardas razoáveis para proteger seu conteúdo, o que pode incluir criptografia em repouso e em trânsito. Configuramos nossos sistemas para excluir automaticamente o conteúdo do cliente dentro de 30 dias a partir da ingestão. AppFabric não gera insights usando artefatos de dados aos quais o usuário não tem mais acesso. Por exemplo, quando um usuário desconecta uma fonte de dados (um aplicativo), AppFabric para de coletar dados desse aplicativo e não usa nenhum artefato remanescente dos aplicativos desconectados para gerar insights. AppFabricOs sistemas da são configurados para excluir esses dados em 30 dias.

AppFabric não usa o conteúdo do usuário para treinar ou melhorar os grandes modelos de linguagem subjacentes usados para gerar insights. Para obter mais informações sobre o recurso de IA generativa AppFabric do Amazon Bedrock, consulte as perguntas frequentes do Amazon Bedrock.

Criptografia inativa

AWS AppFabric oferece suporte à criptografia em repouso, um recurso de criptografia do lado do servidor que criptografa de AppFabric forma transparente todos os dados relacionados aos usuários quando eles são mantidos no disco e os descriptografa quando você acessa os dados.

Criptografia em trânsito

AppFabric protege todo o conteúdo em trânsito usando o TLS 1.2 e assina solicitações de API para AWS serviços com o AWS Signature versão 4.

Terminologia e conceitos

Este tópico descreve a terminologia e os conceitos principais AWS AppFabric para ajudar você a começar.

Pacote de aplicativos

Um pacote de AppFabric aplicativos armazena todas as autorizações e ingestões do seu AppFabric aplicativo (consulte a definição de ingestão a seguir). Você pode criar um pacote de aplicativos Conta da AWS por cada. Região da AWS

AppClient (também cliente de aplicativo e cliente de aplicativo)

Um OAuth AppClient para o aplicativo destinatário dos dados. Cada aplicativo destinatário de dados precisa se registrar e AppClient acessar AppFabric os dados. Um usuário desenvolvedor precisa de uma AWS conta para se registrar AppClient. Cada AWS conta só pode registrar uma AppClient. AppFabric venderá tokens de acesso com base em. AppClient AppClient conterá informações sobre o aplicativo destinatário de dados que acessará AppFabric os dados por meio dele AppClient.

Autorização do aplicativo

Uma autorização de aplicativo concede AppFabric permissão para se conectar e interagir com seus aplicativos. Permite a ingestão de logs de auditoria de seus aplicativos, com credenciais OAuth (Autorização Aberta - um padrão aberto para delegação de acesso para conceder acesso aos aplicativos) ou token de acesso pessoal (personal access token, PAT). Você pode configurar várias autorizações de aplicativos (até 50) por pacote de aplicativos. Isso permite AppFabric ingerir registros de auditoria de vários inquilinos de aplicativos, repetindo a etapa de criação da autorização do aplicativo conforme necessário para cada inquilino do aplicativo. As credenciais que são compartilhadas são criptografadas com uma Chave pertencente à AWS chave gerenciada pelo cliente do AWS Key Management Service (AWS KMS) e são armazenadas em AppFabric.

Ingestão

Uma AppFabric ingestão usa uma autorização de aplicativo para extrair registros de auditoria de um aplicativo por meio das APIs públicas do aplicativo. Em seguida, ele entrega os logs de auditoria para um ou mais (até cinco) destinos.

ID de cliente

Quando você cria uma autorização de aplicativo para se conectar a um aplicativo que usa o fluxo OAuth, AppFabric pode solicitar o ID e o segredo do cliente. A ID do cliente e o segredo do cliente podem ser encontrados no aplicativo de autenticação do seu aplicativo. Para obter instruções sobre onde encontrar a ID do cliente em um determinado aplicativo de autenticação, consulte Aplicativos compatíveis. O ID do cliente e o segredo do cliente que são compartilhados são criptografados com uma chave Chave pertencente à AWS ou uma AWS KMS chave gerenciada pelo cliente e armazenados em AppFabric.

Segredo do cliente

Quando você cria uma autorização de aplicativo para se conectar a um aplicativo que usa o fluxo OAuth, AppFabric pode solicitar o ID e o segredo do cliente. A ID do cliente e o segredo do cliente podem ser encontrados no aplicativo de autenticação do seu aplicativo. Para obter instruções sobre onde encontrar o segredo do cliente em um determinado aplicativo de autenticação, consulte Aplicativos compatíveis. O ID do cliente e o segredo do cliente que são compartilhados são criptografados com uma chave Chave pertencente à AWS ou uma AWS KMS chave gerenciada pelo cliente e armazenados em AppFabric.

Destino de ingestão

Um destino de ingestão define onde os logs de auditoria extraídos de uma ingestão devem ser armazenados. Cada ingestão pode entregar registros de auditoria para um ou mais destinos (até cinco), que são um bucket do Amazon Simple Storage Service (Amazon S3) ou um Amazon Data Firehose no seu. Conta da AWS Para cada destino, você pode definir se deseja que os logs estejam em formato raw ou normalizados em um esquema Open Cybersecurity Schema Framework (OCSF). Ao selecionar o esquema OCSF, você pode definir o formato dos logs (JSON ou Apache Parquet). O formato Apache Parquet só pode ser usado se o Amazon S3 for selecionado como destino.

Aplicações destinatárias de dados

Aplicativos que ligarão AppFabric para obter informações geradas a partir de AppFabric.

OAuth

O OAuth é um protocolo aberto que permite a autorização segura em um método simples e padrão a partir de aplicativos da web, móveis e desktop. AppFabric usa o OAuth para criar algumas autorizações de aplicativos.

