Guida di amministrazione

AWS AppFabric

AWS AppFabric: Guida di amministrazione

Table of Contents

Che cos'è AWS AppFabric?

AWS AppFabric collega rapidamente le applicazioni SaaS (Software as a Service) in tutta l'organizzazione, in modo che i team IT e di sicurezza possano gestire e proteggere facilmente le applicazioni utilizzando uno schema standard e i dipendenti possano completare più rapidamente le attività quotidiane utilizzando l'intelligenza artificiale generativa.

Argomenti

Prodotti

Esplora i due aspetti AWS AppFabric: AppFabric per la sicurezza, progettata per una gestione e una sicurezza semplificate, e AppFabric per la produttività (anteprima), potenziata con funzionalità di intelligenza artificiale generativa. Per ulteriori informazioni, consulta i seguenti argomenti:

- Cosa c'è AWS AppFabric per la sicurezza?
- A cosa serve AWS AppFabric la produttività?

Vantaggi

Puoi usare AppFabric per fare quanto segue:

- Connect le applicazioni in pochi minuti e riduci i costi operativi.
- Aumenta la visibilità sui dati delle applicazioni SaaS per elevare il tuo livello di sicurezza.
- Semplifica automaticamente le attività tra le applicazioni con l'intelligenza artificiale generativa.

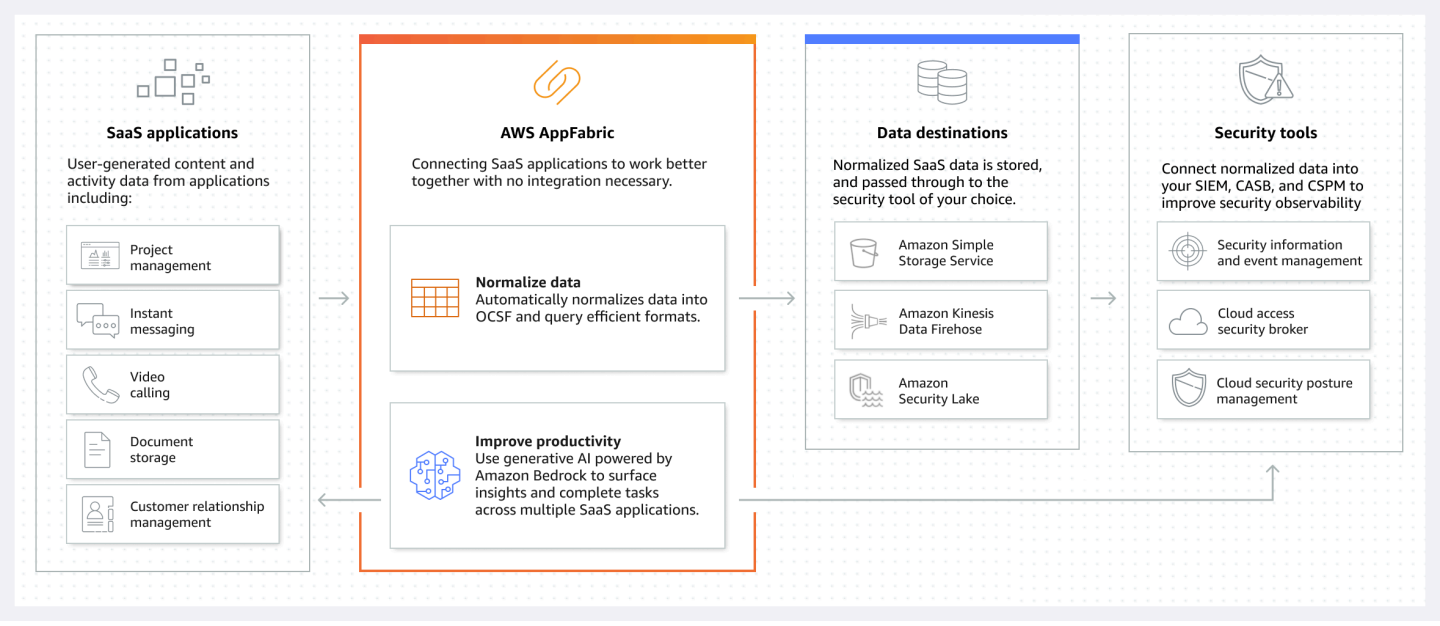
Casi d'uso

Puoi utilizzarlo AppFabric per:

- Connect rapidamente le applicazioni SaaS
  - AppFabric for security collega nativamente le principali applicazioni di produttività e sicurezza SaaS tra loro, fornendo una soluzione di interoperabilità SaaS completamente gestita.
- Migliora il tuo livello di sicurezza
  - I dati delle applicazioni vengono normalizzati automaticamente, consentendo agli amministratori di impostare policy comuni, standardizzare gli avvisi di sicurezza e gestire facilmente l'accesso degli utenti su più applicazioni.
- Reimmagina la produttività
  - Con un assistente AI generativo comune, AppFabric for productivity consente ai dipendenti di ottenere risposte rapidamente, automatizzare la gestione delle attività e generare approfondimenti nelle loro applicazioni di produttività SaaS.

Come funziona AppFabric

AppFabric collega rapidamente più applicazioni SaaS senza bisogno di codifica per una maggiore produttività e sicurezza. Il diagramma seguente mostra i vantaggi di. AppFabric



> **Note**
>
> AppFabric for productivity è attualmente lanciato in anteprima e disponibile negli Stati Uniti orientali (Virginia settentrionale). Regione AWS Per ulteriori informazioni su Regioni AWS, consulta AWS AppFabric endpoint e quote in. Riferimenti generali di AWS

Prezzi

Per dettagli ed esempi AppFabric sui prezzi, vedi AWS AppFabric Prezzi.

Disponibilità

Per visualizzare le AWS regioni e gli endpoint attualmente supportati AppFabric, consulta AWS AppFabric endpoint e quote nel AWS Riferimento generale.

Cosa c'è AWS AppFabric per la sicurezza?

AWS AppFabric for security collega rapidamente le applicazioni SaaS (Software as a Service) in tutta l'organizzazione, in modo che i team IT e di sicurezza possano gestire e proteggere facilmente le applicazioni utilizzando uno schema standard.

Argomenti

Vantaggi

AppFabric Per sicurezza puoi usare le seguenti operazioni:

- Connect le applicazioni in pochi minuti e riduci i costi operativi.
- Aumenta la visibilità sui dati delle applicazioni SaaS per elevare il tuo livello di sicurezza.

Casi d'uso

Puoi utilizzare AppFabric per motivi di sicurezza per:

- Connect rapidamente le applicazioni SaaS
  - AppFabric for security collega nativamente le principali applicazioni di produttività e sicurezza SaaS tra loro, fornendo una soluzione di interoperabilità SaaS completamente gestita.
- Aumento del livello di sicurezza

- I dati delle applicazioni vengono normalizzati automaticamente, consentendo agli amministratori di impostare policy comuni, standardizzare gli avvisi di sicurezza e gestire facilmente l'accesso degli utenti su più applicazioni.

Accesso per motivi di sicurezza AppFabric

AppFabric for security è disponibile negli Stati Uniti orientali (Virginia settentrionale), Europa (Irlanda) e Asia Pacifico (Tokyo). Regioni AWS Per ulteriori informazioni su Regioni AWS, consulta AWS AppFabric endpoint e quote in. Riferimenti generali di AWS

In ogni regione puoi accedere AppFabric per motivi di sicurezza in uno dei modi seguenti:

AWS Management Console

AWS Management Console È un'interfaccia basata sul browser che puoi utilizzare per creare e gestire le AWS risorse. La AppFabric console fornisce l'accesso alle risorse. AppFabric È possibile utilizzare la AppFabric console per creare e gestire tutte le AppFabric risorse.

AppFabric API

Per accedere a livello di AppFabric programmazione, utilizza le AppFabric API e invia richieste HTTPS direttamente al servizio. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di AWS AppFabric .

AWS Command Line Interface (AWS CLI)

Con AWS CLI, puoi inviare comandi alla riga di comando del tuo sistema per interagire AppFabric e altro Servizi AWS. Se desideri creare script che eseguono le attività di, sono inoltre utili gli strumenti a riga di comando. Per informazioni sull'installazione e l'utilizzo di AWS CLI, consultate la Guida per AWS Command Line Interface l'utente della versione 2. Per informazioni sui AWS CLI comandi per AppFabric, consultate la AppFabric sezione della Guida di AWS CLI riferimento.

Servizi correlati

È possibile utilizzare quanto segue Servizi AWS con AppFabric per motivi di sicurezza:

Amazon Data Firehose

Amazon Data Firehose è un servizio ETL (estrazione, trasformazione e caricamento) dei dati che acquisisce, trasforma e fornisce dati di streaming a data lake, data store e servizi di analisi. Quando

si utilizza AppFabric, è possibile scegliere di inviare i log di controllo normalizzati o non elaborati di Open Cybersecurity Schema Framework (OCSF) in formato JSON su un flusso Firehose come destinazione. Per ulteriori informazioni, consultate Creare una posizione di output in Firehose.

Amazon Security Lake

Amazon Security Lake centralizza automaticamente i dati di sicurezza provenienti da AWS ambienti, provider SaaS, origini on-premise e cloud in un data lake creato appositamente e archiviato nel tuo account. Puoi integrare i dati dei log di AppFabric controllo con Security Lake selezionando Amazon Data Firehose come destinazione e configurando Firehose per fornire i dati nel formato e nel percorso corretti in Security Lake. Per ulteriori informazioni, consulta Raccolta di dati da fonti personalizzate nella Guida per l'utente di Amazon Security Lake.

Amazon Simple Storage Service

Amazon Simple Storage Service (Amazon S3) è un servizio di archiviazione di oggetti che offre scalabilità, disponibilità dei dati, sicurezza e prestazioni tra le migliori del settore. Quando lo utilizzi AppFabric, puoi scegliere di inviare i log di controllo OCSF normalizzati (JSON oApache Parquet) o non elaborati (JSON) su un bucket Amazon S3 nuovo o esistente come destinazione. Per ulteriori informazioni, consulta Creare una posizione di output in Amazon S3.

Amazon QuickSight

QuickSight alimenta le organizzazioni basate sui dati con business intelligence (BI) unificata su larga scala. Con QuickSight, tutti gli utenti possono soddisfare le diverse esigenze di analisi dalla stessa fonte di verità attraverso dashboard interattivi moderni, report impaginati, analisi integrate e query in linguaggio naturale. Puoi analizzare i dati dei log di AppFabric QuickSight controllo scegliendo come origine il bucket Amazon S3 in cui sono archiviati AppFabric i log. Per ulteriori informazioni, consulta Creazione di un set di dati utilizzando i file Amazon S3 nella Guida per QuickSight l'utente. Puoi anche importare AppFabric dati da Amazon S3 ad Amazon Athena e selezionare Amazon Athena come origine dati in. QuickSight Per ulteriori informazioni, consulta Creazione di un set di dati utilizzando i dati di Amazon Athena nella Guida per QuickSight l'utente.

AWS Key Management Service

Con AWS Key Management Service (AWS KMS), puoi creare, gestire e controllare le chiavi crittografiche tra le tue applicazioni e. Servizi AWS Quando create un pacchetto di app AppFabric, impostate una chiave di crittografia per proteggere in modo sicuro i dati delle applicazioni autorizzate. Questa chiave crittografa i dati all'interno del servizio. AppFabric AppFabric può utilizzare una chiave Chiave di proprietà di AWS creata e gestita da per tuo AppFabric conto o una chiave gestita dal

cliente da te creata e gestita dall'utente. AWS KMS Per ulteriori informazioni, consulta Creare una AWS KMS chiave.

Open Cybersecurity Schema Framework per AWS AppFabric

L'Open Cybersecurity Schema Framework (OCSF) è uno sforzo collaborativo AWS e open source di partner leader nel settore della sicurezza informatica. OCSF fornisce uno schema standard per gli eventi di sicurezza più comuni, definisce i criteri di controllo delle versioni per facilitare l'evoluzione dello schema e include un processo di autogoverno per produttori e consumatori di registri di sicurezza. Il codice sorgente pubblico per OCSF è ospitato su. GitHub

Schema basato su OCSF in AppFabric

Lo schema basato su OCSF 1.1 AWS AppFabric per la sicurezza è personalizzato specificamente per soddisfare le esigenze di osservabilità normalizzata, coerente e a basso sforzo del loro portafoglio di software as a service (SaaS). AppFabric determina la mappatura corretta per ogni campo ed evento. AppFabric, in collaborazione con la comunità open source OCSF, ha introdotto nuove categorie di eventi, classi di eventi, attività e oggetti OCSF in modo che OCSF sia applicabile agli eventi delle applicazioni SaaS. AppFabric normalizza automaticamente gli eventi di controllo che riceve dalle applicazioni SaaS e fornisce questi dati ai servizi Amazon Simple Storage Service (Amazon S3) o Amazon Data Firehose del tuo. Account AWS Per una destinazione Amazon S3, puoi scegliere tra due opzioni di normalizzazione (OCSF o Raw) e due opzioni di formato dei dati (JSON o Parquet). Quando si effettua la consegna a Firehose, è anche possibile scegliere tra due opzioni di normalizzazione (OCSF o Raw), ma il formato dei dati è limitato a JSON.

Prerequisiti e consigli per l'uso AWS AppFabric

Se sei un nuovo AWS cliente, completa i prerequisiti di configurazione elencati in questa pagina prima di iniziare a utilizzare AWS AppFabric For Security. Per queste procedure di configurazione, utilizzi il servizio AWS Identity and Access Management (IAM). Per informazioni complete su IAM, consulta la Guida per l'utente di IAM.

Argomenti

- Registrati per un Account AWS
- Crea un utente con accesso amministrativo
- (Obbligatorio) Prerequisiti completi per l'applicazione

- (Facoltativo) Creare una posizione di output
- (Facoltativo) Crea una chiave AWS KMS

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Parte della procedura di registrazione prevede la ricezione di una telefonata o di un messaggio di testo e l'immissione di un codice di verifica sulla tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

(Obbligatorio) Prerequisiti completi per l'applicazione

AppFabric Per motivi di sicurezza, la ricezione di informazioni sugli utenti e registri di controllo dalle applicazioni, molte applicazioni richiedono che l'utente disponga di ruoli e tipi di piano specifici. Assicuratevi di aver esaminato i prerequisiti per ogni applicazione con cui desiderate autorizzare l'autorizzazione AppFabric per motivi di sicurezza e di disporre dei piani e dei ruoli appropriati. Per ulteriori informazioni sui prerequisiti specifici dell'applicazione, consultate Applicazioni supportate o scegliete uno dei seguenti argomenti specifici dell'applicazione.

- Configura 1Password per AppFabric
- Configura Asana per AppFabric
- Configura Azure Monitor per AppFabric
- Configura Atlassian Confluence per AppFabric
- Configura Atlassian Jira suite per AppFabric
- Configura Box per AppFabric
- Configura Cisco Duo per AppFabric
- Configura Dropbox per AppFabric
- Configura Genesys Cloud per AppFabric
- Configura GitHub per AppFabric
- Configura Google Analytics per AppFabric
- Configura Google Workspace per AppFabric
- Configura HubSpot per AppFabric
- Configura IBM Security® Verify per AppFabric
- Configura JumpCloud per AppFabric
- Configura Microsoft 365 per AppFabric
- Configura Miro per AppFabric
- Configura Okta per AppFabric
- Configura OneLogin by One Identity per AppFabric
- Configura PagerDuty per AppFabric
- Configura Ping Identity per AppFabric
- Configura Salesforce per AppFabric
- Configura ServiceNow per AppFabric

- Configura Singularity Cloud per AppFabric
- Configura Slack per AppFabric
- Configura Smartsheet per AppFabric
- Configura Terraform Cloud per AppFabric
- Configura Webex by Cisco per AppFabric
- Configura Zendesk per AppFabric
- Configura Zoom per AppFabric

(Facoltativo) Creare una posizione di output

AppFabric per la sicurezza supporta Amazon Simple Storage Service (Amazon S3) e Amazon Data Firehose come destinazioni di acquisizione dei log di controllo.

Amazon S3

Puoi creare un nuovo bucket Amazon S3 utilizzando la AppFabric console quando crei una destinazione di importazione. Puoi anche creare un bucket utilizzando il servizio Amazon S3. Se scegli di creare il bucket utilizzando il servizio Amazon S3, devi creare il bucket prima di creare la destinazione di ingestione e quindi selezionare AppFabric il bucket quando crei la destinazione di importazione. Puoi scegliere di utilizzare un bucket Amazon S3 esistente nel tuo Account AWS, purché soddisfi i seguenti requisiti per i bucket esistenti:

- AppFabric per motivi di sicurezza, è necessario che il bucket Amazon S3 si trovi nelle Regione AWS stesse risorse Amazon S3.
- Puoi crittografare il tuo bucket utilizzando uno dei seguenti metodi:
  - Crittografia lato server con chiavi gestite da Amazon S3 (SSE-S3)
  - Crittografia lato server con chiavi AWS Key Management Service (AWS KMS) (SSE-KMS) utilizzando il valore predefinito (). Chiave gestita da AWS `aws/s3`

Amazon Data Firehose

Puoi scegliere di utilizzare Amazon Data Firehose come destinazione di importazione per AppFabric i dati di sicurezza. Per utilizzare Firehose, puoi creare il flusso di distribuzione Firehose Account AWS prima di creare un'ingestione o mentre crei una destinazione di ingestione in. AppFabric È possibile creare un flusso di distribuzione Firehose utilizzando il AWS Management Console AWS

CLI, o il AWS APIs o. SDKs Per le istruzioni sulla configurazione dello stream, consultate i seguenti argomenti:

- AWS Management Console istruzioni — Creazione di un Amazon Data Firehose Delivery Stream nella Amazon Data Firehose Developer Guide
- AWS CLI istruzioni: create-delivery-streamnella guida di riferimento ai comandi AWS CLI
- AWS APIs e SDKs istruzioni: CreateDeliveryStreamnell'Amazon Data Firehose API Reference

I requisiti AppFabric per l'utilizzo di Amazon Data Firehose come destinazione di output di sicurezza sono i seguenti:

- È necessario creare lo stream utilizzando le Regione AWS stesse risorse utilizzate AppFabric per la sicurezza.
- È necessario selezionare Direct PUT come sorgente.
- Allega la politica AmazonKinesisFirehoseFullAccess AWS gestita al tuo utente o assegna le seguenti autorizzazioni all'utente:

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

Firehose supporta l'integrazione con una varietà di strumenti di sicurezza di terze parti, come eSplunk. Logz.io Per informazioni su come configurare correttamente Amazon Kinesis in modo che invii dati a questi strumenti, consulta Destination Settings nella Amazon Data Firehose Developer Guide.

(Facoltativo) Crea una chiave AWS KMS

Durante il processo di creazione di un pacchetto di app AppFabric for security, selezionerai o configurerai una chiave di crittografia per proteggere in modo sicuro i tuoi dati da tutte le applicazioni autorizzate. Questa chiave verrà utilizzata per crittografare i dati all'interno del servizio. AppFabric

AppFabric for security crittografa i dati per impostazione predefinita. AppFabric for security può utilizzare una chiave Chiave di proprietà di AWS creata e gestita da per tuo AppFabric conto o una chiave gestita dal cliente che crei e gestisci in AWS Key Management Service (AWS KMS). Chiavi di proprietà di AWS sono una raccolta di AWS KMS chiavi Servizio AWS possedute e gestite per essere utilizzate in più lingue Account AWS. Le chiavi gestite dal cliente sono AWS KMS chiavi Account AWS che create, possedete e gestite dall'utente. Per ulteriori informazioni sulle chiavi Chiavi di proprietà di AWS gestite dai clienti, consulta Customer keys and AWS keys nella AWS Key Management Service Developer Guide.

Se desideri utilizzare una chiave gestita dal cliente per crittografare i tuoi dati, come i token di autorizzazione, AppFabric per motivi di sicurezza, puoi crearne una con. AWS KMS Per ulteriori informazioni sulla politica di autorizzazione che garantisce l'accesso alla chiave gestita dal cliente AWS KMS, consulta la sezione Politica chiave di questa guida.

Inizia con AWS AppFabric la sicurezza

Per iniziare a usare AWS AppFabric la sicurezza, devi prima creare un pacchetto di app, quindi autorizzare e connettere le applicazioni al tuo app bundle. Dopo aver collegato le autorizzazioni delle app alle applicazioni, puoi utilizzarle AppFabric per funzionalità di sicurezza come l'inserimento dei log di controllo e l'accesso degli utenti.

Questa sezione spiega come iniziare a utilizzare AppFabric in. AWS Management Console

Argomenti

Prerequisiti

Prima di iniziare, è necessario creare un utente Account AWS e un utente amministrativo. Per ulteriori informazioni, consultare Registrati per un Account AWS e Crea un utente con accesso amministrativo.

Passaggio 1: creare un pacchetto di app

Un pacchetto di app memorizza tutte le autorizzazioni e le acquisizioni delle app AppFabric per la sicurezza. Per creare un pacchetto di app, configura una chiave di crittografia per proteggere in modo sicuro i dati dell'applicazione autorizzata.

1. Apri la AppFabric console all'indirizzo. https://console.aws.amazon.com/appfabric/
2. Nel selettore Seleziona una regione nell'angolo superiore destro della pagina, seleziona un. Regione AWS AppFabric è disponibile solo nelle regioni Stati Uniti orientali (Virginia settentrionale), Europa (Irlanda) e Asia Pacifico (Tokyo).
3. Selezionare Getting started (Nozioni di base).
4. Nella pagina Guida introduttiva, per la Fase 1. Crea un pacchetto di app, scegli Crea pacchetto di app.
5. Nella sezione Crittografia, configura una chiave di crittografia per proteggere in modo sicuro i tuoi dati da tutte le applicazioni autorizzate. Questa chiave viene utilizzata per crittografare i dati all'interno del servizio AppFabric di sicurezza.

   AppFabric for security crittografa i dati per impostazione predefinita. AppFabric può utilizzare una chiave Chiave di proprietà di AWS creata e gestita da per tuo AppFabric conto o una chiave gestita dal cliente che crei e gestisci in AWS Key Management Service (AWS KMS).
6. Per AWS KMS Chiave, scegli Usa Chiave di proprietà di AWS o Chiave gestita dal cliente.

   Se scegli di utilizzare una chiave gestita dal cliente, inserisci l'Amazon Resource Name (ARN) o l'ID chiave della chiave esistente che desideri utilizzare oppure scegli Crea una AWS KMS chiave.

   Quando scegli una chiave Chiave di proprietà di AWS o una chiave gestita dal cliente, considera quanto segue:

   - Chiavi di proprietà di AWSsono una raccolta di AWS Key Management Service (AWS KMS) chiavi Servizio AWS possedute e gestite da un utente per l'utilizzo multiplo Account AWS. Sebbene non Chiavi di proprietà di AWS siano presenti nel tuo account Account AWS, Servizio AWS puoi utilizzarne una Chiave di proprietà di AWS per proteggere le risorse del tuo account. Chiavi di proprietà di AWS non influiscono sulle AWS KMS quote del tuo account. Non è necessario creare o mantenere la chiave o la relativa policy delle chiavi. La rotazione di Chiavi di proprietà di AWS varia tra i servizi. Per informazioni sulla rotazione di un Chiave di proprietà di AWS for AppFabric, vedete Encryption at rest.

- Le chiavi gestite dal cliente sono chiavi KMS Account AWS che create, possedete e gestite dall'utente. Hai il pieno controllo su queste AWS KMS chiavi. Puoi stabilire e mantenere le loro politiche chiave, le politiche AWS Identity and Access Management (IAM) e le sovvenzioni. È possibile abilitarli e disabilitarli, ruotare il loro materiale crittografico, aggiungere tag, creare alias che fanno riferimento alle AWS KMS chiavi e programmare l' AWS KMS eliminazione delle chiavi. Le chiavi gestite dal cliente vengono visualizzate nella pagina Chiavi gestite dal cliente del modulo. AWS Management Console AWS KMS

  Per identificare in modo definitivo una chiave gestita dal cliente, utilizza l'`DescribeKey`operazione. Per le chiavi gestite dal cliente, il valore del campo `KeyManager` della risposta di `DescribeKey` è `CUSTOMER`. È possibile utilizzare la chiave gestita dal cliente nelle operazioni crittografiche e controllare l'utilizzo nei AWS CloudTrail log. Con molte di Servizi AWS esse che si integrano con AWS KMS, puoi specificare una chiave gestita dal cliente per proteggere i dati archiviati e gestiti per te. Le chiavi gestite dal cliente sono soggette a un canone mensile e a una tariffa d'uso superiore al piano AWS gratuito. Le chiavi gestite dal cliente vengono conteggiate nelle AWS KMS quote del tuo account.

Per ulteriori informazioni sulle chiavi Chiavi di proprietà di AWS gestite dal cliente, consulta Customer keys and AWS keys nella AWS Key Management Service Developer Guide.

> **Note**
>
> Quando viene creato un pacchetto di app, AppFabric per motivi di sicurezza crea anche un ruolo IAM speciale nell'ambito del pacchetto Account AWS denominato service-linked role (SLR) per. AppFabric Consente al servizio di inviare metriche ad Amazon CloudWatch. Dopo aver aggiunto una destinazione di audit log, la SLR consente ai servizi di sicurezza AppFabric di accedere alle risorse AWS (bucket Amazon S3, flussi di distribuzione Amazon Data Firehose). Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AppFabric.

7. (Facoltativo) Per i tag, hai la possibilità di aggiungere tag al pacchetto dell'app. I tag sono coppie chiave-valore che assegnano metadati alle risorse che crei. Per ulteriori informazioni, consulta Taggare le AWS risorse nella Guida per l'AWS utente di Tag Editor.
8. Per creare il tuo pacchetto di app, scegli Crea pacchetto di app.

Passaggio 2: autorizza le applicazioni

Dopo aver creato correttamente il pacchetto di app, ora puoi autorizzare la AppFabric sicurezza a connetterti e interagire con ciascuna delle tue applicazioni. Le applicazioni autorizzate vengono crittografate e archiviate nel pacchetto di app. Per configurare più autorizzazioni per app bundle, ripeti il passaggio di autorizzazione dell'app secondo necessità per ciascuna applicazione.

Prima di iniziare la procedura per autorizzare le applicazioni, esamina e verifica i prerequisiti per ciascuna applicazione, ad esempio il tipo di piano necessario, in. Applicazioni supportate AppFabric per la sicurezza

1. Nella pagina Guida introduttiva, per la Fase 2. Autorizza le applicazioni, scegli Crea autorizzazione app.
2. Nella sezione Autorizzazione dell'app, seleziona l'applicazione a cui desideri concedere l'autorizzazione AppFabric per motivi di sicurezza alla quale connetterti dal menu a discesa Applicazione. Le applicazioni mostrate sono quelle attualmente supportate da AppFabric for security.
3. Quando si seleziona un'applicazione, vengono visualizzati i campi di informazioni obbligatori. Questi campi includono l'ID del tenant e il nome del tenant e possono includere anche l'ID cliente, il segreto del cliente o il token di accesso personale. I valori di input per questi campi variano in base all'applicazione. Per istruzioni dettagliate specifiche dell'applicazione su come trovare questi valori, vedere. Applicazioni supportate AppFabric per la sicurezza
4. (Facoltativo) Per i tag, hai la possibilità di aggiungere tag all'autorizzazione dell'app. I tag sono coppie chiave-valore che assegnano metadati alle risorse che crei. Per ulteriori informazioni, consulta Taggare le AWS risorse nella Guida per l'AWS utente di Tag Editor.
5. Scegli l'autorizzazione per la creazione dell'app.
6. Se viene visualizzata una finestra pop-up (a seconda dell'applicazione a cui si sta collegando), seleziona Consenti AppFabric per autorizzare per motivi di sicurezza la connessione all'applicazione.

   Se l'autorizzazione dell'app ha avuto esito positivo, nella pagina Guida introduttiva verrà visualizzato il messaggio di avvenuta autorizzazione dell'app connessa.
7. Puoi controllare lo stato dell'autorizzazione dell'app in qualsiasi momento nella pagina Autorizzazioni dell'app elencata nel riquadro di navigazione, sotto lo stato di ciascuna applicazione. Lo stato Connesso indica che l'autorizzazione dell'app è stata concessa AppFabric per motivi di sicurezza per la connessione all'applicazione ed è completa.

8. I possibili stati di autorizzazione delle app sono riportati nella tabella seguente, inclusi i passaggi per la risoluzione dei problemi che è possibile eseguire per correggere gli errori correlati.

Nome dello stato	Descrizione dello stato	Fasi per la risoluzione dei problemi
Pending (In attesa)	Lo stato In sospeso indica che è stata creata un'autorizzazione per l'applicazione, ma AppFabric per motivi di sicurezza non è ancora connessa all'applicazione.	Quando vedi questo stato, seleziona Connect dal menu a discesa Azioni della pagina di autorizzazione dell'app per avviare una connessione. Se l'errore persiste, controlla se il blocco pop-up del tuo browser è disabilitato. Se viene visualizzato un messaggio di errore, ad esempio 400 Bad Request nella finestra pop-up, controlla che tutte le informazioni, come l'ID tenant, l'ID client e il segreto del client, siano state inserite correttamente. È anche possibile che l'autorizzazione dell'applicazione all'app non sia stata creata correttamente. Per ulteriori informazioni, consulta Applicazioni supportate.

Nome dello stato	Descrizione dello stato	Fasi per la risoluzione dei problemi
Convalida della connessione non riuscita	Uno stato di convalida della connessione non riuscita significa che, AppFabric per motivi di sicurezza, non è possibile convalidare l'autorizzazione della connessione dell'app con un'applicazione.	Verifica che tutte le informazioni, come l'ID tenant, l'ID client e il client secret, siano inserite correttamente per l'autorizzazione dell'app.
Rotazione automatica del token non riuscita	Uno stato di rotazione automatica del token non riuscito significa che il token di OAuth aggiornamento non è riuscito dopo che l'autorizzazione dell'app è stata connessa correttamente.	Se l'errore persiste, controlla l'applicazione di autenticazione dell'applicazione. Per ulteriori informazioni, consulta Applicazioni supportate.

9. Per autorizzare applicazioni aggiuntive, ripetere i passaggi da 1 a 8, se necessario.

Fase 3: Configurare le acquisizioni dei log di controllo

Dopo aver creato almeno un'autorizzazione per l'app nel pacchetto dell'app, ora puoi configurare l'inserimento dei registri di controllo. L'inserimento dei log di controllo utilizza i log di controllo di un'applicazione autorizzata e li normalizza nell'Open Cybersecurity Schema Framework (OCSF). Quindi li consegna a una o più destinazioni all'interno. AWS Puoi anche scegliere di inviare file JSON non elaborati alle tue destinazioni.

1. Nella pagina Guida introduttiva, per lo Step 3. Configura la sezione relativa alle acquisizioni dei log di controllo, seleziona Configurazione rapida delle acquisizioni.

> **Note**
>
> Per una configurazione più rapida, utilizza la pagina di configurazione rapida di Ingestions, accessibile solo dalla pagina Guida introduttiva, per creare inserimenti per più autorizzazioni di app contemporaneamente, con la stessa destinazione di importazione.

Ad esempio, lo stesso bucket Amazon S3 o lo stesso flusso di dati Amazon Data Firehose.
Puoi anche creare acquisizioni dalla pagina Ingestioni, accessibile dal pannello di navigazione. Nella pagina Inserimenti, è possibile configurare un'importazione alla volta per destinazioni distinte. Nella pagina Inserimenti, puoi anche creare un tag per un'ingestione. Le seguenti istruzioni si riferiscono alla pagina di configurazione rapida di Ingestions.

2. Per Seleziona le autorizzazioni dell'app, seleziona le autorizzazioni dell'app per cui desideri creare le acquisizioni dei log di controllo. I nomi dei tenant che compaiono nel menu a discesa delle autorizzazioni delle app sono i nomi dei tenant delle applicazioni per le quali hai precedentemente creato un'autorizzazione per l'app con for security. AppFabric
3. Per Aggiungi destinazione, seleziona una destinazione per le acquisizioni dei log di controllo delle applicazioni selezionate. Le opzioni di destinazione includono Amazon S3 - Existing Bucket, Amazon S3 - New Bucket o Amazon Data Firehose. Se selezioni più nomi di tenant, la destinazione scelta viene applicata a ogni acquisizione di un'autorizzazione di app.
4. Quando scegli una destinazione, vengono visualizzati i campi obbligatori aggiuntivi.

    a. Se scegli Amazon S3 — New bucket come destinazione, devi inserire il nome del bucket S3 che desideri creare. Per ulteriori istruzioni su come creare un bucket Amazon S3, consulta Creare una destinazione di output.

    b. Se scegli Amazon S3 — bucket esistente come destinazione, seleziona il nome del bucket Amazon S3 che desideri utilizzare.

    c. Se scegli Amazon Data Firehose come destinazione, seleziona il nome del flusso di consegna dall'elenco a discesa Firehose Delivery Stream Name. Per ulteriori istruzioni su come creare un flusso di distribuzione di Amazon Data Firehose, consulta Creare una destinazione di output e prendere nota della politica di autorizzazione richiesta per AppFabric motivi di sicurezza.

5. Per Schema & Format, puoi scegliere di archiviare i log di controllo in formato Raw - JSON, OCSF - JSON, OCSF - Parquet per bucket Amazon S3 o Raw - JSON o OCSF-JSON per Firehose.

    Il formato di dati Raw fornisce i dati del registro di controllo convertiti in JSON da una stringa di dati. Il formato di dati OCSF normalizza i dati del registro di controllo secondo lo schema Open Cybersecurity Schema Framework (OCSF) AppFabric per motivi di sicurezza. Per ulteriori informazioni su come utilizza OCSF, vedere. AppFabric Open Cybersecurity Schema Framework

per AWS AppFabric È possibile selezionare solo uno schema e un tipo di dati di formato alla volta per un'ingestione. Se desideri aggiungere uno schema e un tipo di dati di formato aggiuntivi, puoi configurare una destinazione di ingestione aggiuntiva ripetendo il processo di creazione dell'ingestione.

6. (Facoltativo) Se desideri aggiungere un tag a un'ingestione, vai alla pagina Inserimenti dal pannello di navigazione. Per accedere alla pagina dei dettagli dell'ingestione, seleziona il nome del tenant. Per i tag, hai la possibilità di aggiungere tag alla tua ingestione. I tag sono coppie chiave-valore che assegnano metadati alle risorse create. Per ulteriori informazioni, consulta Taggare le AWS risorse nella Guida per l'AWS utente di Tag Editor.
7. Scegli Configura le acquisizioni.

   Quando configuri correttamente un'ingestione, nella pagina Guida introduttiva verrà visualizzato un messaggio di successo di Ingestion creato.
8. Puoi anche controllare lo stato delle tue importazioni e lo stato delle tue destinazioni di importazione in qualsiasi momento nella pagina Ingestioni dal pannello di navigazione. In questa pagina, puoi vedere il nome del tenant creato durante la creazione dell'autorizzazione dell'app, la destinazione e lo stato delle tue acquisizioni. Lo stato Abilitato per l'ingestione significa che l'ingestione è abilitata. Se scegli il nome del tenant di un'autorizzazione dell'app in questa pagina, puoi visualizzare una pagina di dettaglio relativa all'autorizzazione dell'app, inclusi i dettagli della destinazione e lo stato. Lo stato Attivo per la destinazione di importazione indica che la destinazione è configurata correttamente e attiva. Se l'autorizzazione dell'app ha lo stato Connesso e lo stato della destinazione di importazione è Attivo, il registro di controllo deve essere elaborato e consegnato. Se lo stato di autorizzazione dell'app o lo stato di destinazione di importazione sono tra gli stati non riusciti, il registro di controllo non verrà elaborato o consegnato anche se lo stato di importazione è abilitato. Per correggere un errore di autorizzazione dell'app, consulta il passaggio 2. Autorizza le applicazioni.
9. I possibili stati di destinazione di ingestione e ingestione sono riportati nella tabella seguente, con le procedure di risoluzione dei problemi che è possibile eseguire per correggere eventuali stati di errore.

Nome dello stato o dello stato	Descrizione	Fasi per la risoluzione dei problemi
Disabilitato	Uno stato Disabilitato per l'ingestione significa che l'ingestione è disabilitata.	È possibile abilitare l'ingesti one selezionando Abilita dal

Nome dello stato o dello stato	Descrizione	Fasi per la risoluzione dei problemi
		menu a discesa Azioni della pagina Inserimenti.
Failed (Non riuscito)	Lo stato Failed per la destinazione di ingestione significa che la destinazione di ingestione non accetta il log di controllo. Ad esempio, questo stato potrebbe verificarsi a causa di una posizione di archiviazione completa.	Per risolvere questi problemi, accedi alle console Amazon S3 o Firehose.

Passaggio 4: utilizza lo strumento di accesso utente

Utilizzando lo strumento AppFabric for security user access, i team addetti alla sicurezza e agli amministratori IT possono vedere rapidamente chi ha accesso a applicazioni specifiche eseguendo una semplice ricerca utilizzando l'indirizzo e-mail aziendale del dipendente. Questo approccio può essere utile per ridurre il tempo dedicato ad attività come il deprovisioning degli utenti, che potrebbero richiedere il controllo o il controllo manuale dell'accesso di un utente tra le applicazioni SaaS. Se viene trovato un utente, AppFabric per motivi di sicurezza fornisce il nome dell'utente nell'applicazione e il suo stato di utente in-app (ad esempio, Attivo), se fornito dall'applicazione. AppFabric for security cerca tutte le applicazioni autorizzate in un pacchetto di app per restituire un elenco di applicazioni a cui l'utente ha accesso.

1. Nella pagina Guida introduttiva, per la Fase 4. Usa lo strumento di accesso utente, scegli Cerca utente.
2. Nel campo Indirizzo e-mail, digita l'indirizzo e-mail di un utente e scegli Cerca.
3. Nella sezione Risultati della ricerca, viene visualizzato un elenco di tutte le applicazioni autorizzate a cui l'utente ha accesso. Per mostrare il nome dell'utente nell'applicazione e il relativo stato (se disponibile), seleziona un risultato di ricerca.

4. Un messaggio di Utente trovato nella colonna dei risultati di ricerca indica che l'utente può accedere all'app elencata. La tabella seguente mostra i possibili risultati di ricerca, gli errori e le azioni che è possibile intraprendere per correggere gli errori.

Risultato della ricerca	Descrizione
L'utente non è stato trovato	Non è stato trovato nessun utente con l'indirizzo e-mail utilizzato.
Non è stato trovato un token di autorizzazione. Connect l'autorizzazione dell'app per l'applicazione.	Verifica che tutte le informazioni, come l'ID tenant, l'ID client e il segreto del cliente, siano inserite correttamente per l'autorizzazione dell'app.
Il token di autorizzazione è stato revocato. Connect l'autorizzazione dell'app per l'applicazione.	Verifica che tutte le informazioni, come l'ID tenant, l'ID client e il segreto del cliente, siano inserite correttamente per l'autorizzazione dell'app.
Non siamo riusciti a ruotare il token di autorizzazione. Connect l'autorizzazione dell'app per l'applicazione.	Il token OAuth di aggiornamento non è riuscito dopo che l'autorizzazione dell'app è stata connessa correttamente. Se l'errore persiste, controlla l'applicazione di autenticazione dell'applicazione. Per ulteriori informazioni, consulta Applicazioni supportate.
Le autorizzazioni richieste non sono state trovate. Connect l'autorizzazione dell'app per l'applicazione.	Verifica che tutte le informazioni, come l'ID tenant, l'ID client e il segreto del cliente, siano inserite correttamente per l'autorizzazione dell'app.
L'autorizzazione dell'app non è valida.	Verifica che tutte le informazioni, come l'ID tenant, l'ID client e il segreto del cliente, siano inserite correttamente per l'autorizzazione dell'app.