Open Cybersecurity Schema Framework (OCSF)

O Open Cybersecurity Schema Framework (OCSF) é um projeto de código aberto que fornece uma estrutura extensível para o desenvolvimento de esquemas, junto com um esquema de segurança central independente do fornecedor. Fornecedores e outros produtores de dados podem adotar e estender o esquema para seus domínios específicos. O objetivo é fornecer um padrão aberto, adotado em qualquer ambiente, aplicativo ou solução, complementando os padrões e processos de segurança existentes. AppFabric estendeu esse esquema para criar uma estrutura de eventos centrada em software como serviço (SaaS), para a qual todos os registros de auditoria de aplicativos SaaS suportados serão normalizados. AppFabric Para ter mais informações, consulte Open Cybersecurity Schema Framework.

Token de acesso pessoal (PAT)

Um token de acesso pessoal (personal access token, PAT) é uma sequência de caracteres que pode ser usada para acessar um sistema de computador em vez da senha usual. Quando você cria uma autorização de aplicativo para se conectar a um aplicativo que usa o fluxo PAT, AppFabric pode solicitar um PAT. O PAT pode ser encontrado no aplicativo de autenticação do seu aplicativo. Para obter instruções sobre onde encontrar o PAT em um aplicativo de autenticação específico, consulte Aplicativos compatíveis. Os tokens da conta de serviço que são compartilhados são criptografados com uma chave gerenciada pelo cliente Chave pertencente à AWS ou por uma AWS KMS chave gerenciada pelo cliente e armazenados em AppFabric.

Token de contas de serviço

Quando você cria uma autorização de AppFabric aplicativo para se conectar a um aplicativo, alguns aplicativos exigem a criação de uma conta de serviço para autenticação do aplicativo. AppFabric pode solicitar o token da conta de serviço como parte do processo de autorização do aplicativo. Para obter instruções sobre onde encontrar o token da conta de serviço em um determinado aplicativo de autenticação, consulte Aplicativos compatíveis. Os tokens da conta de serviço que são compartilhados são criptografados com uma chave gerenciada pelo cliente Chave pertencente à AWS ou por uma AWS KMS chave gerenciada pelo cliente e armazenados em AppFabric.

ID de locatário

Quando você cria uma autorização de aplicativo, AppFabric pode solicitar o ID do inquilino e o nome do locatário do seu aplicativo. A ID do locatário é um identificador exclusivo para o locatário do seu aplicativo. Cada aplicativo pode ter termos diferentes para um locatário, como ID do espaço de trabalho para Slack ou ID do domínio para Asana. Para obter instruções sobre onde encontrar a ID do locatário em um aplicativo específico, consulte Aplicativos compatíveis.

Nome do locatário

Quando você cria uma autorização de aplicativo, AppFabric pode solicitar o ID do inquilino e o nome do locatário do seu aplicativo. O nome do locatário é um nome exclusivo que você dá à ID do locatário, para ser usado em um pacote de aplicativos. Esse valor é usado para rotular a autorização do aplicativo e qualquer ingestão relacionada.

Segurança em AWS AppFabric

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que é executada Serviços da AWS no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade aplicáveis AWS AppFabric, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS service (Serviço da AWS) que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AppFabric. Os tópicos a seguir mostram como configurar para atender AppFabric aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros Serviços da AWS que o ajudem a monitorar e proteger seus AppFabric recursos.

Tópicos

- Proteção de dados em AWS AppFabric
- Gerenciamento de identidade e acesso para AWS AppFabric
- Validação de conformidade para AWS AppFabric
- Práticas recomendadas de segurança para AWS AppFabric
- Resiliência em AWS AppFabric
- Segurança da infraestrutura em AWS AppFabric
- Análise de configuração e vulnerabilidade em AWS AppFabric

Proteção de dados em AWS AppFabric

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS AppFabric. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AppFabric ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você

fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

> **Note**
>
> Para obter mais informações sobre a proteção de dados no que se refere AppFabric à segurança, consulteProcessamento de dados.

Criptografia em repouso

AWS AppFabric oferece suporte à criptografia em repouso, um recurso de criptografia do lado do servidor que criptografa de AppFabric forma transparente todos os dados relacionados aos pacotes de aplicativos quando eles são mantidos no disco e os descriptografa quando você acessa os dados. Por padrão, AppFabric criptografa seus dados usando um Chave pertencente à AWS from AWS Key Management Service (AWS KMS). Você também pode optar por criptografar seus dados usando sua própria chave gerenciada pelo cliente em. AWS KMS

Quando você exclui um pacote de aplicativos, todos os seus metadados são excluídos permanentemente.

Criptografia em trânsito

Ao configurar um pacote de aplicativos, você pode escolher uma chave gerenciada pelo cliente Chave pertencente à AWS ou uma chave gerenciada pelo cliente. Ao coletar e normalizar os dados para a ingestão de um log de auditoria, AppFabric armazena dados temporariamente em um bucket intermediário do Amazon Simple Storage Service (Amazon S3) e os criptografa usando essa chave. Esse bucket intermediário é excluído após 30 dias em cumprimento a uma política de ciclo de vida de buckets.

AppFabric protege todos os dados em trânsito usando o TLS 1.2 e assina solicitações de API Serviços da AWS com o AWS Signature V4.

Gerenciamento de chaves

AppFabric suporta a criptografia de dados com uma chave gerenciada pelo cliente Chave pertencente à AWS ou com uma chave gerenciada pelo cliente. Recomendamos que você use uma chave gerenciada pelo cliente, pois ela dá controle total sobre seus dados criptografados. Quando

você escolhe uma chave gerenciada pelo cliente, AppFabric anexa uma política de recursos à chave gerenciada pelo cliente que lhe concede acesso à chave gerenciada pelo cliente.

Chave gerenciada pelo cliente

Para criar uma chave gerenciada pelo cliente, siga as etapas para Criar chaves KMS de criptografia simétrica no Guia do desenvolvedor do AWS KMS .

Política de chave

As políticas de chave controlam o acesso à chave gerenciada pelo cliente. Cada chave gerenciada pelo cliente deve ter exatamente uma política de chaves, que contém declarações que determinam quem pode usar a chave e como pode usá-la. Ao criar a chave gerenciada pelo cliente, é possível especificar uma política de chaves. Para obter mais informações sobre como criar uma política de chave, consulte Criar uma política de chave no Guia do desenvolvedor do AWS KMS .

Para usar uma chave gerenciada pelo cliente com AppFabric, o usuário ou a função AWS Identity and Access Management (IAM) que está criando seus AppFabric recursos deve ter permissão para usar sua chave gerenciada pelo cliente. Recomendamos que você crie uma chave que use somente com AppFabric e adicione seus AppFabric usuários como usuários da chave. Essa abordagem limita o escopo do acesso aos seus dados. As permissões de que seus usuários precisam são as seguintes:

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Decrypt`

O AWS KMS console orienta você na criação de uma chave com a política de chaves apropriada. Para obter mais informações sobre políticas de chave, consulte Políticas de chave no AWS KMS no Guia do desenvolvedor do AWS KMS .

Abaixo, um exemplo de uma política de chave que permite:

- O controle Usuário raiz da conta da AWS total da chave.
- Usuários autorizados a usar AppFabric para usar sua chave gerenciada pelo cliente com AppFabric.
- Uma política de chave para a configuração de um pacote de aplicativos em `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"
                }
            }
        }
    ]
```

```
}
```

Como AppFabric usa subsídios em AWS KMS

AppFabric exige uma concessão para usar sua chave gerenciada pelo cliente. Para obter mais informações, consulte Concessões no AWS KMS no Guia do desenvolvedor AWS KMS .

Quando você cria um pacote de aplicativos, AppFabric cria uma concessão em seu nome enviando uma `CreateGrant` solicitação para AWS KMS. As concessões AWS KMS são usadas para dar AppFabric acesso a uma AWS KMS chave na conta do cliente. AppFabric exige que a concessão use sua chave gerenciada pelo cliente para as seguintes operações internas:

- Envie `GenerateDataKey` solicitações AWS KMS para gerar chaves de dados criptografadas pela chave gerenciada pelo cliente.
- Envie `Decrypt` solicitações AWS KMS para descriptografar as chaves de dados criptografadas para que elas possam ser usadas para criptografar seus dados e descriptografar tokens de acesso ao aplicativo em trânsito.
- Envie `Encrypt` solicitações para AWS KMS criptografar tokens de acesso ao aplicativo em trânsito.

Veja a seguir um exemplo de concessão.

```
{
  "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"
```

```
    }
  }
},
```

Quando você exclui um pacote de aplicativos, AppFabric retira as concessões emitidas em sua chave gerenciada pelo cliente.

Monitorando suas chaves de criptografia para AppFabric

Ao usar chaves gerenciadas pelo AWS KMS cliente com AppFabric, você pode usar AWS CloudTrail registros para rastrear solicitações AppFabric enviadas para AWS KMS o.

Veja a seguir um exemplo de um CloudTrail evento registrado quando AppFabric usado `CreateGrant` para sua chave gerenciada pelo 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"
```

```
    }
}
```

Gerenciamento de identidade e acesso para AWS AppFabric

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AppFabric os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

- Público
- Autenticando com identidades
- Gerenciando acesso usando políticas
- Como AWS AppFabric funciona com o IAM
- Exemplos de políticas baseadas em identidade para o AWS AppFabric
- Usar funções vinculadas ao serviço do AppFabric
- AWS políticas gerenciadas para AWS AppFabric
- Solução de problemas AWS AppFabric de identidade e acesso

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AppFabric.

Usuário do serviço — Se você usar o AppFabric serviço para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais AppFabric recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no AppFabric, consulteSolução de problemas AWS AppFabric de identidade e acesso.

Administrador de serviços — Se você é responsável pelos AppFabric recursos da sua empresa, provavelmente tem acesso total AppFabric a. É seu trabalho determinar quais AppFabric recursos

e recursos seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com AppFabric, consulteComo AWS AppFabric funciona com o IAM.

Administrador do IAM — Se você for administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso AppFabric. Para ver exemplos de políticas AppFabric baseadas em identidade que você pode usar no IAM, consulte. Exemplos de políticas baseadas em identidade para o AWS AppFabric

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação Multifator no Guia do Usuário do AWS IAM Identity Center . Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do Usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no Manual do Usuário do AWS IAM Identity Center .

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários

de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para identidades do IAM no Guia do Usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no Manual do Usuário do AWS Organizations .
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do Usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como AWS AppFabric funciona com o IAM

Antes de usar o IAM para gerenciar o acesso AppFabric, saiba com quais recursos do IAM estão disponíveis para uso AppFabric.

Recursos do IAM que você pode usar com AWS AppFabric

Atributo do IAM	AppFabric apoio
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim

Atributo do IAM	AppFabric apoio
Atributos de políticas	Sim
Chaves de condição de políticas	Não
ACLs	Não
ABAC (tags em políticas)	Sim
Credenciais temporárias	Não
Permissões de entidade principal	Sim
Perfis de serviço	Não
Funções vinculadas ao serviço	Sim

Para ter uma visão de alto nível de como AppFabric e outros Serviços da AWS funcionam com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Políticas baseadas em identidade para AppFabric

Suporta políticas baseadas em identidade	Sim

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criando políticas do IAM no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte Referência de elementos da política JSON do IAM no Guia do Usuário do IAM.