Risultato della ricerca	Descrizione
Non è stato possibile chiamare l'API dell'appl icazione a causa di autorizzazioni insuffici enti.	Verifica che tutte le informazioni, come l'ID tenant, l'ID client e il segreto del cliente, siano inserite correttamente per l'autoriz zazione dell'app.
Il limite di richieste di applicazione è stato superato.	Si tratta di un messaggio di errore ricevuto dall'applicazione. Puoi provare a cercare un indirizzo email in un secondo momento.
L'applicazione ha rilevato un errore interno del server	Si tratta di un messaggio di errore ricevuto dall'applicazione. Puoi provare a cercare un indirizzo email in un secondo momento.
L'applicazione ha riscontrato un errore di gateway errato	Si tratta di un messaggio di errore ricevuto dall'applicazione. Puoi provare a cercare un indirizzo email in un secondo momento.
L'applicazione non è pronta a gestire la richiesta	Si tratta di un messaggio di errore ricevuto dall'applicazione. Puoi provare a cercare un indirizzo email in un secondo momento.
L'applicazione ha riscontrato un errore di richiesta errato.	Questo è un messaggio di errore che abbiamo ricevuto dall'applicazione. Puoi provare a cercare nuovamente un'e-mail più tardi.
L'applicazione ha rilevato un errore di disponibilità del servizio.	Questo è un messaggio di errore che abbiamo ricevuto dall'applicazione. Puoi provare a cercare nuovamente un'e-mail più tardi.

Passaggio 5: Connect AppFabric per accedere ai dati di sicurezza negli strumenti di sicurezza e in altre destinazioni

I dati normalizzati (o non elaborati) delle applicazioni da AppFabric sono compatibili con qualsiasi strumento che supporti l'inserimento di dati da Amazon S3 e l'integrazione con Firehose, inclusi strumenti di sicurezza come Barracuda XDR, Dynatrace, Logz.io, Netskope, NetWitness, Rapid7e Splunko la tua soluzione di sicurezza proprietaria. Per ottenere dati applicativi normalizzati (o non elaborati) da AppFabric, seguite i passaggi precedenti da 1 a 3. Per ulteriori dettagli su come configurare strumenti e servizi di sicurezza specifici, consulta Strumenti e servizi di sicurezza compatibili.

Applicazioni supportate AppFabric per la sicurezza

AWS AppFabric for security supporta l'integrazione con le seguenti applicazioni. Scegli il nome di un'applicazione per ulteriori informazioni su come configurare AppFabric la sicurezza per la connessione ad essa.

Argomenti

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

Configura 1Password per AppFabric

1Password è un gestore di password che ti aiuta a creare, archiviare e utilizzare password sicure per tutti i tuoi account online. Inoltre, protegge i tuoi dati con la crittografia, ti avvisa in caso di violazioni e ti consente di condividere le password.

È possibile utilizzare, a fini di sicurezza, AWS AppFabric per controllare i registri e i dati degli utenti da 1Password, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per 1Password

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da 1Password.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da 1Password verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- Devi avere un account a pagamento attivo 1Password Piano di abbonamento Business o Enterprise. Per ulteriori informazioni, consulta 1Password Enterprise su 1Password sito web.
- È necessario avere un ruolo di amministratore o un proprietario del team nel 1Password account. Per ulteriori informazioni, consulta Gruppi in 1Password sito web di supporto.

Considerazioni sui limiti di velocità

Il 1Password AuditLog L'API Events limita le richieste a 600 al minuto e fino a 30.000 all'ora. Il superamento di questi limiti restituisce un errore. Per ulteriori informazioni, consulta 1Password Limiti di velocità API in 1Password Riferimento all'API Events.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric 1Password account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con 1Password. Per trovare le informazioni necessarie per l'autorizzazione 1Password con AppFabric, attenersi alla seguente procedura.

Crea un account personale 1Password token di accesso

1Password supporta token di accesso personali per clienti pubblici. Completa i seguenti passaggi per generare un token di accesso personale.

1. Accedi al tuo 1Password conto.
2. Scegli Integrazioni nel riquadro di navigazione.
3. Se sono presenti integrazioni esistenti, scegli Directory. In alternativa, passa alla fase successiva.
4. Scegli Altro in Events Reporting Integration.

5. Nella pagina Aggiungi integrazione, inserisci il nome del sistema SIEM (Security Information and Event Management) (ad esempio, AppFabric Sicuro)
6. Scegli Aggiungi integrazione, quindi completa i seguenti passaggi nella pagina di configurazione del token.

    a. Fornisci il nome del token da utilizzare nell'ambiente AppFabric sicuro.
    b. Ti consigliamo di scegliere Mai nell'elenco a discesa Scadenza dopo. Se viene selezionato un altro valore allora 1Password revoca il token allo scadere del tempo di scadenza.
    c. Nella sezione Eventi da segnalare, scegli Tentativi di accesso, Eventi di utilizzo degli articoli ed Eventi di controllo.
7. Scegli Issue Token per creare il token.
8. Scegli Salva in 1Passworde completa i seguenti passaggi.

    a. Il titolo verrà compilato automaticamente in base al sistema e ai nomi dei token.
    b. Scegli Privato in Seleziona un deposito.
    c. Seleziona Salva.

Per ulteriori informazioni, consulta Inizia con 1Password Rapporti sugli eventi su 1Password sito web.

Autorizzazioni dell'app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID inquilino inserito AppFabric sarà il tuo 1Password indirizzo di accesso. Completa i seguenti passaggi per trovare l'ID del tuo inquilino.

1. Accedi al tuo 1Password conto.
2. Scegliere Settings (Impostazioni) nel riquadro di navigazione.
3. Il tuo 1Password l'accesso è elencato nella pagina. Ad esempio, example-account.1password.com.

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco 1Password organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

Token dell'account di servizio

È necessario disporre di un token per l'account di servizio fornito da un 1Password account di servizio da inserire nel AppFabric 1Password autorizzazione dell'app. Se non disponi di un token per l'account di servizio, utilizza le seguenti istruzioni:

AppFabric richiederà un token per l'account di servizio. Il token dell'account di servizio in AppFabric è il token di accesso personale che hai creato. Completa i seguenti passaggi nel portale 1Password per trovare il token di accesso personale.

1. Seleziona Dashboard (Pannello di controllo).
2. Scegli Persone.
3. Scegli il nome del proprietario dell'account.
4. Scegli Privato.
5. Scegli View Vault.
6. Scegli il nome del token.

Autorizzazione del cliente

Crea un'autorizzazione all'app AppFabric utilizzando l'ID tenant, il nome del tenant e il token dell'account di servizio. Quindi scegli Connect per attivare l'autorizzazione.

Configura Asana per AppFabric

Asana è una piattaforma di gestione del lavoro che aiuta individui, team e organizzazioni a orchestrare il lavoro, dalle attività quotidiane alle iniziative strategiche interfunzionali. Fornisce un sistema vivente di chiarezza in cui tutti possono comunicare, collaborare e coordinare il lavoro. Con Asana, i team integrano gli strumenti aziendali fondamentali in un unico posto in modo che il lavoro prosegua indipendentemente da dove si svolge.

È possibile utilizzare a AWS AppFabric fini di sicurezza per controllare i registri e i dati degli utenti da Asana, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Asana

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Asana.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Asana verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un account Enterprise con Asana. Per ulteriori informazioni sulla creazione o l'aggiornamento a un Asana Account aziendale, vedi Asana Enterprise su Asana sito web.
- Devi avere un utente con il ruolo di Super Amministratore nel tuo Asana account. Per ulteriori informazioni sui ruoli, consulta Ruoli di amministratore e super amministratore in Asanasul Asana sito web.

Considerazioni sui limiti di velocità

Asana impone limiti di aliquota al Asana API. Per ulteriori informazioni su Asana Limiti di velocità delle API, consulta Limiti di velocità su Asana Sito Web Developers Guide. Se la combinazione di AppFabric e quella esistente Asana le applicazioni superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Asana account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Asana. Per trovare le informazioni necessarie per l'autorizzazione Asana con AppFabric, attenersi alla seguente procedura.

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID tenant in AppFabric è chiamato ID di dominio in Asana. Per trovare l'ID del dominio, utilizza le seguenti istruzioni fornite da Asana schermata iniziale:

1. Scegli l'immagine del profilo del tuo account e seleziona Admin Console.
2. Quindi seleziona Impostazioni.
3. Scorri fino a Impostazioni del dominio.
4. Inserisci l'ID del dominio da questa sezione nella configurazione del AppFabric Tenant ID.

Nome del tenant

Inserisci un nome che identifichi questo nome univoco Asana organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

Token dell'account di servizio

È necessario disporre di un token per l'account di servizio fornito da un Asana account di servizio da inserire nel AppFabric Asana autorizzazione dell'app. Se non disponi di un token per l'account di servizio, utilizza le seguenti istruzioni:

1. Per creare un account di servizio, segui le istruzioni riportate nella sezione Account di servizio sul Asana Sito web della guida.
2. Copia e salva il token dalla parte inferiore della pagina Aggiungi account di servizio la prima volta che visualizzi la pagina Aggiungi account di servizio.
3. Se si chiude la pagina Aggiungi account di servizio prima di salvare il token, è necessario modificare l'account di servizio, generare un nuovo token e salvarlo.

Configura Azure Monitor per AppFabric

Azure Monitor è una soluzione di monitoraggio completa per la raccolta, l'analisi e la risposta ai dati di monitoraggio provenienti dagli ambienti cloud e locali. È possibile utilizzare… Azure Monitor per massimizzare la disponibilità e le prestazioni delle applicazioni e dei servizi. Consente di comprendere le prestazioni delle applicazioni e di rispondere manualmente e programmaticamente agli eventi di sistema.

Azure Monitor raccoglie e aggrega i dati da ogni livello e componente del sistema in più sottoscrizioni e tenant di Azure e non Azure. Li archivia in una piattaforma di dati comune per essere utilizzati da un set comune di strumenti in grado di correlare, analizzare, visualizzare e/o rispondere ai dati. Puoi anche integrare altri strumenti Microsoft e non Microsoft. Il Azure Monitor activity log è un registro della piattaforma che fornisce informazioni sugli eventi a livello di abbonamento. Il registro delle

attività include informazioni come quando una risorsa viene modificata o viene avviata una macchina virtuale.

È possibile utilizzare, a AWS AppFabric fini di sicurezza, per controllare i log e i dati utente di Azure Monitor, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Azure Monitor

AppFabric è in grado di ricevere informazioni sugli utenti e registri di controllo da quanto segue Azure Monitor servizi:

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

Prerequisiti

Da utilizzare AppFabric per trasferire i registri di controllo da Azure Monitor verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un Microsoft Azure account con una prova gratuita o un pay-as-you-go abbonamento.
- È necessario almeno un abbonamento per recuperare gli eventi inclusi in tale abbonamento.

Considerazioni sui limiti di velocità

Azure Monitor impone limiti di tariffa al responsabile della sicurezza (utente o applicazione) che effettua le richieste e all'ID dell'abbonamento o all'ID del tenant. Per ulteriori informazioni sul Azure Monitor Limiti di velocità delle API, vedi Scopri come Azure Resource Manager limita le richieste su Azure Monitor Sito web per sviluppatori.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Azure Monitor account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Azure Monitor. Per trovare le informazioni necessarie per l'autorizzazione Azure Monitor con AppFabric, attenersi alla seguente procedura.

Crea un' OAuthapplicazione

AppFabric si integra con Azure Monitor utilizzando OAuth2. Completa i seguenti passaggi per creare un' OAuth2 applicazione in Azure Monitor:

1. Passare alla .Microsoft Azure Portale e accesso.
2. Accedere a Microsoft Entra ID.
3. Scegli Registrazioni all'app.
4. Scegli Nuova registrazione.
5. Inserisci un nome per il cliente, ad esempio Azure Monitor OAuthCliente. Questo sarà il nome dell'applicazione registrata.
6. Verifica che i tipi di account supportati siano impostati su Single Tenant.
7. Per l'URI di reindirizzamento, seleziona Web come piattaforma e aggiungi un URI di reindirizzamento. Utilizza il seguente formato per l'URI di reindirizzamento:

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

   In quell'indirizzo, *<region>* c'è il codice del pacchetto Regione AWS in cui hai configurato il pacchetto AppFabric dell'app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`

   La risposta di autenticazione verrà inviata all'URI fornito dopo aver autenticato correttamente l'utente. Fornirlo ora è facoltativo e può essere modificato in seguito, ma è necessario un valore per la maggior parte degli scenari di autenticazione.

8. Scegli Registrati.
9. Nell'app registrata, scegli Certificati e segreti e poi Nuovo segreto del cliente.
10. Aggiungi una descrizione del segreto.
11. Seleziona la durata di scadenza segreta. Puoi selezionare qualsiasi durata preimpostata dal menu a discesa o impostare una durata personalizzata.
12. Scegli Aggiungi. I valori segreti del client possono essere visualizzati solo immediatamente dopo la creazione. Assicurati di salvare il segreto in un posto sicuro prima di lasciare la pagina.

Autorizzazioni richieste

È necessario aggiungere le seguenti autorizzazioni all' OAuth applicazione. Per aggiungere autorizzazioni, segui le istruzioni nella sezione Aggiungi autorizzazioni per accedere alla tua API web del Microsoft Entra Guida per gli sviluppatori.

- Microsoft Graph API di accesso utente > User.Read.All (seleziona il tipo delegato)
- Microsoft Graph API di accesso utente > offline_access (seleziona il tipo delegato)
- Azure API Service Management Audit Log > user_impersonation (seleziona il tipo delegato)

Dopo aver aggiunto le autorizzazioni, per concedere il consenso dell'amministratore per le autorizzazioni, segui le istruzioni nella sezione relativa al pulsante Consenso dell'amministratore del Microsoft Entra Guida per gli sviluppatori.

Autorizzazioni delle app

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo dal Azure Monitor conto. Per ricevere sia i registri di controllo che i dati degli utenti da Azure Monitor, è necessario creare due autorizzazioni per l'app, una denominata Azure Monitornell'elenco a discesa delle autorizzazioni delle app e un'altra denominata Azure Monitor Registri di controllo nell'elenco a discesa delle autorizzazioni dell'app. Puoi utilizzare lo stesso ID tenant, ID client e client secret per entrambe le autorizzazioni dell'app. Per ricevere i registri di controllo da Azure Monitor hai bisogno di entrambi Azure Monitor e Azure Monitor Autorizzazioni dell'app Audit Logs. Per utilizzare solo lo strumento di accesso utente, solo Azure Monitorè richiesta l'autorizzazione dell'app.

ID tenant

AppFabric richiederà il tuo ID inquilino. Completa i seguenti passaggi per trovare il tuo ID cliente in Azure Monitor:

1. Passare alla .Microsoft Azure Portale.
2. Passa ad Azure Active Directory.
3. Nella sezione Registrazioni app, scegli l'app creata in precedenza.
4. Nella sezione Panoramica, copia l'ID del tenant dal campo Directory (tenant) ID.

Nome del tenant

Inserisci un nome che identifichi questo univoco Azure Monitor abbonamento. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

> **Note**
>
> Il nome del tenant deve contenere un massimo di 2.048 caratteri composti da numeri, lettere minuscole e maiuscole e i seguenti caratteri speciali: punto (.), trattino basso (_), trattino (-) e spazio vuoto.

ID client

AppFabric richiederà un ID cliente. Completa la seguente procedura per trovare il tuo ID cliente in Azure Monitor:

1. Passare alla .Microsoft Azure Portale.
2. Passa ad Azure Active Directory.
3. Nella sezione Registrazioni app, scegli l'app creata in precedenza.
4. Nella sezione Panoramica, copia l'ID client dal campo ID dell'applicazione (client).

Client secret

AppFabric richiederà un segreto per il cliente. Il segreto del cliente per l' OAuth app registrata è quello che hai generato nel passaggio 11 della sezione Creazione dell' OAuth app. Se perdi il client secret generato durante la creazione dell' OAuth app, ripeti i passaggi 8-11 nella sezione Creazione dell' OAuth app per rigenerarne uno nuovo.

Autorizzazione dell'app

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da Microsoft Azure per approvare l'autorizzazione. Accedi al tuo account dalla finestra e approva l' AppFabric autorizzazione selezionando Consenti.

Configura Atlassian Confluence per AppFabric

Crea, collabora e organizza tutto il tuo lavoro in un unico posto. Confluence è uno spazio di lavoro in team in cui conoscenza e collaborazione si incontrano. Le pagine dinamiche offrono al team un luogo in cui creare, acquisire e collaborare su qualsiasi progetto o idea. Gli spazi aiutano il team a strutturare, organizzare e condividere il lavoro, in modo che ogni membro del team abbia visibilità sulle conoscenze istituzionali e l'accesso alle informazioni di cui ha bisogno per lavorare al meglio.

È possibile utilizzare AWS AppFabric per motivi di sicurezza la ricezione di registri di controllo e dati utente da Confluence, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Atlassian Confluence

AppFabric supporta la ricezione di registri di controllo da Atlassian Confluence.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Atlassian Confluence verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- Per accedere ai registri di controllo, è necessario disporre di un account standard, premium o aziendale. Per ulteriori informazioni sulla creazione o l'aggiornamento alla versione applicabile Confluence tipo di piano, vedere Confluence Prezzi indicati su Atlassian sito web.
- Per accedere ai registri di controllo, devi disporre delle autorizzazioni di amministratore per il tuo account. Per ulteriori informazioni sui ruoli, consulta Concedere agli utenti le autorizzazioni di amministratore su Atlassian Sito Web di supporto.

Considerazioni sui limiti di velocità

Confluence impone limiti di aliquota al Atlassian Confluence API. Se la combinazione di AppFabric e sei esistente Atlassian Confluence Le applicazioni API superano Atlassian Confluence, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Atlassian Confluence account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Atlassian Confluence. Per trovare le informazioni necessarie per l'autorizzazione Atlassian Confluence con AppFabric, attenersi alla seguente procedura.

Crea un' OAuthapplicazione

AppFabric si integra con Atlassian Confluence utilizzando OAuth. Per creare un' OAuth applicazione in Atlassian Confluence, attenersi alla seguente procedura.

1. Passare alla .Atlassian Console per sviluppatori.
2. Scegli l'icona del tuo profilo in alto a destra e scegli Console per sviluppatori.
3. Accanto a Le mie app, scegli Create, integrazione OAuth 2.0.
4. Scegli Autorizzazioni nel riquadro di navigazione a sinistra e scegli Aggiungi accanto a Confluence API.
5. In Ambiti classici, seleziona Read user (`read:confluence-user`).
6. In Ambiti granulari, seleziona Visualizza i record di controllo (). `read:audit-log:confluence`
7. Scegli Autorizzazione nel riquadro di navigazione a sinistra e scegli Aggiungi accanto a OAuth 2.0 (3LO).
8. Utilizza un URL di reindirizzamento con il seguente formato nella casella di testo URL di callback e scegli Salva modifiche.

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

In questo URL, *<region>* c'è il codice del pacchetto Regione AWS in cui hai configurato il pacchetto AppFabric dell'app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`

Ambiti richiesti

È necessario aggiungere uno dei seguenti ambiti al Atlassian Confluence OAuth applicazione. Per ulteriori informazioni sugli oscilloscopi, consulta le app Scopes for OAuth 2.0 (3LO) e Forge sul Atlassian Sito web per sviluppatori. Usa il cannocchiale classico, se disponibile.

- Ambiti classici:
  - `read:confluence-user`
- Ambiti granulari:
  - `read:audit-log:confluence`

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant inserito è il tuo AppFabric Atlassian Confluence sottodominio dell'istanza. Puoi trovare il tuo Atlassian Confluence sottodominio di istanza nella barra degli indirizzi del browser compreso tra https://e.atlassian.net.

Nome dell'inquilino

Inserisci un nome che identifichi questo nome univoco Atlassian Confluence organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. Per trovare il tuo ID cliente in Atlassian Confluence, utilizza i seguenti passaggi:

1. Passare alla .Atlassian Console per sviluppatori.
2. Scegli l'icona del tuo profilo in alto a destra e scegli Console per sviluppatori, Le mie app.

3. Seleziona l' OAuth applicazione che usi per AppFabric connetterti.
4. Inserisci l'ID client dalla pagina Impostazioni nel campo ID client in AppFabric.

Client secret

AppFabric richiederà un segreto per il cliente. Per trovare il segreto del tuo cliente in Atlassian Confluence, segui i seguenti passaggi:

1. Passare alla .Atlassian Console per sviluppatori.
2. Scegli l'icona del tuo profilo in alto a destra e scegli Console per sviluppatori, Le mie app.
3. Seleziona l' OAuth applicazione che usi per AppFabric connetterti.
4. Inserisci il segreto dalla pagina Impostazioni nel campo Client Secret in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da Atlassian Confluence per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione, scegli consenti.

Configura Atlassian Jira suite per AppFabric

Atlassian libera il potenziale di ogni squadra. Il loro software agile e DevOps agile per la gestione dei servizi IT e della gestione del lavoro aiuta i team a organizzare, discutere e completare il lavoro condiviso. La maggior parte delle aziende Fortune 500 e oltre 240.000 aziende di tutte le dimensioni in tutto il mondo, inclusa la NASA, Kiva, Deutsche Banke Salesforce - affidati a Atlassian soluzioni per aiutare i loro team a lavorare meglio insieme e a fornire risultati di qualità in tempo. Scopri di più su Atlassian prodotti, tra cui Jira Software, Confluence, Jira Service Management, Trello, Bitbuckete Jira Align in Atlassian.

È possibile utilizzare AWS AppFabric per motivi di sicurezza per controllare i registri e i dati utente di Jira suite (diverso da Jira Align), normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

- AppFabric supporto per Jira suite

- Connessione al tuo AppFabric Jira account

AppFabric supporto per Jira suite

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo dal Jira suite, ad eccezione di Jira Align.

Prerequisiti

Da utilizzare AppFabric per trasferire i registri di controllo dal Jira suite verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un Jira Piano standard o superiore. Per ulteriori informazioni sulle funzionalità di Jira piani, vedi Jira software, Jira Gestione dei servizi, Jira Gestione del lavoro e Jira Pagine dei prezzi di Product Discovery.
- Devi avere un utente con il ruolo di amministratore dell'organizzazione nel tuo Jira account. Per ulteriori informazioni sui ruoli, consulta Concedere agli utenti le autorizzazioni di amministratore su Atlassian Sito Web di supporto.

Considerazioni sui limiti di velocità

Il Jira la suite impone limiti di velocità al Jira API. Per ulteriori informazioni su Jira suite Limiti di velocità per le API, vedi Limitazione della velocità su Atlassian Sito Web Developers Guide. Se la combinazione di AppFabric e quella esistente Jira Le applicazioni API superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Jira account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Jira. Per trovare le informazioni necessarie per l'autorizzazione Jira con AppFabric, attenersi alla seguente procedura.

Crea un' OAuth applicazione

AppFabric si integra con Jira suite utilizzando OAuth. Per creare un' OAuth applicazione in Jira, attenersi alla seguente procedura:

1. Passare alla .Atlassian Console per sviluppatori.
2. Accanto a Le mie app, scegli Create, integrazione OAuth 2.0.
3. Assegna un nome alla tua app e scegli Crea.
4. Vai alla sezione Autorizzazione e scegli Aggiungi accanto a OAuth 2.0.
5. Usa un URL con il seguente formato nel campo URL di callback e scegli Salva modifiche.

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

   In questo URL, *<region>* è riportato il codice Regione AWS in cui hai configurato il pacchetto AppFabric dell'app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`
6. Vai alla sezione Impostazioni, copia l'ID cliente e il segreto del cliente e salvalo per utilizzarli per l'autorizzazione dell' AppFabric app.

Ambiti richiesti

È necessario aggiungere i seguenti ambiti al Jira OAuth pagina delle autorizzazioni dell'applicazione:

- In Classic Scopes:
  - Jira API > `read:jira-user`
- Nell'ambito degli ambiti granulari:
  - Jira API > `read:audit-log:jira`
  - Jira API > `read:user:jira`

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant inserito è il tuo AppFabric Jira sottodominio dell'istanza. Puoi trovare il tuo Jira sottodominio di istanza nella barra degli indirizzi del browser compreso tra https://e.atlassian.net.

Nome dell'inquilino

Inserisci un nome che identifichi questo nome univoco Jira server. AppFabricutilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà il tuo ID cliente. Per trovare il tuo ID cliente in Jira, segui i seguenti passaggi:

1. Passare alla .Atlassian Console per sviluppatori.
2. Seleziona l' OAuth applicazione che usi per connetterti AppFabric.
3. Inserisci l'ID client dalla pagina Impostazioni nel campo ID client in AppFabric.

Client secret

AppFabric richiederà il segreto del tuo cliente. Il client secret in AppFabric è il Secret in Jira. Per trovare il tuo segreto in Jira, segui i seguenti passaggi:

1. Passare alla .Atlassian Console per sviluppatori.
2. Seleziona l' OAuth applicazione che usi per connetterti AppFabric.
3. Inserisci il segreto dalla pagina Impostazioni nel campo Client Secret in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app, AppFabric riceverai una finestra pop-up da Jira per approvare l'autorizzazione. Per approvare l' AppFabricautorizzazione, scegli Consenti.

Configura Box per AppFabric

Box è il Content Cloud leader nel settore, un'unica piattaforma che consente alle organizzazioni di gestire l'intero ciclo di vita dei contenuti, lavorare in sicurezza da qualsiasi luogo e integrarsi tra le app. best-of-breed

È possibile utilizzare AWS AppFabric per ricevere registri di controllo e dati utente da Box, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e inviali in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Box

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Box.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Box verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- Per accedere ai registri di controllo, è necessario disporre di un abbonamento a pagamento attivo ai piani Business, Business Plus, Enterprise o Enterprise Plus.
- È necessario disporre di un utente con i privilegi di amministratore.
- È necessario che l'autenticazione a 2 fattori sia abilitata sul Box account per visualizzare e copiare il segreto del client dell'applicazione dalla scheda di configurazione.

Considerazioni sui limiti di velocità

Box impone limiti di aliquota al Box API. Per ulteriori informazioni su Box Limiti di velocità delle API, vedi Limiti di velocità su Box Sito Web Developers Guide. Se la combinazione di AppFabric e quella esistente Box le applicazioni superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

In un evento di verifica, potresti riscontrare un ritardo fino a 30 minuti nella consegna a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo può essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione AppFabric al tuo Box account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi AppFabric autorizzare con Box. Per trovare le informazioni necessarie per l'autorizzazione Box con AppFabric, attenersi alla seguente procedura.

Crea un' OAuth applicazione

AppFabric si integra con Box utilizzando OAuth. Utilizza i seguenti passaggi per creare un' OAuth applicazione in Box, Per ulteriori informazioni, vedere Creazione di un' OAuth app su Box sito web.

1. Effettua il login a Box e vai alla Developer Console.
2. Scegli Crea nuova app.
3. Scegli App personalizzata dall'elenco dei tipi di applicazione. Apparirà un modale per richiedere una selezione per il passaggio successivo.
4. Inserisci il nome e la descrizione dell'app.
5. Scegli Integrazione dall'elenco a discesa Scopo.
    a. Scegli Sicurezza e conformità dall'elenco a discesa Categorie.
    b. Inserisci AWS AppFabric Securein Con quale sistema esterno ti stai integrando? casella di testo.
6. Scegliete Server Authentication (Client Credentials Grant) se desiderate verificare l'identità dell'applicazione con un ID client e un client secret.
7. Scegli Create App (Crea app).
8. Scegli la scheda Configurazione.
9. Nella sezione App Access Level della pagina, scegli App + Enterprise Access.
10. Nella sezione Ambiti applicativi della pagina, scegli Gestisci utenti e Gestisci proprietà aziendali.
11. Seleziona Salva modifiche.

    A Box L'amministratore deve autorizzare l'applicazione all'interno di Box La console di amministrazione prima di poter utilizzare l'applicazione. Completa i seguenti passaggi per richiedere un'autorizzazione.

    a. Scegli la scheda Autorizzazione per la tua applicazione nella Developer Console.
    b. Scegli Rivedi e invia per inviare un'email al tuo Box amministratore aziendale per l'approvazione. Per ulteriori informazioni, vedere Autorizzazione nella Box guida.

    > **Note**
    >
    > È necessario inviare nuovamente l'app se vengono apportate modifiche dopo l'invio.

Ambiti richiesti

Sono richiesti i seguenti ambiti applicativi. Per ulteriori informazioni sugli ambiti, consulta Scopes sul sito Web di documentazione di Box.

- Gestisci le proprietà aziendali () `manage_enterprise_properties`
- Gestisci gli utenti (`manage_managed_users`)

Autorizzazioni delle app

ID tenant

AppFabric richiederà un ID inquilino. L'ID del tenant in AppFabric è il Box ID aziendale. Il Box L'Enterprise ID è disponibile nella console di amministrazione in Account e fatturazione > Informazioni sull'account > Enterprise ID. Per ulteriori informazioni, consulta Enterprise ID nel sito Web della documentazione di Box.

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco Box organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e qualsiasi importazione creata dall'autorizzazione dell'app.

Client ID e client secret

1. Accedi a Box e vai alla Developer Console.
2. Scegli Le mie app nel menu di navigazione.
3. Scegli l' OAuth applicazione che usi per connetterti AppFabric.
4. Scegli la scheda Configurazione.
5. Scorri fino alla sezione Credenziali Oauth 2.0 della pagina.
6. Inserisci l'ID cliente dal tuo ID OAuth cliente nel campo ID cliente in. AppFabric
7. Scegli Fetch Client Secret.
8. Inserisci il segreto del cliente contenuto nel tuo OAuth Client Secret nel campo Client Secret in AppFabric.

Configura Cisco Duo per AppFabric

Cisco Duo protegge dalle violazioni con una suite di gestione degli accessi all'avanguardia che offre solide difese a più livelli e funzionalità innovative che consentono agli utenti legittimi di entrare e tengono lontani i malintenzionati. Per qualsiasi organizzazione preoccupata di subire violazioni e che necessiti di una soluzione rapida, Cisco Duo consente rapidamente una forte sicurezza migliorando al contempo la produttività degli utenti.

È possibile utilizzare AWS AppFabric per motivi di sicurezza per ricevere registri di controllo e dati utente da Cisco Duo, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e inviali in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Cisco Duo

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Cisco Duo.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Cisco Duo verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- Per accedere ai registri di controllo, è necessario disporre di un abbonamento attivo a un'edizione Duo Essentials, Duo Advantage o Duo Premier. In alternativa, possono accedere anche nuovi clienti con una versione di prova di Advantage o Premier. Per ulteriori informazioni sull' Cisco Duo edizioni, vedi Edizioni e prezzi.
- Devi essere un amministratore con ruolo di proprietario per creare o modificare l'API di amministrazione.
- È necessario aggiungere le autorizzazioni «Grant read log resource» per accedere ai log di controllo nell'API di amministrazione.

Considerazioni sui limiti di velocità

Cisco Duo impone limiti di aliquota al Cisco Duo API. Per ulteriori informazioni su Cisco Duo Limiti di velocità delle API, consulta i limiti di velocità in Registri di autenticazione. Se la combinazione di AppFabric e quella esistente Cisco Duo Le applicazioni API superano Cisco Duo, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi. Contatta Cisco Duo se hai bisogno di un aumento del limite di velocità.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connect AppFabric al tuo Cisco Duo account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Cisco Duo. Per trovare le informazioni necessarie per l'autorizzazione Cisco Duo con AppFabric, attenersi alla seguente procedura.

Crea un Cisco Duo Applicazione API di amministrazione

AppFabric si integra con Cisco Duo utilizzando un token di servizio API. Per creare un'applicazione in Cisco Duo, attenersi alla seguente procedura.

- Per creare un Cisco Duo Applicazione API di amministrazione, segui le istruzioni riportate in Primi passaggi della Cisco Duo API di amministrazione.

Autorizzazioni richieste

È necessario aggiungere i seguenti ambiti al Cisco Duo applicazione:

- Concedi il registro di lettura
- Concedi una risorsa di lettura

Autorizzazioni dell'app

ID tenant

AppFabric richiederà un ID inquilino. Puoi trovare l'ID del tenant nel Cisco Duo nome host. Per trovare il nome host in Cisco Duo, segui questi passaggi.

1. Passare alla .Cisco DuoPagina di accesso dell'amministratore e accedi.
2. Vai su Applicazioni, quindi scegli Proteggi un'applicazione.
3. Individua la voce Admin API nell'elenco delle applicazioni, quindi scegli Proteggi all'estrema destra per configurare l'applicazione e ottenere il nome host dell'API.
4. Il nome host dell'API è formattato come`api-`*`<tenant-id>`*`.duosecurity.com`, in cui *`<tenant-id>`* si trova l'ID del tenant.

Nome del tenant

Inserisci un nome che identifichi questo univoco Cisco Duo organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

Token di servizio

AppFabric richiederà un token di servizio. Il token di servizio è una chiave di integrazione separata da due punti e una chiave segreta con il seguente formato.

```
integrationkey:secretkey
```

Per trovare la chiave di integrazione e la chiave segreta in Cisco Duo, utilizza i seguenti passaggi.

1. Passare alla .Cisco DuoPagina di accesso all'amministratore e accedi.
2. Vai su Applicazioni, quindi scegli Proteggi un'applicazione.
3. «Fai clic su Proteggi un'applicazione e individua la voce Admin API nell'elenco delle applicazioni. Fai clic su Proteggi all'estrema destra per configurare l'applicazione. Scorri verso il basso fino alla sezione degli ambiti e aggiungi e. **`Grant read log`** **`Grant read resource`**

Configura Dropbox per AppFabric

Dropbox aiuta la tua organizzazione a lavorare meglio e più rapidamente riunendo i dipendenti, indipendentemente da cosa stiano lavorando, dove lavorino o che tipo di strumenti stiano utilizzando. Consente agli utenti di accelerare l'innovazione e l'efficienza fornendo un modo semplice e sicuro per condividere i contenuti. Dropbox è un posto in cui organizzare la vita e mantenere il lavoro in movimento. Con oltre 700 milioni di utenti registrati in 180 paesi, Dropbox ha la missione di progettare un modo di lavorare più illuminato.

È possibile utilizzare AWS AppFabric per motivi di sicurezza per controllare i registri e i dati utente di Dropbox, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Dropbox

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Dropbox.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Dropbox verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un Dropbox Account aziendale. Per ulteriori informazioni sulla creazione o l'aggiornamento a un Dropbox Account aziendale, vedi Dropbox Affari su Dropbox sito web.
- Devi avere un utente con il ruolo di amministratore del team nel tuo Dropbox account. Per ulteriori informazioni sui ruoli, vedi Come modificare i diritti di amministratore per i Dropbox team di Dropbox Sito web del Centro assistenza.

Considerazioni sui limiti di velocità

Dropbox impone limiti di aliquota al Dropbox API. Per ulteriori informazioni su Dropbox Limiti di velocità delle API, vedi Limiti di velocità su Dropbox Sito Web della Guida alle prestazioni. Se la combinazione di AppFabric e quella esistente Dropbox Le applicazioni API superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Dropbox account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Dropbox. Per trovare le informazioni necessarie per l'autorizzazione Dropbox con AppFabric, attenersi alla seguente procedura.

Crea un' OAuthapplicazione

AppFabric si integra con Dropbox utilizzando OAuth. Per creare un' OAuthapplicazione in Dropbox, attenersi alla seguente procedura:

1. Scegli Crea app nel Dropbox App Console https://www.dropbox.com/developers/nelle app.
2. Nella nuova pagina di configurazione dell'applicazione, scegli Accesso con ambito per l'API.
3. Quindi, seleziona Completo Dropboxper il tipo di accesso.
4. Assegna un nome OAuth all'applicazione, quindi scegli Crea app per completare la configurazione iniziale OAuth dell'applicazione.
5. Nella pagina delle informazioni sull'applicazione, aggiungi un URL di reindirizzamento con il seguente formato nel campo di OAuth2 reindirizzamento URIs .

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

   In questo URL, *<region>* è riportato il codice Regione AWS in cui hai configurato il pacchetto AppFabric dell'app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`
6. Scegli Aggiungi.
7. Copia e salva la chiave dell'app e il segreto dell'app per utilizzarli nell'autorizzazione dell' AppFabric app.
8. Puoi lasciare tutti gli altri campi nella scheda Impostazioni con i valori predefiniti.

Ambiti richiesti

È necessario aggiungere i seguenti ambiti al Dropbox app che utilizza la scheda Autorizzazioni nella schermata delle informazioni sull'app:

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

Scegli Invia dopo aver finito.

Autorizzazioni dell'app

ID tenant

AppFabric richiederà il tuo ID inquilino. Inserisci un valore che identifichi in modo univoco il tuo Dropbox account, ad esempio il nome del team.

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco Dropbox conto. AppFabricutilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. L'ID cliente inserito AppFabric è il tuo Dropbox chiave dell'app. Per trovare il codice dell'app Dropbox, procedi nel seguente modo:

1. Vai al Dropbox App Console https://www.dropbox.com/developers/nelle app.
2. Trova l'app che usi per connetterti AppFabric.
3. Trova la chiave dell'app nella sezione Stato della pagina informativa dell'app.
4. Inserisci la chiave dell'app per il tuo Dropbox app nel campo Client ID in AppFabric.

Client secret

AppFabric richiederà un segreto per il cliente. Il segreto del cliente AppFabric è tuo Dropbox app segreta. Per trovare il tuo Dropbox app secret, segui i seguenti passaggi:

1. Vai al Dropbox App Console https://www.dropbox.com/developers/nelle app.
2. Trova l'app che usi per connetterti AppFabric.
3. Trova il segreto dell'app nella sezione Stato della pagina informativa dell'app.
4. Inserisci il segreto dell'app per il tuo Dropbox app nel campo Client Secret in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da Dropbox per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione, scegli Consenti.

Configura Genesys Cloud per AppFabric

Genesys Cloud crea conversazioni fluide su canali digitali e vocali in un' all-in-oneinterfaccia semplice. Ciò consente alle aziende di offrire esperienze eccezionali a dipendenti e clienti e di sfruttare i vantaggi di implementazioni rapide, complessità ridotta e amministrazione semplice.

È possibile utilizzare For Security AWS AppFabric per ricevere registri di controllo e dati utente da Genesys Cloud, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

- AppFabric supporto per Genesys Cloud
- Connessione al tuo AppFabric Genesys Cloud account

AppFabric supporto per Genesys Cloud

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Genesys Cloud.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Genesys Cloud verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un Genesys Cloud conto.
- È necessario disporre di un utente con il ruolo di amministratore nel Genesys Cloud account.

Considerazioni sui limiti di velocità

Genesys Cloud impone limiti di aliquota al Genesys Cloud API. Per ulteriori informazioni su Genesys Cloud Limiti di velocità delle API, consulta Limiti di velocità su Genesys Cloud Developer sito web.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Genesys Cloud account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Genesys Cloud. Per trovare le informazioni necessarie per l'autorizzazione Genesys Cloud con AppFabric, attenersi alla seguente procedura.

Crea un' OAuthapplicazione

AppFabric si integra con Genesys Cloud utilizzando OAuth. Per creare un' OAuthapplicazione in Genesys Cloud, attenersi alla seguente procedura:

1. Segui le istruzioni riportate nella sezione Crea un OAuth cliente sul Genesys Cloud Sito web del Resource Center.

   Per i tipi di sovvenzione, scegli Code Authorization.
2. Utilizza un URL di reindirizzamento con il seguente formato come URIsreindirizzamento autorizzato.

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

   In questo URL, *<region>* c'è il codice del pacchetto Regione AWS in cui hai configurato il pacchetto AppFabric dell'app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`
3. Seleziona la casella Ambito per visualizzare un elenco di ambiti disponibili per l'app. Seleziona ambito `audits:readonly` e. `users:readonly` Per informazioni sugli ambiti, vedere OAuth Ambiti in Genesys Cloud Centro per sviluppatori.
4. Scegli Save (Salva). Genesys Cloud crea un Client ID e un Client Secret (token).

Ambiti richiesti

È necessario aggiungere i seguenti ambiti al Genesys Cloud OAuthapplicazione:

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

Autorizzazioni dell'app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant inserito è il tuo AppFabric Genesys Cloud nome dell'istanza. Puoi trovare il tuo ID inquilino nella barra degli indirizzi del tuo browser. Ad esempio, `usw2.pure.cloud` è l'ID del tenant nel seguente URL. `https://login.usw2.pure.cloud`

Nome dell'inquilino

Inserisci un nome che identifichi questo nome univoco Genesys Cloud organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. Per trovare il tuo ID cliente in Genesys Cloud, utilizza i seguenti passaggi:

1. Scegli Amministratore.
2. In Integrazioni, scegli OAuth.
3. Scegli il OAuth client per ottenere l'ID cliente.

Client secret

AppFabric richiederà un segreto per il cliente. Per trovare il segreto del tuo cliente in Genesys Cloud, segui i seguenti passaggi:

1. Scegli Amministratore.
2. In Integrazioni, scegli OAuth.
3. Scegli il OAuth client per ottenere il Client Secret.

Configura GitHub per AppFabric

GitHub è una piattaforma e un servizio basato su cloud per lo sviluppo di software e il controllo delle versioni tramite Git, che consente agli sviluppatori di archiviare e gestire il proprio codice. Fornisce il controllo della versione distribuita di Git più il controllo degli accessi, il tracciamento dei bug, le richieste di funzionalità software, la gestione delle attività, l'integrazione continua e i wiki per ogni progetto.