Exemplos de políticas baseadas em identidade para AppFabric

Para ver exemplos de políticas AppFabric baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS AppFabric

Políticas baseadas em recursos dentro AppFabric

Oferece compatibilidade com políticas baseadas em recursos	Não

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Ações políticas para AppFabric

Oferece compatibilidade com ações de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de AppFabric ações, consulte Ações definidas por AWS AppFabric na Referência de Autorização de Serviço.

As ações de política AppFabric usam o seguinte prefixo antes da ação:

```
appfabric
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "appfabric:action1",
      "appfabric:action2"
         ]
```

É possível especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `List`, inclua a ação a seguir:

```
"Action": "appfabric:List*"
```

Para ver exemplos de políticas AppFabric baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS AppFabric

Recursos políticos para AppFabric

Oferece compatibilidade com recursos de políticas	Sim

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de AppFabric recursos e seus ARNs, consulte Tipos de recursos definidos por AWS AppFabric na Referência de Autorização de Serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações definidas por. AWS AppFabric

Para ver exemplos de políticas AppFabric baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS AppFabric

Chaves de condição de política para AppFabric

Suporta chaves de condição de política específicas de serviço	Não

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar

vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos da política do IAM: variáveis e tags no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Para ver uma lista de chaves de AppFabric condição, consulte Chaves de condição AWS AppFabric na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas por AWS AppFabric.

Para ver exemplos de políticas AppFabric baseadas em identidade, consulte. Exemplos de políticas baseadas em identidade para o AWS AppFabric

ACLs em AppFabric

Oferece compatibilidade com ACLs	Não

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

ABAC com AppFabric

Oferece compatibilidade com ABAC (tags em políticas)	Sim

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir

operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte O que é ABAC? no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte Utilizar controle de acesso baseado em atributos (ABAC) no Guia do usuário do IAM.

Usando credenciais temporárias com AppFabric

Oferece compatibilidade com credenciais temporárias	Não

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “Trabalhe com o IAM” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte Alternar para um perfil (console) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte Credenciais de segurança temporárias no IAM.

Permissões principais entre serviços para AppFabric

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.

Funções de serviço para AppFabric

Oferece suporte a perfis de serviço	Não

Um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper AppFabric a funcionalidade. Edite as funções de serviço somente quando AppFabric fornecer orientação para fazer isso.

Funções vinculadas a serviços para AppFabric

Oferece suporte a perfis vinculados ao serviço	Sim

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções AppFabric vinculadas a serviços, consulte. Usar funções vinculadas ao serviço do AppFabric

Exemplos de políticas baseadas em identidade para o AWS AppFabric

Por padrão, usuários e funções não têm permissão para criar ou modificar AppFabric recursos. Eles também não podem realizar tarefas usando a AWS API AWS Management Console, AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte Criação de políticas do IAM no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos por AppFabric, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte Ações, recursos e chaves de condição AWS AppFabric na Referência de Autorização de Serviço.

Sumário

- Melhores práticas de política
- Usar o console do AppFabric
- AppFabric para exemplos de políticas de segurança do IAM
  - Permite acesso aos pacotes de aplicativos
  - Restringir o acesso a pacotes de aplicativos
  - Restringir a exclusão ou interrupção de ingestões
- AppFabric exemplos de políticas de IAM para produtividade
  - Permitir acesso somente de leitura a recursos de produtividade
  - Permitir acesso total a recursos de produtividade
  - Permitir acesso para criar AppClients
  - Permita o acesso para obter detalhes de AppClients

  - Permitir acesso à lista AppClients
  - Permitir acesso à atualização AppClients
  - Permitir acesso para excluir AppClients
  - Permitir acesso para autorizar aplicações
- Exemplos de outras políticas do IAM
  - Permitir que usuários visualizem suas próprias permissões

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir AppFabric recursos em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do Usuário do IAM.
- Aplique permissões de privilégio mínimo –- ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do Usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso –- você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: Condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais –- o IAM Access Analyzer valida as políticas novas e existentes para que elas

sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas Recomendadas de Segurança no IAM no Guia do Usuário do IAM.

Usar o console do AppFabric

Anexe a política `AWSAppFabricReadOnlyAccess` AWS gerenciada às suas identidades do IAM para conceder a elas permissão somente de leitura para o AppFabric serviço, incluindo o AppFabric console no. AWS Management Console Ou você pode anexar a política `AWSAppFabricFullAccess` AWS gerenciada às suas identidades do IAM para conceder a elas permissão administrativa total para o AppFabric serviço. Para ter mais informações, consulte AWS políticas gerenciadas para AWS AppFabric.

AppFabric para exemplos de políticas de segurança do IAM

Os exemplos de políticas a seguir se aplicam AppFabric aos recursos de segurança.

Permite acesso aos pacotes de aplicativos

O exemplo de política a seguir concede acesso aos pacotes de aplicativos no AppFabric serviço.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
```

```
    ],
    "Version": "2012-10-17"
}
```

Restringir o acesso a pacotes de aplicativos

O exemplo de política a seguir restringe o acesso aos pacotes de aplicativos no AppFabric serviço.

```
{
    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Restringir a exclusão ou interrupção de ingestões

O exemplo de política a seguir restringe a exclusão ou interrupção de ingestões no serviço. 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 exemplos de políticas de IAM para produtividade

O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Os exemplos de políticas a seguir se aplicam AppFabric aos recursos de produtividade.

Permitir acesso somente de leitura a recursos de produtividade

O exemplo de política a seguir concede acesso somente de leitura aos recursos AppFabric de produtividade.