È possibile utilizzare AWS AppFabric per motivi di sicurezza per ricevere registri di controllo e dati utente da GitHub, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per GitHub

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da GitHub.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da GitHub verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- Per accedere ai registri di controllo è necessario disporre di un account aziendale.
- Per accedere ai log di controllo aziendali è necessario avere il ruolo di amministratore per il proprio account aziendale.
- Per ottenere i log di controllo dall'organizzazione, devi essere il proprietario dell'organizzazione.

Considerazioni sui limiti di velocità

GitHub impone limiti di aliquota al GitHub API. Per ulteriori informazioni su GitHub Limiti di velocità delle API, consulta Limiti e allocazioni delle richieste API su GitHub sito web. Se la combinazione di AppFabric e quella esistente GitHub Le applicazioni API superano GitHub’s limiti, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric GitHub account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con GitHub. Per trovare le informazioni necessarie per l'autorizzazione GitHub con AppFabric, attenersi alla seguente procedura.

Crea un' OAuth applicazione

AppFabric si integra con GitHub utilizzando OAuth. Utilizza i seguenti passaggi per creare un' OAuth applicazione in GitHub. Per ulteriori informazioni, consulta Creazione di GitHubs app su GitHub sito Web.

1. Scegli la tua foto del profilo situata nell'angolo in alto a destra della pagina, quindi scegli Impostazioni.
2. Scegli Impostazioni sviluppatore nel riquadro di navigazione a sinistra.
3. Scegli OAuth le app nel riquadro di navigazione a sinistra.
4. Scegli Nuova OAuth app.

> **Note**
>
> Questo pulsante sarà denominato Registra una nuova applicazione se non ne hai mai creata un' OAuthaltra in precedenza.

5. Inserisci il nome della tua app nella casella di testo Nome applicazione.
6. Immettete l'URL completo dell'istanza dell'applicazione nella casella di testo URL della home page.
7. (Facoltativo) Inserisci una descrizione per l'app nella casella di testo Descrizione dell'applicazione. Gli utenti vedranno questa descrizione.
8. Inserisci un URL con il seguente formato nella casella di testo URL di richiamata di autorizzazione.

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

In questo URL, *<region>* è riportato il codice Regione AWS in cui hai configurato il pacchetto di AppFabric app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`

9. Scegli Abilita Device Flow se la tua OAuth app utilizzerà Device Flow per identificare e autorizzare gli utenti. Per ulteriori informazioni sul flusso dei dispositivi, consulta Autorizzazione delle OAuth app su GitHub sito web.
10. Scegli Registra applicazione.

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant deve essere fornito in uno dei seguenti formati:

Registro di controllo aziendale:

Utilizza il registro di controllo aziendale se desideri conoscere le azioni aggregate di tutte le organizzazioni di proprietà del tuo account aziendale.

Per utilizzare il registro di controllo aziendale, l'ID tenant è l'ID aziendale del tuo account. Puoi trovare il tuo ID aziendale nella barra degli indirizzi del browser. Ad esempio, *exampleenterprise* è l'ID aziendale nel seguente URL`https://github.com/settings/enterprises/`*`examplenterprise`*.

Quando si specifica l'ID tenant per il registro di controllo aziendale, è necessario prefissarlo con. `enterprise:` Pertanto, specificate l'esempio precedente come. `enterprise:examplenterprise`

Registro di controllo dell'organizzazione:

Utilizza il registro di controllo dell'organizzazione come amministratore dell'organizzazione se desideri conoscere le azioni eseguite dai membri della tua organizzazione. Include dettagli come chi ha eseguito l'azione, qual è stata l'azione e quando è stata eseguita.

Per utilizzare il registro di controllo dell'organizzazione, l'ID tenant è l'ID dell'organizzazione. Puoi trovare l'ID della tua organizzazione nella barra degli indirizzi del browser. Ad esempio,

exampleorganization è l'ID dell'organizzazione nel seguente URL`https://github.com/settings/organizations/`*exampleorganization*.

Quando si specifica l'ID tenant per il registro di controllo dell'organizzazione, è necessario prefissarlo con. `organization:` Pertanto, specificate l'esempio precedente come. `organization:exampleorganization`

Nome dell'inquilino

Inserisci un nome che identifichi questo nome univoco GitHub impresa o organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. Utilizza i seguenti passaggi per trovare il tuo ID cliente in GitHub,

1. Scegli la tua foto del profilo situata nell'angolo in alto a destra della pagina, quindi scegli Impostazioni.
2. Scegli Impostazioni sviluppatore nel riquadro di navigazione a sinistra.
3. Scegli OAuth le app nel riquadro di navigazione a sinistra.
4. Scegli l' OAuth app specifica, quindi cerca il valore del Client ID.

Client secret

AppFabric richiederà un segreto per il cliente. Segui i seguenti passaggi per trovare il segreto del tuo cliente in GitHub.

1. Scegli la foto del tuo profilo che si trova nell'angolo in alto a destra della pagina, quindi scegli Impostazioni.
2. Scegli Impostazioni sviluppatore nel riquadro di navigazione a sinistra.
3. Scegli OAuth le app nel riquadro di navigazione a sinistra.
4. Scegli l' OAuth app specifica, quindi cerca il valore Client Secret. Se non riesci a trovare un client secret esistente, potrebbe essere necessario generarne uno nuovo.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da GitHub per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione, scegli Consenti.

Assicurati che le tue organizzazioni abbiano concesso l'accesso all' OAuth app, se le restrizioni di accesso all'OAuth app sono abilitate.

Configura Google Analytics per AppFabric

Google Analytics è un servizio di analisi web che fornisce statistiche e strumenti analitici di base per l'ottimizzazione dei motori di ricerca (SEO) e scopi di marketing. Google Analytics viene utilizzato per monitorare le prestazioni del sito Web e raccogliere informazioni sui visitatori. Può aiutare le organizzazioni a determinare le principali fonti di traffico degli utenti, valutare il successo delle loro attività e campagne di marketing, tenere traccia del raggiungimento degli obiettivi (ad esempio acquisti, aggiunta di prodotti al carrello), scoprire modelli e tendenze del coinvolgimento degli utenti e ottenere altre informazioni sui visitatori, come i dati demografici. I siti web di vendita al dettaglio di piccole e medie dimensioni spesso utilizzano Google Analytics per ottenere e analizzare varie analisi del comportamento dei clienti, che possono essere utilizzate per migliorare le campagne di marketing, indirizzare il traffico del sito Web e fidelizzare meglio i visitatori.

È possibile utilizzare, a AWS AppFabric fini di sicurezza, per controllare i registri e i dati utente di Azure Monitor, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e inviali in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

- AppFabric supporto per Google Analytics
- Connessione al tuo AppFabric Google Analytics account

AppFabric supporto per Google Analytics

AppFabric supporta la ricezione di registri di controllo da Google Analytics.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Google Analytics verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario essere l'amministratore di Google Analytics conto.
- AppFabric Per recapitare i log, è necessario abilitare Google Analytics API di amministrazione sul tuo Google Cloud progetto. Assicurati di utilizzare un nuovo progetto durante la configurazione di Google Analytics OAuth applicazione.

Considerazioni sui limiti di velocità

Google Analytics impone limiti di aliquota al Google Analytics API. Per ulteriori informazioni sull' Google Analytics Limiti di velocità delle API, vedi Limiti e quote sul sito web di Google Analytics. Se la combinazione delle applicazioni API di Google Analytics esistenti AppFabric e quelle esistenti superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Google Analytics account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Google Analytics. Utilizza i seguenti passaggi per trovare le informazioni necessarie per l'autorizzazione Google Analytics con AppFabric.

Creare un' OAuthapplicazione

AppFabric si integra con Google Analytics utilizzando OAuth. Completa i seguenti passaggi per creare un' OAuth applicazione in Google Analytics:

1. Per configurare la schermata di OAuth consenso, segui le istruzioni in Configurare la schermata di OAuth consenso nella Google Developer Guide sul sito web di Google.
2. Scegli Esterno per il tipo di utente
3. Per configurare OAuth le credenziali per AppFabric, segui le istruzioni nella sezione Credenziali ID OAuth client della pagina Crea credenziali di accesso nella Google Developer Guide.
4. Utilizza un URL di reindirizzamento con il seguente formato.

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

   In quell'indirizzo, *<region>* c'è il codice del pacchetto Regione AWS in cui hai configurato il pacchetto di AppFabric app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`

Ambiti richiesti

È necessario aggiungere il seguente ambito al Google Analytics OAuthapplicazione:

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

Autorizzazioni dell'app

ID tenant

AppFabric richiederà un ID inquilino. L'ID del tenant inserito è il tuo AppFabric Google Analytics ID dell'account.

1. Vai al Google Analytics pagina iniziale.
2. Scegli Amministratore nel riquadro di navigazione.
3. Troverai l'ID del tuo account in Account > Impostazioni account > Dettagli account > ID account.

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco Google Analytics organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. Utilizza i seguenti passaggi per trovare il tuo ID cliente in Google Analytics:

1. Vai alla pagina Credenziali.
2. Nella IDs sezione Client OAuth 2.0, scegli l'ID client che hai creato.
3. L'ID client è elencato nella sezione Informazioni aggiuntive della pagina.

Client secret

AppFabric richiederà un segreto per il cliente. Segui i seguenti passaggi per trovare il segreto del tuo cliente in Google Analytics:

1. Vai alla pagina Credenziali.

2. Nella IDs sezione Client OAuth 2.0, scegli il nome del client.
3. Il segreto del client è elencato nella sezione Client secret della pagina.

Autorizzazione dell'app

Dopo aver creato l'autorizzazione dell'app AppFabric , riceverai una finestra pop-up da Google Analytics per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione selezionando Consenti.

Configura Google Workspace per AppFabric

Google Workspace è una raccolta di strumenti, software e prodotti per il cloud computing, la produttività e la collaborazione sviluppati e commercializzati da Google.

È possibile utilizzare a AWS AppFabric fini di sicurezza per controllare i registri e i dati utente di Google Workspace, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Google Workspace

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Google Workspace.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Google Workspace verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario abbonarsi al Google Workspace Piano Enterprise Standard. Per ulteriori informazioni sulla creazione o l'aggiornamento a Google Workspace Piano Enterprise Standard, consulta il Google WorkspaceSito web Plans.
- Devi avere un utente con il ruolo di amministratore nel tuo Google Workspace.

- AppFabric Per fornire i log, devi abilitare l'API Google Admin SDK sul tuo progetto Google Cloud. Per ulteriori informazioni, consulta Abilitare Google Workspace APIs nel Google Workspace Guida per gli sviluppatori.

Considerazioni sui limiti di velocità

Google Workspace impone limiti di aliquota al Google Workspace API. Per ulteriori informazioni sull' Google Workspace Limiti di velocità delle API, vedi Limiti e quote sul Google Workspace Guida per amministratori su Google Workspace sito web. Se la combinazione di AppFabric e quella esistente Google Workspace Le applicazioni API superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti per la maggior parte degli eventi di controllo e fino a 4 ore per la consegna a destinazione di determinati eventi di controllo. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Per ulteriori informazioni, consulta Conservazione dei dati e tempi di ritardo nel sito Web di assistenza per gli WorkSpace amministratori di Google. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contatta. Supporto

Connessione AppFabric al tuo Google Workspace account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Google Workspace. Per trovare le informazioni necessarie per l'autorizzazione Google Workspace con AppFabric, attenersi alla seguente procedura.

Crea un' OAuthapplicazione

AppFabric si integra con Google Workspace utilizzando OAuth. Per creare un' OAuth applicazione in Google Workspace, attenersi alla seguente procedura:

1. Per configurare la schermata di OAuth consenso, segui le istruzioni in Configurare la schermata di OAuth consenso nel Google Workspace Guida per gli sviluppatori su Google Workspace sito web.

   Scegli Interno per il tipo di utente.
2. Per configurare OAuth le credenziali per AppFabric, segui le istruzioni nella sezione Credenziali ID OAuth client della pagina Crea credenziali di accesso nel Google Workspace Guida per gli sviluppatori.

3. Utilizza un URL di reindirizzamento con il seguente formato.

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

   In questo URL, *<region>* è il codice Regione AWS in cui hai configurato il pacchetto di AppFabric app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`

Ambiti richiesti

È necessario aggiungere i seguenti ambiti al Google Workspace OAuthapplicazione:

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

Se non vedi questi ambiti, aggiungi l'API Admin SDK al tuo Google Libreria di API cloud.

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant inserito è il tuo AppFabric Google Workspace ID del progetto. Per trovare l'ID del progetto, consulta Individuare l'ID del progetto sul Google Sito web di assistenza di API Console.

Nome del tenant

Inserisci un nome che identifichi questo univoco Google Workspace. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà il tuo ID cliente. Per trovare il tuo ID cliente, procedi nel seguente modo:

1. Trova il tuo ID cliente utilizzando le informazioni nella sezione Visualizza credenziali della pagina Gestisci le credenziali nel Google Workspace Guida per gli sviluppatori.
2. Inserisci l'ID cliente OAuth del tuo cliente nel campo ID cliente in AppFabric.

Client secret

AppFabric richiederà il segreto del tuo cliente. Per trovare il segreto del tuo cliente, procedi nel seguente modo:

1. Trova il segreto del tuo client utilizzando le informazioni nella sezione Visualizza credenziali della pagina Gestisci le credenziali sul Google Workspace Guida per gli sviluppatori.
2. Se devi reimpostare il segreto del tuo client, utilizza le istruzioni nella sezione Reimposta segreto del client della pagina Gestisci le credenziali sul Google Workspace Guida per gli sviluppatori.
3. Inserisci il segreto del tuo cliente nel campo Segreto del cliente in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app, AppFabric riceverai una finestra pop-up da Google Workspace per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione, scegli consenti.

Configura HubSpot per AppFabric

HubSpot è una piattaforma per i clienti con tutto il software, le integrazioni e le risorse necessarie per collegare marketing, vendite, gestione dei contenuti e assistenza clienti. HubSpotti consente di far crescere la tua attività più velocemente concentrandoti su ciò che conta di più: i tuoi clienti.

È possibile utilizzare AWS AppFabric per motivi di sicurezza per ricevere registri di controllo e dati utente da HubSpot, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

- AppFabric supporto per HubSpot
- Connessione al tuo AppFabric HubSpot account

AppFabric supporto per HubSpot

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da HubSpot.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da HubSpot verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un account con abbonamento Enterprise in HubSpot per accedere ai log di controllo degli accessi. Per ulteriori informazioni sull' HubSpot abbonamenti, vedi Gestisci i tuoi HubSpot abbonamento su HubSpot Base di conoscenza.
- È necessario disporre di un account sviluppatore e di un'app associata all'account.
- Devi essere un super amministratore per installare app nel tuo HubSpot account o disponi dell'autorizzazione di accesso all'App Marketplace più le autorizzazioni utente per accettare gli ambiti richiesti dall'app.

Considerazioni sui limiti di velocità

HubSpot impone limiti di aliquota al HubSpot API. Per ulteriori informazioni su HubSpot Limiti di velocità delle API, inclusi i limiti per l'utilizzo delle app OAuth, consulta Rate Limits su HubSpot sito web. Se la combinazione di AppFabric e quella esistente HubSpot Le applicazioni API superano HubSpot, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric HubSpot account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con HubSpot. Per trovare le informazioni necessarie per l'autorizzazione HubSpot con AppFabric, attenersi alla seguente procedura.

Crea un' OAuthapplicazione

AppFabric si integra con HubSpot utilizzando OAuth. Per creare un' OAuthapplicazione in HubSpot, attenersi alla seguente procedura:

1. Segui le istruzioni nella sezione Creare un'app pubblica del HubSpot guida su HubSpot sito web.

2. Dalla scheda Auth, aggiungi i tre ambiti elencati in. Ambiti richiesti
3. Utilizza un URL di reindirizzamento con il seguente formato in Redirect URL.

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

   In questo URL, *<region>* c'è il codice per il pacchetto Regione AWS in cui hai configurato il pacchetto AppFabric dell'app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`
4. Scegli Crea app.

Ambiti richiesti

È necessario aggiungere i seguenti ambiti al HubSpot OAuthapplicazione:

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

Autorizzazioni dell'app

ID tenant

Inserisci un ID che identifichi questo codice univoco HubSpot organizzazione. Ad esempio, inserisci il tuo HubSpot ID dell'account.

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco HubSpot organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. Per trovare il tuo ID cliente in HubSpot, utilizza i seguenti passaggi:

1. Passare alla .HubSpot pagina di accesso e accedi utilizzando le credenziali del tuo account sviluppatore.

2. Dal menu App, scegli la tua app.
3. Nella scheda Auth, cerca il valore Client ID.

Client secret

AppFabric richiederà un segreto per il cliente. Per trovare il segreto del tuo cliente in HubSpot, segui i seguenti passaggi:

1. Passare alla .HubSpot pagina di accesso e accedi utilizzando le credenziali del tuo account sviluppatore.
2. Dal menu App, scegli la tua app.
3. Nella scheda Auth, cerca il valore segreto del client.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da HubSpot per approvare l'autorizzazione. Accedi al tuo account utilizzando le credenziali del tuo account aziendale (non il tuo account sviluppatore) per approvare l'autorizzazione. AppFabric Scegli consenti.

Configura IBM Security® Verify per AppFabric

Il IBM Security® Verify La famiglia offre funzionalità automatizzate, basate sul cloud e locali per amministrare la governance delle identità, gestire l'identità e l'accesso della forza lavoro e dei consumatori e controllare gli account privilegiati. Sia che tu debba implementare una soluzione cloud o locale, IBM Security® Verify ti aiuta a creare fiducia e a proteggerti dalle minacce interne sia per la forza lavoro che per i consumatori.

Puoi utilizzare AWS AppFabric for security per ricevere registri di controllo e dati utente da IBM Security® Verify, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

- AppFabric supporto per IBM Security® Verify
- Connessione AppFabric al tuo IBM Security® Verify account

AppFabric supporto per IBM Security® Verify

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da IBM Security® Verify.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da IBM Security® Verify verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- Per accedere ai log di controllo, è necessario disporre di un IBM Security® Verify Account SaaS.
- Per accedere ai log di controllo, è necessario disporre di un ruolo di amministratore IBM Security® Verify Account SaaS.

Considerazioni sui limiti di velocità

IBM Security® Verify impone limiti di aliquota al IBM Security® Verify API. Per ulteriori informazioni su IBM Security® Verify Limiti di velocità delle API, consulta IBM Terms. Se la combinazione di AppFabric e quella esistente IBM Security® Verify Le applicazioni API superano IBM Security® Verify limiti, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti in un evento di verifica prima che la consegna a destinazione venga effettuata. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo può essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione AppFabric al tuo IBM Security® Verify account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con IBM Security® Verify. Per trovare le informazioni necessarie per l'autorizzazione IBM Security® Verify con AppFabric, attenersi alla seguente procedura.

Crea un' OAuthapplicazione

AppFabric si integra con IBM Security® Verify utilizzando OAuth. Per creare un' OAuth applicazione in IBM Security® Verify, consulta Creare un client API sul sito Web di documentazione IBM.

1. Per il primo accesso, utilizza l'URL di accesso e le credenziali che sono state inviate al tuo indirizzo email registrato.

2. Accedi alla console di amministrazione all'indirizzo. `https://<hostname>.verify.ibm.com/ui/admin/` Per ulteriori informazioni, vedere Accesso IBM Security® Verify.
3. Nella console di amministrazione, in Sicurezza < Accesso API < Client API, scegli Aggiungi.
4. Seleziona le seguenti opzioni. Sono necessari per leggere il registro di controllo e i dettagli dell'utente.
   - Leggi i report
   - Lettura di utenti e gruppi
5. Mantieni l'opzione predefinita nel metodo di autenticazione del client.