> **Important**
>
> Talvez você veja um erro de ação inválida ao adicionar essa política no editor de políticas JSON do console do IAM. Isso ocorre porque os recursos AppFabric de produtividade estão atualmente em versão prévia. Você deve ignorar o erro e prosseguir com a criação da política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
                "appfabric:ListActionableInsights",
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights"
            ],
            "Resource": "*"
        }
```

```
    ],
    "Version": "2012-10-17"
}
```

Permitir acesso total a recursos de produtividade

O exemplo de política a seguir concede acesso total AppFabric aos recursos de produtividade.

> **Important**
>
> Talvez você veja um erro de ação inválida ao adicionar essa política no editor de políticas JSON do console do IAM. Isso ocorre porque os recursos AppFabric de produtividade estão atualmente em versão prévia. Você deve ignorar o erro e prosseguir com a criação da 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"
}
```

Permitir acesso para criar AppClients

O exemplo de política a seguir concede acesso para criar AppClients. Para obter mais informações, consulte Criar um AppFabric para produtividade AppClient.

> **Important**
>
> Talvez você veja um erro de ação inválida ao adicionar essa política no editor de políticas JSON do console do IAM. Isso ocorre porque os recursos AppFabric de produtividade estão atualmente em versão prévia. Você deve ignorar o erro e prosseguir com a criação da política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Permita o acesso para obter detalhes de AppClients

O exemplo de política a seguir concede acesso para obter detalhes de AppClients. Para obter mais informações, consulte Obter detalhes de um AppClient.

> **Important**
>
> Talvez você veja um erro de ação inválida ao adicionar essa política no editor de políticas JSON do console do IAM. Isso ocorre porque os recursos AppFabric de produtividade estão atualmente em versão prévia. Você deve ignorar o erro e prosseguir com a criação da política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "appfabric:GetAppClient",
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Permitir acesso à lista AppClients

O exemplo de política a seguir concede acesso à lista AppClients. Para obter mais informações, consulte Obter detalhes de um AppClient.

> **Important**
>
> Talvez você veja um erro de ação inválida ao adicionar essa política no editor de políticas JSON do console do IAM. Isso ocorre porque os recursos AppFabric de produtividade estão atualmente em versão prévia. Você deve ignorar o erro e prosseguir com a criação da política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:ListAppClients"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Permitir acesso à atualização AppClients

O exemplo de política a seguir concede acesso à atualização AppClients. Para obter mais informações, consulte Atualizar um AppClient.

> **Important**
>
> Talvez você veja um erro de ação inválida ao adicionar essa política no editor de políticas JSON do console do IAM. Isso ocorre porque os recursos AppFabric de produtividade estão atualmente em versão prévia. Você deve ignorar o erro e prosseguir com a criação da política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:UpdateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Permitir acesso para excluir AppClients

O exemplo de política a seguir concede acesso à exclusão AppClients. Para obter mais informações, consulte Atualizar um AppClient.

> **Important**
>
> Talvez você veja um erro de ação inválida ao adicionar essa política no editor de políticas JSON do console do IAM. Isso ocorre porque os recursos AppFabric de produtividade estão atualmente em versão prévia. Você deve ignorar o erro e prosseguir com a criação da política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "appfabric:DeleteAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Permitir acesso para autorizar aplicações

O exemplo de política a seguir concede acesso para autorizar aplicações usando a API Token. Para obter mais informações, consulte Autenticar e autorizar sua aplicação.

> **Important**
>
> Talvez você veja um erro de ação inválida ao adicionar essa política no editor de políticas JSON do console do IAM. Isso ocorre porque os recursos AppFabric de produtividade estão atualmente em versão prévia. Você deve ignorar o erro e prosseguir com a criação da política.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:Token"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Exemplos de outras políticas do IAM

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui

permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou 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": "*"
        }
    ]
}
```

Usar funções vinculadas ao serviço do AppFabric

AWS AppFabric usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente

a. AppFabric As funções vinculadas ao serviço são predefinidas AppFabric e incluem todas as permissões que o serviço exige para ligar para outras pessoas Serviços da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração AppFabric porque você não precisa adicionar manualmente as permissões necessárias. AppFabric define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AppFabric pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Um perfil vinculado a serviço poderá ser excluído somente após a exclusão dos recursos relacionados. Isso protege seus AppFabric recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com perfis vinculados ao serviço, consulte serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Perfis vinculados aos serviços. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculada ao serviço AppFabric

AppFabric usa a função vinculada ao serviço chamada `AWSServiceRoleForAppFabric` — Permite AppFabric colocar dados em um recurso de destino de ingestão, como um bucket do Amazon S3 ou um stream de entrega do Amazon Data Firehose. Também permite AppFabric colocar dados CloudWatch métricos no `AWS/AppFabric` namespace.

A função vinculada ao serviço `AWSServiceRoleForAppFabric` confia nos seguintes serviços para aceitar a função:

- `appfabric.amazonaws.com`

A política de permissões de função nomeada `AWSAppFabricServiceRolePolicy` AppFabric permite concluir as seguintes ações nos recursos especificados:

- Ação: `cloudwatch:PutMetricData` no namespace do `AWS/AppFabric`. Essa ação concede permissão AppFabric para colocar dados métricos no CloudWatch `AWS/AppFabric` namespace da Amazon. Para obter mais informações sobre as AppFabric métricas disponíveis em CloudWatch, consulteMonitoramento AWS AppFabric com a Amazon CloudWatch.
- Ação: `s3:PutObject` em um bucket do Amazon S3. Essa ação concede permissão AppFabric para colocar dados ingeridos em um bucket do Amazon S3 que você especificar.

- Ação: `firehose:PutRecordBatch` em um stream de entrega do Amazon Data Firehose. Essa ação concede permissão AppFabric para colocar dados ingeridos em um stream de entrega do Amazon Data Firehose que você especificar.

Para obter mais informações, consulte políticas AWS gerenciadas para AppFabric.

Você deve configurar permissões para permitir que seus usuários, grupos ou perfis criem, editem ou excluam um perfil vinculado ao serviço. Para ter mais informações, consulte Service-linked role permissions (Permissões de nível vinculado a serviços) no Guia do usuário do IAM.

Criação de uma função vinculada ao serviço para AppFabric

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria um pacote de AppFabric aplicativos na AWS Management Console, na ou na AWS API AWS CLI, AppFabric cria a função vinculada ao serviço para você.

Editando uma função vinculada ao serviço para AppFabric

AppFabric não permite que você edite a função `AWSServiceRoleForAppFabric` vinculada ao serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você poderá editar a descrição do perfil usando o IAM. Para ter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para AppFabric

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve excluir todos os seus pacotes de AppFabric aplicativos antes de excluir a função vinculada ao serviço.

Limpar um perfil vinculado ao serviço

Antes de usar o IAM para excluir um perfil vinculado ao serviço, você deverá excluir qualquer recurso usado pelo perfil. Os pacotes de aplicativos que você cria AppFabric são usados pela função. Para ter mais informações, consulte Excluir AWS AppFabric para recursos de segurança.

> **Note**
>
> Se o AppFabric serviço estiver usando a função quando você tentar excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSServiceRoleForAppFabric` vinculada ao serviço. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões suportadas para funções vinculadas a AppFabric serviços

AppFabric suporta o uso de funções vinculadas ao serviço em todos os lugares em Regiões da AWS que o serviço está disponível. Para obter mais informações, consulte AppFabric endpoints e cotas no. Referência geral da AWS

AWS políticas gerenciadas para AWS AppFabric

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

Serviços da AWS manter e atualizar políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada fornece acesso somente de leitura a todos Serviços da AWS os recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.

AWS política gerenciada: AWSAppFabricReadOnlyAccess

É possível anexar a política `AWSAppFabricReadOnlyAccess` a suas identidades do IAM. Essa política concede permissões somente de leitura ao AppFabric serviço.

> **Note**
>
> A `AWSAppFabricReadOnlyAccess` política não concede acesso somente de leitura aos recursos AppFabric de produtividade.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `appfabric` – Concede permissão para obter um pacote de aplicativos, listar pacotes de aplicativos, obter uma autorização de aplicativo, listar autorizações de aplicativos, obter uma ingestão, listar ingestões, obter um destino de ingestão, listar destinos de ingestão e listar tags 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 gerenciada: AWSAppFabricFullAccess

É possível anexar a política `AWSAppFabricFullAccess` a suas identidades do IAM. Essa política concede permissões administrativas ao AppFabric serviço.

> **Important**
>
> A `AWSAppFabricFullAccess` política não concede acesso aos recursos AppFabric de produtividade porque eles estão atualmente em versão prévia. Para obter mais informações sobre como conceder acesso aos recursos AppFabric de produtividade, consulteAppFabric exemplos de políticas de IAM para produtividade.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `appfabric`— Concede permissão administrativa total para AppFabric.
- `kms` – Concede permissão para listar aliases.
- `s3` – Concede permissão para listar todos os seus buckets do Amazon S3 e obter a localização do bucket.
- `firehose`— Concede permissão para listar os fluxos de entrega do Amazon Data Firehose e descrever os fluxos de entrega.
- `iam`— Concede permissão para criar a função `AWSServiceRoleForAppFabric` vinculada ao serviço para. AppFabric Para ter mais informações, consulte Usar funções vinculadas ao serviço do 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 gerenciada: AWSAppFabricServiceRolePolicy

Não é possível anexar a política `AWSAppFabricServiceRolePolicy` às suas entidades do IAM. Essa política está vinculada a uma função vinculada ao serviço que permite AppFabric realizar ações em seu nome. Para obter mais informações, consulte Usar funções vinculadas ao serviço do AppFabric.

Detalhes de permissão

Esta política inclui as seguintes permissões:

- `cloudwatch`— Concede permissão AppFabric para colocar dados métricos no CloudWatch `AWS/AppFabric` namespace da Amazon. Para obter mais informações sobre as AppFabric métricas disponíveis em CloudWatch, consulteMonitoramento AWS AppFabric com a Amazon CloudWatch.
- `s3`— Concede permissão AppFabric para colocar dados ingeridos em um bucket do Amazon S3 que você especificar.
- `firehose`— Concede permissão AppFabric para colocar dados ingeridos em um stream de entrega do Amazon Data Firehose que você especificar.

```
{
    "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 atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AppFabric desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AppFabric documento.

Alteração	Descrição	Data
AWSAppFabricReadOnlyAccess – Nova política	AppFabric adicionou uma nova política para conceder permissões somente de leitura ao AppFabric serviço.	27 de junho de 2023
AWSAppFabricFullAccess – Nova política	AppFabric adicionou uma nova política para conceder permissões administrativas ao AppFabric serviço.	27 de junho de 2023
AWSAppFabricServiceRolePolicy – Nova política	AppFabric adicionou uma nova política para a função `AWSServiceRoleForAppFabric` vinculada ao serviço.	27 de junho de 2023

Alteração	Descrição	Data
AppFabric começou a rastrear as alterações	AppFabric começou a rastrear as mudanças em suas políticas AWS gerenciadas.	27 de junho de 2023

Solução de problemas AWS AppFabric de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AppFabric um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em AppFabric
- Não tenho autorização para executar iam:PassRole
- Quero permitir que pessoas fora da minha Conta da AWS acessem meus AppFabric recursos

Não estou autorizado a realizar uma ação em AppFabric

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `appfabric:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 appfabric:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `appfabric:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não tenho autorização para executar iam:PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você transfira uma função para AppFabric o.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no AppFabric. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS acessem meus AppFabric recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AppFabric compatível com esses recursos, consulteComo AWS AppFabric funciona com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.

- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Validação de conformidade para AWS AppFabric

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).

- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Práticas recomendadas de segurança para AWS AppFabric

AWS AppFabric fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

Monitorar o aplicativo sem acesso de administrador

Com a permissão somente leitura AWS Identity and Access Management (IAM), qualquer pessoa pode se integrar à AppFabric Amazon QuickSight e a outras ferramentas de gerenciamento de eventos e informações de segurança (SIEM), como. Splunk Para monitorar a segurança do aplicativo, os dados são entregues em um bucket do Amazon Simple Storage Service (Amazon S3) ou em um stream de entrega do Amazon Data Firehose.

Monitor de AppFabric eventos

Você pode monitorar AppFabric usando as CloudWatch métricas da Amazon. CloudWatch coleta dados a AppFabric cada minuto e os processa em métricas. Você pode definir alarmes que enviam

notificações quando as métricas correspondem aos limites especificados. Para ter mais informações, consulte Monitoramento AWS AppFabric com a Amazon CloudWatch.

Resiliência em AWS AppFabric

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Segurança da infraestrutura em AWS AppFabric

Como serviço gerenciado, AWS AppFabric é protegido pelos procedimentos AWS globais de segurança de rede descritos no whitepaper Amazon Web Services: Visão geral dos processos de segurança.

Você usa chamadas de API AWS publicadas para acessar AppFabric pela rede. Os clientes devem ser compatíveis com o TLS 1.0 ou posterior. Recomendamos usar o TLS 1.2 ou posterior. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Análise de configuração e vulnerabilidade em AWS AppFabric

A configuração e os controles de TI são uma responsabilidade compartilhada entre você AWS e você, nosso cliente. Para obter mais informações, consulte o modelo de responsabilidade AWS compartilhada.

Monitoramento AWS AppFabric

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho de AWS AppFabric suas outras AWS soluções. AWS fornece as seguintes ferramentas de monitoramento para observar AppFabric, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- O Amazon CloudWatch Logs permite que você monitore, armazene e acesse seus arquivos de log a partir de instâncias do Amazon EC2 e de outras fontes. AWS CloudTrail CloudWatch Os registros podem monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o Guia do usuário do Amazon CloudWatch Logs.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por você ou em seu nome Conta da AWS e entrega os arquivos de log em um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para mais informações, consulte o Guia do usuário do AWS CloudTrail.

Monitoramento AWS AppFabric com a Amazon CloudWatch

Você pode monitorar AWS AppFabric o uso CloudWatch, que coleta dados brutos e os processa em métricas legíveis e quase em tempo real. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como o aplicativo web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

O AppFabric serviço relata as seguintes métricas no `AWS/AppFabric` namespace.

Métrica	Descrição
AppFabric Status de autorização do aplicativo	O status da autorização do aplicativo (1para conectado; `0` para qualquer outro).
AppFabric Latência de entrega de dados	O tempo gasto (em segundos) AppFabric para coletar registros de auditoria do aplicativo SaaS e entregá-los ao destino configurado (Amazon S3 ou Amazon Data Firehose).
Status do destino de ingestão	O status do destino da ingestão (1para ativo; `0` para qualquer outro).
Atraso geral de dados	A diferença de tempo (em segundos) entre o momento em que os eventos aconteceram no aplicativo SaaS e o momento em que os registros de auditoria correspondentes foram entregues ao destino configurado (Amazon S3 ou Amazon Data Firehose) pela. AppFabric
Volume de dados ingeridos	O tamanho dos dados que são entregues ao Amazon Simple Storage Service (Amazon S3) ou ao Amazon Data Firehose.

A dimensão a seguir é compatível com AppFabric métricas.

Dimensão	Descrição
ARN de destino de ingestão	O nome do recurso da Amazon (ARN) do destino de ingestão.

Registrando chamadas de AWS AppFabric API usando AWS CloudTrail

AWS AppFabric é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um AWS service (Serviço da AWS) usuário AppFabric.

CloudTrail captura todas as chamadas de API AppFabric como eventos. As chamadas capturadas incluem chamadas do AppFabric console e chamadas de código para as operações AppFabric da API. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para. AppFabric Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita AppFabric, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para obter mais informações sobre CloudTrail, consulte o Guia AWS CloudTrail do usuário.

AppFabric informações em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre em AppFabric, essa atividade é registrada em um CloudTrail evento junto com outros AWS service (Serviço da AWS) eventos no histórico de eventos. Você pode exibir, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualização de CloudTrail eventos com histórico de eventos no Guia AWS CloudTrail do usuário.

Para um registro contínuo dos eventos em sua Conta da AWS, incluindo eventos para AppFabric, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros. Para obter mais informações, consulte os seguintes tópicos no Guia do usuário do AWS CloudTrail :

- Visão geral da criação de uma trilha
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas AppFabric as ações são registradas CloudTrail e documentadas na Referência da AWS AppFabric API. Por exemplo, chamadas para as `GetAppBundle` ações `CreateAppBundle`, `UpdateAppBundle`, e geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS service (Serviço da AWS).

Para obter mais informações, consulte o CloudTrail userIdentityelemento no Guia AWS CloudTrail do usuário.