   Non modificare il campo Ambiti personalizzati.
6. Scegli Next (Successivo).
7. Non modificare il campo del filtro IP.
8. Scegli Next (Successivo).
9. Non modificare il campo Proprietà aggiuntive.
10. Scegli Next (Successivo).
11. Specificare un nome e una descrizione. La descrizione è facoltativa.
12. Scegli Crea client API.

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. È possibile individuare l'ID del tenant nel IBM Security® Verify URL standard. Ad esempio, nell'`https://hostname.verify.ibm.com`/URL, l'ID del tenant è *hostname* quello che può essere trovato prima `.verify.ibm.com` (o prima `ice.ibmcloud.com` se si utilizza un nome host precedente). Se utilizzi un vanity URL, contatta il IBM Security® Verify team di supporto per ottenere il tuo URL standard.

Nome dell'inquilino

Inserisci un nome che identifichi questo nome univoco IBM Security® Verify inquilino. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e qualsiasi importazione creata dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. Per trovare il tuo ID cliente in IBM Security® Verify, utilizza i seguenti passaggi:

1. Per il primo accesso, utilizza l'URL di accesso e le credenziali che sono state inviate al tuo indirizzo email registrato.
2. Accedi alla console di amministrazione all'indirizzo. `https://<hostname>.verify.ibm.com/ui/admin/` Per ulteriori informazioni, vedere Accesso IBM Security® Verify.
3. Nella console di amministrazione, in Sicurezza < Accesso API < API Client, scegli i puntini di sospensione (⋮) accanto all'app specifica OAuth .
4. Scegli Dettagli di connessione.
5. Individua l'ID client nelle credenziali API.

Client secret

AppFabric richiederà un segreto per il cliente. Per trovare il segreto del tuo cliente in IBM Security® Verify, segui i seguenti passaggi:

1. Per il primo accesso, utilizza l'URL di accesso e le credenziali che sono state inviate al tuo indirizzo email registrato.
2. Accedi alla console di amministrazione all'indirizzo. `https://<hostname>.verify.ibm.com/ui/admin/` Per ulteriori informazioni, vedere Accesso IBM Security® Verify.
3. Nella console di amministrazione, in Sicurezza < Accesso API < API Client, scegli i puntini di sospensione (⋮) accanto all'app specifica OAuth .
4. Scegli Dettagli di connessione.
5. Individua il segreto del client nelle credenziali API.

Configura JumpCloud per AppFabric

JumpCloud Inc. è una società americana di software aziendale che fornisce una piattaforma di directory basata su cloud per la gestione delle identità. Centralizza e semplifica la gestione delle identità, consentendo agli utenti di accedere in modo sicuro ai propri sistemi, app, reti e file server

con un unico set di credenziali, indipendentemente dalla piattaforma, dal protocollo, dal provider o dalla posizione.

Puoi utilizzarlo AWS AppFabric per ricevere log di controllo e dati utente da JumpCloud, normalizzare i dati in formato Open Cybersecurity Schema Framework (OCSF) e inviarli a un bucket Amazon Simple Storage Service (Amazon S3) o a un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per JumpCloud

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da JumpCloud.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da JumpCloud verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- Devi avere un account a pagamento attivo JumpCloud piano di abbonamento. Per ulteriori informazioni, consulta Select a package that's right for yousul JumpCloud sito web.
- Devi avere il ruolo «Amministratori con fatturazione».

Considerazioni sui limiti di velocità

JumpCloud non pubblica limiti di velocità. È necessario creare una richiesta di supporto o contattare il JumpCloud Team clienti. Se la combinazione di AppFabric e quella esistente JumpCloud Le applicazioni API superano JumpCloud's limiti, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto ai ritardi negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric JumpCloud account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con JumpCloud. Per trovare le informazioni necessarie per l'autorizzazione JumpCloud con AppFabric, segui i passaggi indicati nella sezione successiva.

Crea un token dell'organizzazione dal JumpCloud account

AppFabric utilizza una chiave API per l'integrazione con JumpCloud Per creare una chiave API JumpCloud, segui questi passaggi:.

1. Accedi al tuo JumpCloudaccount come amministratore.
2. Nel portale di amministrazione, scegli le iniziali del tuo account, in alto a destra, e scegli La mia chiave API dal menu.
3. Scegli Genera nuova chiave API o seleziona una chiave esistente.

> **Note**
>
> JumpCloud consente solo una chiave API attiva. La generazione di una nuova chiave API revocherà l'accesso alla chiave API corrente. Ciò renderà inaccessibili tutte le chiamate che utilizzano la chiave API precedente. Dovrai aggiornare tutte le integrazioni esistenti che utilizzano la chiave API precedente con il nuovo valore della chiave.

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. Qui «Organization Id» sarà l'ID del tenant. Per trovare l' «ID dell'organizzazione», segui questi passaggi.

1. Accedi al tuo JumpCloud conto.
2. Nel riquadro di navigazione, scegli Impostazioni, quindi Profilo dell'organizzazione, quindi Generale.
3. Scegli l'icona «occhio» per rimuovere la vista oscurata.
4. Scegli l'icona «doppia pagina» per copiare l'ID.

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco JumpCloud organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

Token dell'account di servizio

AppFabric richiederà il token del tuo account di servizio. In AppFabric, si tratta del token API dell'organizzazione creato in Crea un token dell'organizzazione dal JumpCloud account precedenza in questo argomento.

Configura Microsoft 365 per AppFabric

Microsoft 365 è una famiglia di prodotti di software di produttività, collaborazione e servizi basati su cloud di proprietà di Microsoft.

È possibile utilizzare a fini di sicurezza AWS AppFabric per controllare i registri e i dati degli utenti da Microsoft 365, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e inviali in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

- AppFabric supporto per Microsoft 365
- Connessione al tuo AppFabric Microsoft Account 365

AppFabric supporto per Microsoft 365

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Microsoft 365.

Prerequisiti

Da utilizzare AppFabric per trasferire i registri di controllo da Microsoft 365 verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario abbonarsi a un Microsoft Piano 365 Enterprise. Per ulteriori informazioni sulla creazione o l'aggiornamento a un Microsoft Piano 365 Enterprise, vedi Microsoft Piani 365 Enterprise su Microsoft sito web.
- Devi avere un utente con autorizzazioni di amministratore nel tuo Microsoft Account 365.
- È necessario attivare la registrazione di controllo per la propria organizzazione. Per ulteriori informazioni, consulta Attivare o disattivare il controllo su Microsoft sito Web.

Considerazioni sui limiti di velocità

Microsoft 365 impone limiti di aliquota al Microsoft 365 API. Per ulteriori informazioni sull' Microsoft Limiti di velocità API 365, vedi Microsoft Rappresenta i limiti di limitazione specifici del servizio nel Microsoft Documentazione grafica su Microsoft sito web. Se la combinazione di AppFabric e quella esistente Microsoft Le applicazioni 365 API superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Microsoft Account 365

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Microsoft 365. Per trovare le informazioni necessarie per l'autorizzazione Microsoft 365 con AppFabric, usa i seguenti passaggi.

Crea un' OAuthapplicazione

AppFabric si integra con Microsoft 365 utilizzando OAuth. Per creare un' OAuthapplicazione in Microsoft 365, segui i seguenti passaggi:

1. Segui le istruzioni nella sezione Registrare un'applicazione nella Guida per gli sviluppatori di Azure Active Directory sul Microsoft sito web.

   Scegli Account in questa directory organizzativa solo nella configurazione dei tipi di account supportati.
2. Segui le istruzioni nella sezione Aggiungi un URI di reindirizzamento nella Guida per sviluppatori di Azure Active Directory.

   Scegli la piattaforma Web.

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

   In questo URL, *<region>* è presente il codice Regione AWS in cui hai configurato il pacchetto di AppFabric app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia

settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`

È possibile ignorare gli altri campi di input per la piattaforma Web.

3. Segui le istruzioni nella sezione Aggiungi un client segreto della Guida per sviluppatori di Azure Active Directory.

Autorizzazioni richieste

È necessario aggiungere le seguenti autorizzazioni all'applicazione OAuth . Per aggiungere le autorizzazioni, segui le istruzioni nella sezione Aggiungere le autorizzazioni per accedere all'API Web della Guida per gli sviluppatori di Azure Active Directory.

- `Microsoft Graph API>` `User.Read` (aggiunto automaticamente)
- `Office 365 Management APIs>` `ActivityFeed.Read` (Seleziona il tipo delegato)
- `Office 365 Management APIs>` `ActivityFeed.ReadDlp` (Seleziona il tipo delegato)
- `Office 365 Management APIs>` `ServiceHealth.Read` (Seleziona il tipo delegato)

Dopo aver aggiunto le autorizzazioni, per concedere il consenso dell'amministratore per le autorizzazioni, segui le istruzioni nella sezione relativa al pulsante di consenso dell'amministratore della Guida per gli sviluppatori di Azure Active Directory.

Autorizzazioni delle app

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo dal tuo Microsoft Account 365. Per ricevere sia i registri di controllo che i dati degli utenti da Microsoft 365, devi creare due autorizzazioni per l'app, una denominata Microsoft 365 nell'elenco a discesa delle autorizzazioni dell'app e un'altra denominata Microsoft 365 Audit Log nell'elenco a discesa delle autorizzazioni dell'app. Puoi utilizzare lo stesso ID tenant, ID client e client secret per entrambe le autorizzazioni dell'app. Per ricevere i registri di controllo da Microsoft 365, sono necessari entrambi i Microsoft 365 e Microsoft Autorizzazioni dell'app 365 Audit Log. Per utilizzare solo lo strumento di accesso utente, solo il Microsoft È richiesta l'autorizzazione dell'app 365.

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant in AppFabric è l'ID del tenant di Azure Active Directory. Per trovare l'ID del tenant di Azure Active Directory, vedi Come trovare l'ID del tenant di Azure Active Directory nella documentazione del prodotto Azure sul Microsoft sito web.

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco Microsoft Account 365. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà il tuo ID cliente. L'ID cliente in AppFabric è il Microsoft ID dell'applicazione 365 (client). Per trovare il tuo Microsoft ID dell'applicazione 365 (client), procedi nel seguente modo:

1. Apri la pagina di panoramica dell' OAuth applicazione con cui utilizzi AppFabric.
2. L'ID dell'applicazione (client) viene visualizzato in Essentials.
3. Inserisci l'ID dell'applicazione (client) OAuth del tuo cliente nel AppFabric campo ID cliente di.

Client secret

AppFabric richiederà il segreto del tuo cliente. Microsoft 365 fornisce questo valore solo quando crei inizialmente il client secret per la tua OAuth applicazione. Per generare un nuovo client secret, se non ne possiedi uno, segui i seguenti passaggi:

1. Per creare un client secret, segui le istruzioni nella sezione Aggiungere un client secret della Guida per sviluppatori di Azure Active Directory.
2. Immettere il contenuto del campo Valore nel campo segreto del cliente in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da Microsoft 365 per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione, scegli consenti.

Configura Miro per AppFabric

Miro è uno spazio di lavoro online per l'innovazione che consente a team distribuiti di qualsiasi dimensione di creare la prossima grande novità. L'area di lavoro infinita della piattaforma consente ai team di condurre workshop e riunioni coinvolgenti, progettare prodotti, scambiare idee e altro ancora. Miro, con sede centrale a San Francisco e Amsterdam, serve più di 50 milioni di utenti in tutto il mondo, incluso il 99% delle aziende Fortune 100. Miro è stata fondata nel 2011 e attualmente conta più di 1.500 dipendenti in 12 hub in tutto il mondo. Per saperne di più, visita Miro.

Miro include una suite completa di funzionalità collaborative progettate per l'innovazione, tra cui diagrammi, wireframing, visualizzazione dei dati in tempo reale, facilitazione dei workshop e supporto integrato per pratiche agili, workshop e presentazioni interattive. Miro annunciato di recente Miro AI che si estende Miro, con mappatura e diagrammi basati sull'intelligenza artificiale, raggruppamento e riepilogo e generazione di contenuti. Miro consente alle organizzazioni di ridurre il numero di strumenti autonomi, riducendo la frammentazione delle informazioni e i costi.

È possibile utilizzare a fini di sicurezza AWS AppFabric per controllare i registri e i dati degli utenti da Miro, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e inviali in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Miro

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Miro.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Miro verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un Miro Piano aziendale. Per ulteriori informazioni sui tipi di piano Miro, consulta il Miropagina dei prezzi sul Miro sito web.
- Devi avere un utente con il ruolo di amministratore aziendale nel tuo Miro account. Per ulteriori informazioni sui ruoli, consultate la sezione A livello aziendale di Ruoli in Miro sul sito Web del Centro assistenza di Miro.
- Devi avere un team di Enterprise Developer nel tuo Miro account. Per informazioni sulla creazione di team di sviluppatori, consultate Enterprise Developer teams sul sito Web del Centro assistenza Miro.

Considerazioni sui limiti di velocità

Miro impone limiti di aliquota al Miro API. Per ulteriori informazioni su Miro Limiti di velocità delle API, vedi Rate Limiting nel Miro Guida per gli sviluppatori su Miro sito web. Se la combinazione di

AppFabric e quella esistente Miro Le applicazioni API superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Miro account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Miro. Per trovare le informazioni necessarie per l'autorizzazione Miro con AppFabric, attenersi alla seguente procedura.

Crea un' OAuth applicazione

AppFabric si integra con Miro utilizzando OAuth. Per creare un' OAuthapplicazione in Miro, attenersi alla seguente procedura:

1. Per creare un' OAuth applicazione, seguite le istruzioni nella sezione Creazione e installazione di app dell'articolo dei team di Enterprise Developer sul sito Web di Miro Help Center.
2. Nella finestra di dialogo per la creazione dell'app, selezionate la casella di controllo Expire user Authorization Token dopo aver selezionato un team di sviluppatori nell'organizzazione aziendale.

   > **Note**
   >
   > È necessario eseguire questa operazione prima di creare l'app perché non è possibile modificare questa opzione dopo aver creato l'app.

3. Nella pagina dell'app, inserisci un URL con il seguente formato nella sezione Redirect URI for OAuth 2.0.

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

   In questo URL, *<region>* è riportato il codice Regione AWS in cui hai configurato il pacchetto AppFabric dell'app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`

4. Copia e salva l'ID cliente e il segreto del cliente da utilizzare nell'autorizzazione dell' AppFabric app.

Ambiti richiesti

È necessario aggiungere i seguenti ambiti nella `Permissions` sezione del Miro OAuth pagina dell'app:

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

Autorizzazioni dell'app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant inserito è il tuo AppFabric Miro ID del team. Per informazioni su come trovare il tuo Miro Team ID, consulta la sezione Domande frequenti di I am a new Miro Amministratore. Da dove iniziare? sul Miro Sito web del Centro assistenza.

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco Miro organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà il tuo ID cliente. Per trovare il tuo ID cliente, procedi nel seguente modo:

1. Vai al tuo Miro impostazioni del profilo.
2. Seleziona la scheda Le tue app.
3. Seleziona l'app con cui ti connetti AppFabric.
4. Inserisci l'ID client dalla sezione Credenziali dell'app nel campo ID client in AppFabric.

Client secret

AppFabric richiederà il segreto del tuo cliente. Per trovare il segreto del tuo cliente, procedi nel seguente modo:

1. Vai al tuo Miro impostazioni del profilo.
2. Seleziona la scheda Le tue app.
3. Seleziona l'app con cui ti connetti AppFabric.
4. Inserisci il segreto del client dalla sezione Credenziali dell'app nel campo Segreto del client in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da Miro per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione, scegli Consenti.

Configura Okta per AppFabric

Okta è la World's Identity Company. In qualità di principale partner indipendente per l'identità, Okta consente a tutti di utilizzare in sicurezza qualsiasi tecnologia, ovunque, su qualsiasi dispositivo o app. I marchi più affidabili si fidano Okta per consentire l'accesso, l'autenticazione e l'automazione sicuri. Con flessibilità e neutralità al centro di Okta Workforce Identity e Customer Identity Clouds, i leader aziendali e gli sviluppatori possono concentrarsi sull'innovazione e accelerare la trasformazione digitale, grazie a soluzioni personalizzabili e più di 7.000 integrazioni predefinite. Okta sta costruendo un mondo in cui l'identità ti appartiene. Scopri di più su okta.com.

È possibile utilizzare AWS AppFabric per motivi di sicurezza per controllare i registri e i dati utente da Okta, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e inviali in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Okta

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Okta.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Okta verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È possibile utilizzare AppFabric con qualsiasi Okta tipo di piano.
- Devi avere un utente con il ruolo di Super Amministratore nel tuo Okta account.
- L'utente che approva l'autorizzazione dell'app AppFabric deve inoltre avere il ruolo di Super Amministratore presso Okta account.

Considerazioni sui limiti di velocità

Okta impone limiti di aliquota al Okta API. Per ulteriori informazioni su Okta Limiti di velocità delle API, vedi Limiti di velocità nel Okta Guida per gli sviluppatori su Okta sito web. Se la combinazione di AppFabric e quella esistente Okta Le applicazioni API superano Okta, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Okta account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Okta. Per trovare le informazioni necessarie per l'autorizzazione Okta con AppFabric, attenersi alla seguente procedura.

Crea un' OAuth applicazione

AppFabric si integra con Okta utilizzando OAuth. Per creare un' OAuthapplicazione con cui connetterti AppFabric, segui le istruzioni in Creare integrazioni di app OIDC sul Okta Sito web del Centro assistenza. Di seguito sono riportate le considerazioni sulla configurazione per AppFabric:

1. Per Tipo di applicazione, scegliete Applicazione Web.
2. Per Tipo di concessione, scegli Codice di autorizzazione e Refresh Token.
3. Utilizza un URL di reindirizzamento con il seguente formato come URI di reindirizzamento per l'accesso e URI di reindirizzamento per la disconnessione.

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

In questo URL, *<region>* è presente il codice del pacchetto Regione AWS in cui hai configurato il pacchetto di app. AppFabric Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`

4. Puoi saltare la configurazione Trusted Origins.
5. Concedi l'accesso a tutti i membri del tuo Okta organizzazione nella configurazione Accesso controllato.

> **Note**
>
> Se salti questo passaggio durante la creazione iniziale OAuth dell'applicazione, puoi assegnare tutti i membri dell'organizzazione come gruppo utilizzando la scheda Assegnazioni nella pagina di configurazione dell'applicazione.

6. È possibile lasciare tutte le altre opzioni con i valori predefiniti.

Ambiti richiesti

È necessario aggiungere i seguenti ambiti al Okta OAuthapplicazione:

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

Autorizzazioni dell'app

ID tenant

AppFabric richiederà un ID inquilino. L'ID del tenant inserito è il tuo AppFabric Okta dominio. Per ulteriori informazioni su come trovare il tuo Okta dominio, vedi Trova il tuo Okta dominio in Okta Guida per gli sviluppatori su Okta sito web.

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco Okta organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. Per trovare il tuo ID cliente in Okta, utilizza i seguenti passaggi:

1. Accedere a Okta console per sviluppatori.
2. Scegli la scheda Applicazioni.
3. Scegli la tua applicazione, quindi scegli la scheda Generale.
4. Scorri fino alla sezione Credenziali del client.
5. Inserisci l'ID cliente del tuo OAuth cliente nel AppFabric campo ID cliente di.

Client secret

AppFabric richiederà un segreto per il cliente. Per trovare il segreto del tuo cliente in Okta, segui i seguenti passaggi:

1. Accedere a Okta console per sviluppatori.
2. Scegli la scheda Applicazioni.
3. Scegli la tua applicazione, quindi scegli la scheda Generale.
4. Scorri fino alla sezione Credenziali del client.
5. Inserisci il segreto del client dalla tua OAuth applicazione nel campo Client Secret in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da Okta per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione, scegli consenti. L'utente che approva il Okta l'autorizzazione deve avere l'autorizzazione Super Admin in Okta.

Configura OneLogin by One Identity per AppFabric

OneLogin by One Identity è una moderna soluzione di gestione degli accessi basata sul cloud che gestisce senza problemi tutte le identità digitali della forza lavoro, dei clienti e dei partner. OneLogin offre single sign-on (SSO) sicuro, autenticazione a più fattori (MFA), autenticazione adattiva, MFA a livello desktop, integrazione delle directory con AD, LDAP, G Suite e altre directory esterne, gestione del ciclo di vita delle identità e molto altro. Con OneLogin, puoi proteggere la tua organizzazione dagli attacchi più comuni, con conseguente maggiore sicurezza, esperienze utente fluide e conformità ai requisiti normativi.