Entendendo as entradas do arquivo de AppFabric log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateAppBundle` ação.


```
{
    "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"
    }
}
```

Cotas para AWS AppFabric

Você Conta da AWS tem cotas padrão, anteriormente chamadas de limites, para cada um. AWS service (Serviço da AWS) A menos que especificado de outra forma, cada cota é específica da região . Você pode solicitar o aumento de algumas cotas, porém, algumas delas não podem ser aumentadas.

Para ver as cotas de AppFabric, abra o console Service Quotas. No painel de navegação, escolha AWS serviços e selecione AppFabric.

Para solicitar um aumento da cota, consulte Requesting a quota increase no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível no Service Quotas, use o formulário de aumento de limite.

As cotas relacionadas AppFabric às suas Conta da AWS são mostradas na tabela a seguir.

Nome	Padrão	Ajustá	Descrição
Pacotes de aplicativos	Cada região compatível: 1	Não	O número máximo de pacotes de aplicativos que você pode criar em uma conta na AWS região atual.
Autorizações de aplicativos	Cada região com suporte: 50	Não	O número máximo de autorizações de aplicativos que você pode criar em uma conta na AWS região atual.
Ingestões	Cada região com suporte: 50	Não	O número máximo de ingestões que você pode criar em uma conta na AWS região atual.
Destinos de ingestão	Cada região com suporte: 5	Não	O número máximo de destinos de ingestão que você pode criar por

Nome	Padrão	Ajustá	Descrição
			ingestão em uma conta na região atual AWS .
AppClient	Cada região compatível: 1	Não	O número máximo AppClients que você pode criar em uma conta na AWS região atual. O recurso AWS AppFabric de produtividade está em versão prévia e está sujeito a alterações.

Histórico do documento para o Guia de AppFabric Administração

A tabela a seguir descreve as versões de documentação do AWS AppFabric.

Alteração	Descrição	Data
Novo aplicativo compatível	Adicionado JumpCloud como um aplicativo compatível. Para obter mais informações, consulte Aplicativos compatíveis em AWS AppFabric.	5 de junho de 2024
Novos aplicativos compatíveis e ferramenta de segurança	Adicionado Azure Monitor e Google Analytics como aplicativos suportados. Para obter mais informações, consulte Aplicativos compatíveis em AWS AppFabric. Adicionado Singularity Cloud como uma ferramenta de segurança compatível. Para obter mais informações, consulte Ferramentas de segurança compatíveis.	30 de abril de 2024
Novo aplicativo compatível	Adicionado SentinelOne como um aplicativo compatível. Para obter mais informações, consulte Aplicativos compatíveis em AWS AppFabric.	25 de abril de 2024
Novo aplicativo compatível	Adicionado 1Password como um aplicativo compatível. Para obter mais informações,	23 de abril de 2024

	consulte Aplicativos compatíveis em AWS AppFabric.	
Nova ferramenta de segurança suportada	Adicionado Dynatrace como uma ferramenta de segurança compatível. Para obter mais informações, consulte Ferramentas de segurança compatíveis.	26 de março de 2024
Nova métrica	Foi adicionada a métrica de status de autorização do AppFabric aplicativo. Para obter mais informaçõ es, consulte Monitoramento AWS AppFabric com Amazon CloudWatch Logs.	8 de março de 2024
Novo aplicativo compatível	Adicionado IBM Security® Verify como um aplicativo compatível. Para obter mais informações, consulte Aplicativos compatíveis em AWS AppFabric.	6 de março de 2024
Novo aplicativo compatível	Adicionado Box como um aplicativo compatível. Para obter mais informações, consulte Aplicativos compatíveis em AWS AppFabric.	28 de fevereiro de 2024

Novos aplicativos e métricas compatíveis	Cisco DuoSalesforceAdicionados e Terraform Cloud como aplicativos compatíveis. Para obter mais informações sobre eles, consulte Aplicativos compatíveis em AWS AppFabric. Foram adicionadas as métricas de latência de entrega de AppFabric dados e atraso geral de dados. Para obter mais informações, consulte Monitoramento AWS AppFabric com Amazon CloudWatch Logs.	1 de fevereiro de 2024
Foram adicionadas Atlassian Confluence, Genesys Cloud, HubSpot, OneLogin by One Identity, PagerDuty e Ping Identity como aplicações com suporte e Barracuda XDR como uma ferramenta de segurança compatível	Para obter mais informações sobre os novos aplicativos compatíveis, consulte Aplicativos compatíveis AWS AppFabric e Ferramentas de segurança compatíveis.	15 de dezembro de 2023
Foram adicionadas Atlassian Confluence, Genesys Cloud, HubSpot, OneLogin by One Identity, PagerDuty e Ping Identity como aplicações com suporte e Barracuda XDR como uma ferramenta de segurança compatível	Para obter mais informações sobre os novos aplicativos compatíveis, consulte Aplicativos compatíveis AWS AppFabric e Ferramentas de segurança compatíveis.	15 de dezembro de 2023
Foi adicionada a documentação de pré-visualização AWS AppFabric para produtividade	Para obter mais informações sobre AppFabric produtividade, consulte O que é AWS AppFabric para produtividade?	27 de novembro de 2023

Foram adicionadas GitHub e ServiceNow como aplicações com suporte	Para obter mais informações sobre as novas aplicações com suporte, consulte Aplicações com suporte.	31 de outubro de 2023
Começou a rastrear políticas AWS gerenciadas para AWS AppFabric	Para obter mais informações sobre as políticas AWS gerenciadas para AppFabric, consulte políticas AWS gerenciadas para AWS AppFabric.	27 de junho de 2023
Lançamento inicial	Versão inicial do Guia de AWS AppFabric Administração.	27 de junho de 2023

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.