È possibile utilizzare, AWS AppFabric per motivi di sicurezza, ricevere registri di controllo e dati utente da OneLogin, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per OneLogin by One Identity

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da OneLogin by One Identity.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da OneLogin by One Identity verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un OneLogin Account avanzato o professionale.
- È necessario disporre di un utente con i privilegi di amministratore/amministratore delegato.

Considerazioni sui limiti di velocità

OneLogin by One Identity impone limiti di aliquota al OneLogin API. Per ulteriori informazioni su OneLogin Limiti di velocità per le API, vedi Get Rate Limit nel OneLogin Riferimento all'API. Se la combinazione di AppFabric e quella esistente OneLogin Le applicazioni API superano OneLogin, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi. Tuttavia, il OneLogin il limite di velocità può essere aumentato. Per assistenza, contatta il OneLogin by One Identity Account Manager o contatta One Identity.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric OneLogin by One Identity account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con OneLogin by One Identity. Per trovare le informazioni necessarie per l'autorizzazione OneLogin con AppFabric, attenersi alla seguente procedura.

Crea un' OAuthapplicazione

AppFabric si integra con OneLogin by One Identity utilizzando OAuth. Per creare un' OAuth applicazione in OneLogin, attenersi alla seguente procedura:

1. Passare alla .OneLogin pagina di accesso e accedi.
2. Dal menu Sviluppatori, scegli Credenziali API.
3. Scegli Nuove credenziali, inserisci un nome per la nuova credenziale, quindi scegli Leggi tutto.
4. Seleziona Salva. OneLogin crea un ID cliente e un segreto client.

Ambiti richiesti

È necessario aggiungere i seguenti ambiti al OneLogin by One Identity OAuth applicazione:

- Leggi tutto Per ulteriori informazioni sugli ambiti e le credenziali del client, consulta Lavorare con le credenziali API nella OneLogin Riferimento all'API.

Autorizzazioni delle app

ID tenant

AppFabric richiederà un ID inquilino. L'ID del tenant in AppFabric è il sottodominio dell'istanza. Puoi trovare il tuo ID tenant nella barra degli indirizzi del tuo browser. Ad esempio, `subdomain` è l'ID del tenant nel seguente URL. `https://subdomain.onelogin.com`

Nome del tenant

Inserisci un nome che identifichi questo univoco OneLogin by One Identity organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. Per trovare il tuo ID cliente in OneLogin by One Identity, utilizza i seguenti passaggi:

1. Passare alla .OneLogin pagina di accesso e accedi.
2. Dal menu Sviluppatori, scegli Credenziali API.
3. Scegli la credenziale API per ottenere l'ID client.

Client secret

AppFabric richiederà un segreto per il cliente. Per trovare il segreto del tuo cliente in OneLogin by One Identity, segui i seguenti passaggi:

1. Passare alla .OneLogin pagina di accesso e accedi.
2. Dal menu Sviluppatori, scegli Credenziali API.
3. Scegli la credenziale API per ottenere il Client Secret.

Autorizzazione dell'app client

In AppFabric, crea un'autorizzazione per l'app utilizzando l'ID e il nome dell'inquilino e l'ID e il nome del cliente. Scegli connetti per attivare l'autorizzazione.

Configura PagerDuty per AppFabric

PagerDuty è una piattaforma di gestione delle operazioni digitali che aiuta i team a mitigare i problemi che hanno un impatto sui clienti trasformando qualsiasi segnale in azione in modo da poter risolvere i problemi più rapidamente e operare in modo più efficiente. Si integra con CloudWatch, GuardDuty, CloudTraile Personal Health Dashboard.

È possibile utilizzare AWS AppFabric per motivi di sicurezza per ricevere registri di controllo e dati utente da PagerDuty, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e inviali in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per PagerDuty

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da PagerDuty.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da PagerDuty verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- Per accedere ai log di controllo, è necessario disporre di un PagerDuty Piano operativo aziendale o digitale.
- Devi essere un amministratore globale o il proprietario dell'account di PagerDuty account.

Considerazioni sui limiti di velocità

PagerDuty impone limiti di aliquota al PagerDuty API. Per ulteriori informazioni su PagerDuty Limiti di velocità delle API, consulta la sezione Limiti di velocità delle API REST su PagerDuty Piattaforma per sviluppatori. Se la combinazione di AppFabric e quella esistente PagerDuty Le applicazioni API superano PagerDuty, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric PagerDuty account

Il PagerDuty la piattaforma supporta le chiavi di accesso API. Per generare una chiave di accesso API, utilizza i seguenti passaggi.

Crea una chiave di accesso API

AppFabric si integra con PagerDuty utilizzando una chiave di accesso API per client pubblici. Per creare una chiave di accesso API in PagerDuty, utilizza i seguenti passaggi:

1. Passare alla .PagerDuty pagina di accesso e accesso.
2. Scegli Integrazioni, Chiavi di accesso API.

3. Scegli Crea nuova chiave API.
4. Inserisci una descrizione, quindi seleziona Chiave API di sola lettura.
5. Scegli Create Key (Crea chiave).
6. Copia e salva la chiave API. Ti servirà più avanti AppFabric. Se chiudi la pagina prima di salvare la chiave API, devi generare una nuova chiave API e salvarla. Questa chiave dovrebbe essere dedicata a AppFabric evitare la condivisione di PagerDuty Limite di velocità dell'API con le altre integrazioni.

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant per il tuo PagerDuty account è l'URL di base del tuo account. Puoi trovarlo accedendo a PagerDuty e copiando dalla barra degli indirizzi del tuo browser web. L'ID del tenant deve seguire uno dei seguenti formati:

- Per gli account statunitensi, *`subdomain`*`.pagerduty.com`
- Per gli account UE, *`subdomain`*`.eu.pagerduty.com`

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco PagerDuty organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

Token dell'account di servizio

AppFabric richiederà il token del tuo account di servizio. Il token dell'account di servizio in AppFabric è la chiave di accesso API in cui hai creatoCrea una chiave di accesso API.

Configura Ping Identity per AppFabric

In Ping Identity, crediamo nel rendere le esperienze digitali sicure e fluide per tutti gli utenti, senza compromessi. Ecco perché più della metà delle aziende Fortune 100 sceglie Ping Identity per proteggere le interazioni digitali dei propri utenti e rendere le esperienze fluide. Il 23 agosto 2023, Ping Identity e ForgeRock uniti per offrire più scelta, competenze più approfondite e una soluzione di identità più completa per clienti e partner.

È possibile utilizzare AWS AppFabric per la sicurezza per ricevere registri di controllo e dati utente da Ping Identity, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e inviali in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Ping Identity

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Ping Identity.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Ping Identity verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- Devi avere un Essential, Plus o Premium Ping Identity conto. Per ulteriori informazioni sulla creazione o l'aggiornamento alla versione applicabile Ping Identity tipo di piano, vedere Ping Identity prezzi per tutte le funzionalità di Ping Identity sito web.
- Devi avere il ruolo Identity Data Read Only nel tuo Ping Identity account. Puoi aggiungere ruoli al tuo account concedendo ruoli per la tua candidatura. Per ulteriori informazioni sui ruoli, consulta Ruoli su Ping Identity Sito Web di supporto.

Considerazioni sui limiti di velocità

Ping Identity non pubblica limiti di velocità. Devi creare una richiesta di supporto o contattare il Ping Identity Team Customer Success. Se la combinazione di AppFabric e quella esistente Ping Identity Le applicazioni API superano Ping Identity, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Ping Identity account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Ping Identity. Per trovare le informazioni necessarie per l'autorizzazione Ping Identity con AppFabric, attenersi alla seguente procedura.

Crea un' OAuthapplicazione

AppFabric si integra con Ping Identity utilizzando OAuth. Per creare un' OAuthapplicazione in Ping Identity, attenersi alla seguente procedura:

1. Segui le istruzioni nella sezione Creare una connessione all'applicazione del PingOne guida per sviluppatori su Ping Identity sito web.
2. Dopo aver creato l'applicazione, personalizza i tipi di sovvenzione.
   a. Una volta effettuato l'accesso all'applicazione, scegli la scheda Configurazione e fai clic sull'icona a forma di matita per apportare modifiche alla configurazione esistente.
   b. In Tipo di concessione, seleziona Codice di autorizzazione. Mantieni PKCE Enforcement come OPZIONALE.
   c. Seleziona Refresh Token e scegli la durata dell'aggiornamento.
3. Utilizza un URL di reindirizzamento con il seguente formato in URL di reindirizzamento/URL di richiamata.

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

   In questo URL, *<region>* c'è il codice del pacchetto Regione AWS in cui hai configurato il pacchetto dell'app. AppFabric Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://`*`us-east-1`*`.console.aws.amazon.com/appfabric/oauth2`

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant inserito è il tuo AppFabric Ping Identity nome dell'istanza. Puoi trovare il tuo ID inquilino nella barra degli indirizzi del tuo browser. Ad esempio, *`API_PATH`*`/v1/environments/`*`environmentID`*. Dove *`API_PATH`* rappresenta il dominio regionale per PingOne server, ad esempio`api.pingone.com`, e *`environmentID`* rappresenta l'ID

dell'ambiente indicato nelle proprietà dell'ambiente dell'applicazione. Per ulteriori informazioni sulle proprietà dell'ambiente, vedere Proprietà dell'ambiente sul Ping Identity sito web.

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco Ping Identity organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. Per trovare il tuo ID cliente in Ping Identity, utilizza i seguenti passaggi:

1. Accedi a PingOne console di amministrazione e scegli Applicazioni.
2. Scegli l'applicazione dall'elenco.
3. Scegli la scheda Panoramica, quindi cerca il valore dell'ID client.

Client secret

AppFabric richiederà un segreto per il cliente. Per trovare il segreto del tuo cliente in Ping Identity, segui i seguenti passaggi:

1. Accedi a PingOne console di amministrazione e scegli Applicazioni.
2. Scegli l'applicazione dall'elenco.
3. Scegli la scheda Panoramica, quindi cerca il valore Client Secret.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da Ping Identity per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione, scegli consenti.

Configura Salesforce per AppFabric

Salesforce crea software basato su cloud progettato per aiutare le aziende a trovare più potenziali clienti, concludere più trattative e stupire i clienti con un servizio straordinario. Salesforce’s Customer 360 offre una suite completa di prodotti, unisce i team di vendita, assistenza, marketing, commercio e IT con un'unica visione condivisa delle informazioni sui clienti, aiutando le organizzazioni a sviluppare relazioni con clienti e dipendenti.

È possibile utilizzarlo AWS AppFabric per ricevere registri di controllo e dati utente da Salesforce, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e inviali in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Salesforce

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Salesforce.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Salesforce verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un'edizione Performance, Enterprise o Unlimited di Salesforce. Contatto Salesforce per eseguire l'aggiornamento a una di queste edizioni.
- Se stai cercando di AppFabric trasferire file di registro degli eventi ogni ora con un set completo di eventi di registro da Salesforce, è necessario abbonarsi a Event Monitoring come parte delle funzionalità Shield di Salesforce. Altrimenti, AppFabric trasferirà eventi limitati (ad esempio Login, Logout, InsecureExternalAssets API Total Usage, CORS Violation ed HostnameRedirects ELF Events) da Salesforce's file di registro giornaliero standard. Puoi verificare se il tuo Salesforce l'account è già abbonato a Shield Features andando su Configurazione > Gestione eventi. Se vedi 19 o più eventi elencati, il tuo account è iscritto all'Event Monitoring. Se non disponi di Event Monitoring, puoi acquistare un abbonamento a questo componente aggiuntivo contattando Salesforce.
- È necessario attivare la generazione del file di registro degli eventi nel Salesforce impostazioni.
- È necessario utilizzare il profilo dell'amministratore di sistema per creare un' OAuthapplicazione e accedere con le stesse credenziali di AppFabric.

> **Note**
>
> Gli eventi API Total Usage, CORS Violation Record, Hostname Redirects, Insecure External Assets, Login e Logout sono disponibili senza costi aggiuntivi nelle edizioni supportate

di Salesforce. Contatto Salesforce per acquistare i restanti tipi di eventi. Per ulteriori informazioni sull' Salesforce tipi di eventi, vedi Tipi di eventi EventLogFile supportati su Salesforce sito web.
AppFabric può supportare fino a 100.000 eventi per tipo di evento per istanza del file di registro (ogni giorno o ogni ora, a seconda dell'abbonamento al componente aggiuntivo Event Monitoring). Un file di registro che supera la soglia potrebbe causare l'esclusione dell'intero file di registro dall'ingestione.

Considerazioni sui limiti di velocità

Salesforce impone limiti di aliquota al Salesforce API. Per ulteriori informazioni su Salesforce Limiti di velocità delle API, vedi Limiti e allocazioni delle richieste API su Salesforce sito web. Se la combinazione di AppFabric e quella esistente Salesforce Le applicazioni API superano Salesforce's limiti, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

È possibile che si verifichi un ritardo fino a 6 ore nel file di registro giornaliero o fino a 29 ore nel file di registro orario prima che un evento di controllo venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Salesforce account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Salesforce. Per trovare le informazioni necessarie per l'autorizzazione Salesforce con AppFabric, attenersi alla seguente procedura.

Crea un' OAuth applicazione

AppFabric si integra con Salesforce utilizzando OAuth. Per creare un' OAuth applicazione in Salesforce, attenersi alla seguente procedura:

1. Accedi al tuo Salesforce conto.
2. Accedere alla pagina di configurazione come descritto nella Salesforce documentazione.
3. Cerca App Manager nella ricerca rapida.

4. Scegli Nuova app connessa.
5. Inserisci le informazioni richieste nei campi del modulo.
6. Scegli Abilita OAuth impostazioni.
7. Assicurati di disattivare le seguenti opzioni:
   - Richiedi l'estensione Proof Key for Code Exchange (PKCE) per i flussi di autorizzazione supportati
   - Richiedi il segreto per Web Server Flow
   - Richiedi un segreto per Refresh Token Flow
   - Abilita la rotazione del token di aggiornamento
8. Immettete un URL con il seguente formato nella casella di testo URL di callback e scegliete Salva modifiche.

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

   In questo URL, *<region>* è riportato il codice Regione AWS in cui hai configurato il pacchetto AppFabric dell'app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`
9. Compila gli ambiti secondo necessità (descritti nella Ambiti richiesti sezione seguente). Tutti gli altri campi possono essere lasciati con i valori predefiniti.
10. Scegli Save (Salva).
11. Completa i seguenti passaggi per verificare la politica del token di aggiornamento per la nuova OAuth app:
    a. Nella pagina di configurazione, inserisci App connesse nella casella di testo Ricerca rapida, quindi scegli Gestisci app connesse.
    b. Scegli Modifica accanto all'app appena creata.
    c. Assicurati che il token Refresh sia valido fino a quando non viene selezionata l'opzione Revoked.
    d. Salvare le modifiche.
12. Completate i seguenti passaggi per verificare che i log di controllo vengano generati:
    a. Nella pagina Configurazione, immettete Event Log File nella casella di testo Quick Find, quindi scegliete Event Log File Browser.

b. Verificate che i registri degli eventi siano elencati nell'Event Log File Browser.

13. Vai all'app creata e scegli Visualizza dal menu a discesa.
14. Scegli Manage Consumer Details (Gestisci i dettagli del consumatore).

    Verrai reindirizzato a una nuova scheda in cui dovrai verificare la tua identità. In quella scheda, prendi nota dei valori Consumer Key e Consumer Secret. Ti serviranno in seguito per accedere.

Ambiti richiesti

È necessario aggiungere i seguenti ambiti al Salesforce OAuthapplicazione:

- Gestisci i dati utente tramite APIs (`API`).
- Esegui la richiesta in qualsiasi momento (`refresh_tokeneoffline_access`).

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant in AppFabric è il sottodominio del tuo Salesforce Il mio dominio. Puoi trovare il sottodominio My Domain nella barra degli indirizzi del browser tra `https://` `e.my.salesforce.com`.

Per trovare il tuo Salesforce Il mio dominio, usa le seguenti istruzioni del Salesforce schermata iniziale.

1. Accedere alla pagina di configurazione come descritto nella Salesforce documentazione.
2. Cerca le impostazioni aziendali nella ricerca rapida e scegli Il mio dominio nei risultati.

Nome dell'inquilino

Inserisci un nome che identifichi questo nome univoco Salesforce organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. Per trovare il tuo ID cliente in Salesforce, utilizza i seguenti passaggi:

1. Vai alla pagina di configurazione.
2. Scegli Configurazione, quindi scegli App Manager.
3. Scegli l'app creata e scegli Visualizza dal menu a discesa.
4. Scegli Manage Consumer Details (Gestisci i dettagli del consumatore). Verrai reindirizzato a una nuova scheda.
5. Verifica la tua identità, quindi cerca il valore Consumer Key.
6. Inserisci la Consumer Key nel campo ID cliente di AppFabric.

Client secret

AppFabric richiederà il segreto del tuo cliente. Il segreto del cliente AppFabric è il segreto del consumatore in Salesforce. Per trovare il tuo segreto in Salesforce, segui i seguenti passaggi:

1. Vai alla pagina di configurazione.
2. Scegli Configurazione, quindi scegli App Manager.
3. Scegli l'app creata e scegli Visualizza dal menu a discesa.
4. Scegli Manage Consumer Details (Gestisci i dettagli del consumatore). Verrai reindirizzato a una nuova scheda.
5. Verifica la tua identità, quindi cerca il valore Consumer Secret.
6. Inserisci il Consumer Secret nel campo segreto del cliente in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da Salesforce per approvare l'autorizzazione. Nella pagina di approvazione, assicurati di utilizzare il Salesforce Ruolo di amministratore di sistema o un Salesforce utente che dispone delle autorizzazioni utente View Event Log Files e API Enabled durante l'autorizzazione. Scegli Consenti per approvare l'autorizzazione. AppFabric

Configura ServiceNow per AppFabric

ServiceNow è un fornitore leader di servizi basati su cloud che automatizzano le operazioni IT aziendali. ServiceNowITOM offre alle aziende la visibilità e il controllo completi dell'intero ambiente IT, inclusa l'infrastruttura virtualizzata e cloud. Semplifica la mappatura, la fornitura e la garanzia dei servizi, consolidando i dati dei servizi IT e dell'infrastruttura in un unico sistema di registrazione.

Inoltre, automatizza e semplifica i processi chiave, tra cui la gestione di eventi, incidenti, problemi, configurazioni e modifiche.

È possibile utilizzare AWS AppFabric per la sicurezza per ricevere registri di controllo e dati utente da ServiceNow, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per ServiceNow

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da ServiceNow.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da ServiceNow verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È possibile utilizzare AppFabric con qualsiasi ServiceNow tipo di piano.
- È necessario disporre di un utente con il ruolo di amministratore nel ServiceNow account.
- Devi avere un ServiceNow istanza.

Considerazioni sui limiti di velocità

ServiceNow impone limiti di aliquota al ServiceNow API. Per ulteriori informazioni su ServiceNow Limiti di velocità delle API, vedi Limitazione della velocità dell'API REST in entrata su ServiceNow sito web. Se la combinazione di AppFabric e quella esistente ServiceNow Le applicazioni API superano i limiti, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric ServiceNow account

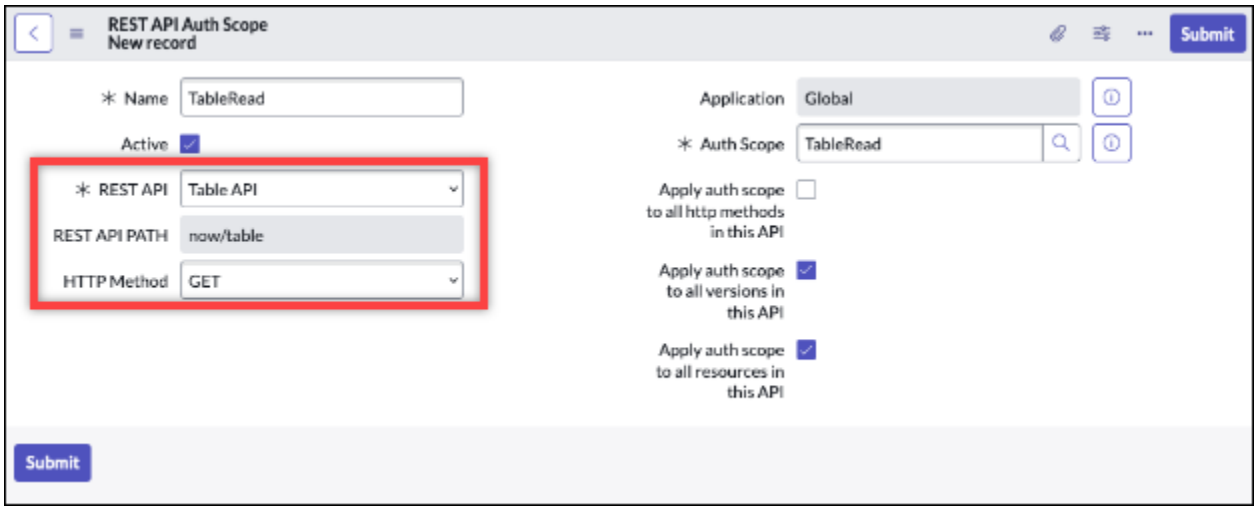
Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con ServiceNow. Utilizza i seguenti passaggi per trovare le informazioni necessarie per l'autorizzazione ServiceNow con AppFabric.

Creare un' OAuth applicazione

Il Now Platform supporta OAuth 2.0 - Tipo di concessione di autorizzazione per i client pubblici per generare un token di accesso.

1. Registra la tua OAuth candidatura. Ciò richiede i seguenti tre passaggi. Per ulteriori informazioni sul completamento di questi passaggi, consulta la sezione Registrare la candidatura con ServiceNowsul ServiceNow sito web.

   a. Registra l'app e assicurati che Auth Scope abbia accesso all'API Table, con un PATH API REST di now/table e un metodo HTTP di GET come mostrato nell'esempio seguente.



   b. Genera un codice di autorizzazione.

   c. Genera un token al portatore utilizzando il codice di autorizzazione.

2. Utilizza un URL di reindirizzamento con il seguente formato.

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

   In questo URL, *<region>* è riportato il codice Regione AWS in cui hai configurato il pacchetto di AppFabric app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`

Autorizzazioni delle app

ID tenant

AppFabric richiederà un ID inquilino. L'ID del tenant in AppFabric è il nome dell'istanza. Puoi trovare il tuo ID tenant nella barra degli indirizzi del tuo browser. Ad esempio, *example* è l'ID del tenant nel seguente URL. `https://example.service-now.com`

Nome dell'inquilino

Inserisci un nome che identifichi questo nome univoco ServiceNow organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. Utilizza i seguenti passaggi per trovare il tuo ID cliente in ServiceNow.

1. Vai al ServiceNow console.
2. Scegli Sistema OAuth, quindi scegli la scheda Registro applicazioni.
3. Scegliere la applicazione.
4. Inserisci l'ID cliente del tuo OAuth cliente nel campo ID cliente di AppFabric.

Client secret

AppFabric richiederà un segreto per il cliente. Segui i seguenti passaggi per trovare il segreto del tuo cliente in ServiceNow.

1. Vai al ServiceNow console.
2. Scegli Sistema OAuth, quindi scegli la scheda Registro applicazioni.
3. Scegliere la applicazione.
4. Inserisci il segreto del client dall' OAuth applicazione nel campo Client Secret in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da ServiceNow per approvare l'autorizzazione. Scegli Consenti per approvare l' AppFabric autorizzazione.

Configura Singularity Cloud per AppFabric

Il Singularity Cloud la piattaforma protegge la tua azienda dalle minacce di tutte le categorie, in tutte le fasi. La sua intelligenza artificiale brevettata estende la sicurezza dalle firme e dai modelli noti agli attacchi più sofisticati, come zero-day e ransomware.

È possibile utilizzare AWS AppFabric per ricevere registri di controllo e dati utente da Singularity Cloud, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

> **Note**
>
> Singularity Cloud è possibile accedere alla documentazione solo dopo aver effettuato l'accesso al Singularity Cloud account. Pertanto, non possiamo collegarci direttamente a Singularity Cloud documentazione tratta da questo documento.

Argomenti

AppFabric supporto per Singularity Cloud

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Singularity Cloud.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Singularity Cloud verso le destinazioni supportate, è necessario avere un ruolo di amministratore nel Singularity Cloud account. Per ulteriori informazioni su Singularity Cloud Limiti di velocità delle API, accedi al tuo account Singularity Cloud, sfoglia la sezione della documentazione e cerca i ruoli.

Considerazioni sui limiti di velocità

Singularity Cloud impone limiti di aliquota al Singularity Cloud API. Per ulteriori informazioni su Singularity Cloud Limiti di velocità delle API, accedi al tuo account Singularity Cloud, sfoglia la sezione della documentazione e cerca i limiti di velocità delle API.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti nella consegna a destinazione di un evento di verifica. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Singularity Cloud account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Singularity Cloud. Per trovare le informazioni necessarie per l'autorizzazione Singularity Cloud con AppFabric, attenersi alla seguente procedura.

Crea un token API per Singularity Cloud

Completare la procedura seguente per creare un token API associato a un utente del servizio. Il token API non sarà collegato a un utente della console o a un indirizzo e-mail specifici.

> **Note**
>
> Crea un nuovo utente o copia l'utente del servizio per ottenere un nuovo token API prima o dopo la scadenza del token API per l'utente del servizio.

1. Accedi al tuo Singularity Cloud conto.
2. Nella barra degli strumenti Impostazioni, scegli Utenti, quindi scegli Utenti del servizio.
3. Scegli Azioni, quindi seleziona Crea nuovo utente del servizio.
4. Nella pagina Crea nuovo utente del servizio, inserisci un nome, una descrizione e una data di scadenza per l'utente del servizio.
5. Scegli Next (Successivo).
6. Nella sezione Seleziona ambito di accesso, seleziona l'ambito.
   - Seleziona Account per il livello di accesso.
   - Seleziona l'account per il quale desideri ricevere i registri di controllo.
7. Scegli Create User (Crea utente).

   Viene generato il token API. Si apre una finestra che mostra la stringa del token con un messaggio che indica che questa è l'ultima volta che è possibile visualizzare il token.

8. (Facoltativo) Scegliete Copy API Token e archiviatelo in un luogo sicuro.
9. Scegli Chiudi.

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant in AppFabric sarà il sottodominio di Sentinel One indirizzo del sito Web a cui si accede al servizio. Ad esempio, se accedi al tuo Singularity Cloud account all'`example-company-1.sentinelone.net`indirizzo, il tuo ID inquilino è`example-company-1`.

Nome dell'inquilino

Inserisci un nome che identifichi questo nome univoco Singularity Cloud organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

Token dell'account di servizio

Utilizza il token che hai generato seguendo i passaggi descritti nella Crea un token API per Singularity Cloud sezione di questa guida. Se smarrisci o non riesci a localizzare il token, puoi generarne uno nuovo seguendo nuovamente la stessa procedura.

> **Note**
>
> Se viene generato un nuovo token API nella console Singularity Cloud durante AppFabric l'acquisizione dei log di controllo, le acquisizioni verranno interrotte. In tal caso, sarà necessario aggiornare l'autorizzazione dell'app con un nuovo token API per riprendere l'inserimento del registro di controllo.

Configura Slack per AppFabric

Slack ha la missione di rendere la vita lavorativa delle persone più semplice, piacevole e produttiva. È la piattaforma di produttività per le aziende clienti che migliora le prestazioni offrendo a tutti l'automazione senza codice, semplificando la condivisione delle ricerche e delle conoscenze e mantenendo i team connessi e coinvolti mentre procedono insieme. Come parte di Salesforce, Slack

è profondamente integrato nel Salesforce Customer 360, che aumenta la produttività dei team di vendita, assistenza e marketing. Per saperne di più e iniziare a Slack gratuitamente, visita slack.com.

È possibile utilizzare AWS AppFabric per motivi di sicurezza per controllare i registri e i dati utente da Slack, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e inviali in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Slack

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Slack.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Slack verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un piano Enterprise Grid con Slack. Per ulteriori informazioni, vedere Introduzione a Slack Enterprise Grid su Slack sito web.
- Devi avere un utente con il ruolo di Org Owner nel tuo Slack account. Per ulteriori informazioni sui ruoli, vedere Tipi di ruoli in Slack nella Slack Centro assistenza su Slack sito web.

Considerazioni sui limiti di velocità

Slack impone limiti di aliquota al Slack API. Per ulteriori informazioni sull' Slack Limiti di velocità delle API, vedi Limiti di velocità nel Slack Guida all'utilizzo delle API su Slack sito web. Se la combinazione di AppFabric e quella esistente Slack Le applicazioni API superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Slack account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Slack. Per trovare le informazioni necessarie per l'autorizzazione Slack con AppFabric, attenersi alla seguente procedura.

Crea un' OAuth applicazione

AppFabric si integra con Slack utilizzando OAuth. Esistono due modi per creare un' OAuth app: utilizzando un manifesto dell'app o Da zero. Per creare un' OAuth applicazione in Slack, attenersi alla seguente procedura.

Using an app manifest

1. Passare alla .Slack Interfaccia utente di gestione delle app nel browser.
2. Scegli Crea nuova app.
3. Scegli Da un manifesto dell'app.
4. Scegli l'area di lavoro per la quale desideri AppFabric autorizzare.
5. Nella casella Inserisci il manifesto dell'app in basso, scegli JSON e sostituisci il JSON esistente con il seguente. *<region>*Sostituiscilo con quello appropriato Regione AWS (ad esempio,*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. Copia e salva l'ID client e il segreto del client dalla pagina delle informazioni di base.
7. Per questo `auditLogs:read` scopo, devi abilitare la distribuzione pubblica della tua app. Per ulteriori informazioni, consulta Abilitare la distribuzione pubblica sul sito Web di Slack.

From scratch

1. Scegli Da zero nella schermata Crea un'app.
2. Assegna un nome alla tua app e scegli uno spazio di lavoro.
3. Copia e salva l'ID cliente e il segreto del cliente dalla pagina delle informazioni di base.
4. Nella pagina OAuth & Autorizzazioni, attiva l'opzione Sicurezza avanzata dei token tramite rotazione dei token.
5. Aggiungi un URL con il seguente formato nella URLs sezione Reindirizzamento della pagina OAuth & Autorizzazioni.

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

   In questo URL, *<region>* c'è il codice per il pacchetto Regione AWS in cui hai configurato il pacchetto AppFabric dell'app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`
6. Per l'`auditLogs:read`ambito, devi abilitare la distribuzione pubblica della tua app. Per ulteriori informazioni, consulta Abilitare la distribuzione pubblica sul sito Web di Slack.

Ambiti richiesti

> **Note**
>
> Questa sezione è applicabile solo se hai scelto di creare l' OAuth app da zero. Salta questa sezione se hai scelto di utilizzare il manifesto dell'app per creare un'autorizzazione dell'applicazione.

È necessario aggiungere i seguenti ambiti di token utente nella pagina OAuth & Autorizzazioni del Slack OAuthapplicazione:

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

Autorizzazioni dell'app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant inserito è il tuo AppFabric Slack ID dell'area di lavoro. Per ottenere il tuo ID inquilino, segui le istruzioni in Localizza il tuo Slack URL nel Slack Centro assistenza su Slack sito web. Tuo Slack L'URL dell'area di lavoro ha un formato simile a `examplecorp.slack.com` o`examplecorp.enterprise.slack.com`. L'ID tenant di cui hai bisogno è `examplecorp` senza `.slack.com` o. `.enterprise.slack.com`

Nome dell'inquilino

Inserisci un nome che identifichi il tuo Slack ID dell'area di lavoro. AppFabricutilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app

ID client

AppFabric richiederà l'ID cliente al tuo Slack OAuthapplicazione. Per trovare l'ID del cliente, procedi nel seguente modo:

1. Passare alla .Slack Interfaccia utente di gestione delle app nel tuo browser.
2. Scegli l' OAuth applicazione con cui utilizzi AppFabric.
3. Inserisci l'ID client dalla pagina Informazioni di base nel campo ID cliente in AppFabric.

Client secret

AppFabric richiederà il segreto del cliente al tuo Slack OAuthapplicazione. Per trovare il segreto del client, procedi nel seguente modo:

1. Passare alla .Slack Interfaccia utente di gestione delle app nel tuo browser.
2. Scegli l' OAuth applicazione con cui utilizzi AppFabric.

3. Inserisci il segreto del client dalla pagina Informazioni di base nel campo Segreto client in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da Slack per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione, scegli consenti.

Configura Smartsheet per AppFabric

Smartsheet è una piattaforma di gestione del lavoro che consente di allineare lavoro, persone e tecnologia all'interno dell'azienda. Smartsheet offre un solido set di funzionalità di livello aziendale per consentire a tutti di gestire progetti, automatizzare i flussi di lavoro e creare rapidamente soluzioni su larga scala, creando un ambiente per l'innovazione mantenendo al contempo sicurezza e conformità.

È possibile utilizzare a fini di sicurezza AWS AppFabric per controllare i registri e i dati degli utenti da Smartsheet, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Smartsheet

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Smartsheet.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Smartsheet verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un Smartsheet Account Business, Enterprise o Advance. Per ulteriori informazioni sulla creazione o l'aggiornamento del Smartsheet account, vedi uno dei due Smartsheet prezzi o SmartsheetAvanzate sul Smartsheet sito web.
- È necessario completare il Smartsheetprocesso di registrazione per sviluppatori.

Considerazioni sui limiti di velocità

Smartsheet impone limiti di aliquota al Smartsheet API. Per ulteriori informazioni su Smartsheet Limiti di velocità delle API, consulta Limitazione della velocità nella Guida alle API Smartsheet sul sito Web di Smartsheet.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Smartsheet account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Smartsheet. Per trovare le informazioni necessarie per l'autorizzazione Smartsheet con AppFabric, attenersi alla seguente procedura.

Crea un' OAuthapplicazione

AppFabric si integra con Smartsheet utilizzando OAuth. Per creare un' OAuthapplicazione in Smartsheet, attenersi alla seguente procedura:

1. Accedi agli strumenti per sviluppatori nel tuo Smartsheet conto.
2. Scegli Crea nuova app dalla schermata degli strumenti per sviluppatori.
3. Completa tutti i campi di input nella schermata Crea nuova app.
4. Utilizza qualsiasi valore univoco per l'URL dell'app e il contatto/supporto dell'app.
5. Utilizza un URL di reindirizzamento con il seguente formato come URL di reindirizzamento dell'app.

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

   In questo URL, *<region>* c'è il codice del pacchetto Regione AWS in cui hai configurato AppFabric l'app bundle. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`
6. Scegli Save (Salva).
7. Copia e salva l'ID client dell'app e il segreto dell'app.

Ambiti richiesti

Smartsheet non richiede l'aggiunta esplicita di ambiti alla configurazione. OAuth AppFabric richiederà i seguenti ambiti nella richiesta di autorizzazione al tuo Smartsheet conto:

- `READ_EVENTS`
- `READ_USERS`

Autorizzazioni dell'app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant inserito è il tuo AppFabric Smartsheet ID dell'account.

Nome dell'inquilino

AppFabric richiederà il tuo ID inquilino. Inserisci un valore che identifichi in modo univoco il tuo Smartsheet conto.

ID client

AppFabric richiederà il tuo ID cliente. L'ID cliente inserito AppFabric è il tuo Smartsheet ID client dell'app. Per trovare l'ID del client dell'app in Smartsheet, utilizza i seguenti passaggi:

1. Accedi agli strumenti per sviluppatori nel tuo Smartsheet conto.
2. Seleziona l' OAuth applicazione con cui ti connetti AppFabric.
3. Inserisci l'ID client dell'app dalla schermata del profilo dell'app nel campo ID client in AppFabric.

Client secret

AppFabric richiederà il segreto del tuo cliente. Il segreto del cliente AppFabric è tuo Smartsheet app segreta. Per trovare la tua app segreta in Smartsheet, segui i seguenti passaggi:

1. Accedi agli strumenti per sviluppatori nel tuo Smartsheet conto.
2. Seleziona l' OAuth applicazione con cui ti connetti AppFabric.
3. Inserisci il segreto dell'app dalla schermata del profilo dell'app nel campo Client Secret in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da Smartsheet per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione, scegli Consenti.

Configura Terraform Cloud per AppFabric

HashiCorp Terraform Cloud è il prodotto di provisioning multi-cloud più utilizzato al mondo. Il Terraform l'ecosistema ha più di 3.000 provider, 14.000 moduli e 250 milioni di download. Terraform Cloud è il modo più veloce da adottare Terraform, fornendo tutto ciò di cui professionisti, team e aziende globali hanno bisogno per creare e collaborare sull'infrastruttura e gestire i rischi per la sicurezza, la conformità e i vincoli operativi.

È possibile utilizzare AWS AppFabric for security per ricevere registri di controllo e dati utente da Terraform Cloud, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

- AppFabric supporto per Terraform Cloud
- Connessione al tuo AppFabric Terraform Cloud account

AppFabric supporto per Terraform Cloud

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Terraform Cloud.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Terraform Cloud verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- Per accedere ai log di controllo, è necessario disporre di un Terraform Cloud Pianifica Plus Edition ed essere il proprietario dell'organizzazione. Per ulteriori informazioni sull' Terraform Cloud piani, vedi Terraform prezzi sul HashiCorp Terraform sito web.
- I registri di controllo TBD sono disponibili per le organizzazioni che possono essere creati dal Terraform Cloud conto.

Considerazioni sui limiti di velocità

Terraform Cloud impone limiti di aliquota al Terraform Cloud API. Per ulteriori informazioni su Terraform Cloud Limiti di velocità delle API, vedi API Rate Limiting nel Terraform Cloud Impostazione generale per l'amministrazione degli sviluppatori su Terraform Cloud sito web. Se la combinazione di AppFabric e quella esistente Terraform Cloud Le applicazioni API superano Terraform Cloud, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Terraform Cloud account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Terraform Cloud. Per trovare le informazioni necessarie per l'autorizzazione Terraform Cloud con AppFabric, attenersi alla seguente procedura.

Crea un token API dell'organizzazione

AppFabric si integra con Terraform Cloud utilizzando un token API dell'organizzazione. Per ulteriori informazioni su Terraform Cloud token API dell'organizzazione, consulta Organization API Tokens. Per creare un'organizzazione, segui le istruzioni in Creating Organizations. Per creare un token API dell'organizzazione in Terraform Cloud, utilizza i seguenti passaggi.

1. Passare alla .Terraform Cloudpagina di accesso e accedi.
2. Scegli Organizzazione, Impostazioni nel pannello a sinistra, quindi scegli Token API.
3. In Organization Tokens, scegli Crea un token dell'organizzazione, quindi scegli Genera token.
4. (Facoltativo) Inserisci la data o l'ora di scadenza del token o crea un token che non scada mai.
5. Copia e salva il token. Ti servirà più avanti AppFabric. Se chiudi la pagina prima di salvare il token, devi revocare il vecchio token e crearne uno nuovo.

Autorizzazioni dell'app

ID tenant

AppFabric richiederà un ID inquilino. L'ID del tenant per il tuo Terraform Cloud account è l'URL dell'organizzazione corrente del tuo account. Puoi trovarlo accedendo al tuo Terraform Cloud organizzazione e copia dell'URL dell'organizzazione corrente. L'ID del tenant deve seguire uno dei seguenti formati:

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

Nome dell'inquilino

Inserisci un nome che identifichi questo nome univoco Terraform Cloud organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

Token dell'account di servizio

AppFabric richiederà il token del tuo account di servizio. Il token dell'account di servizio in AppFabric è il token dell'API dell'organizzazione in cui hai creatoCrea un token API dell'organizzazione.

Configura Webex by Cisco per AppFabric

Cisco è leader mondiale nella tecnologia che alimenta Internet. Cisco ispira nuove possibilità reinventando le applicazioni, proteggendo i dati, trasformando l'infrastruttura e potenziando i team per un futuro globale e inclusivo.

Informazioni su Webex by Cisco

Webex è un fornitore leader di soluzioni di collaborazione basate su cloud che includono videoconferenze, chiamate, messaggistica, eventi, soluzioni per l'esperienza dei clienti come contact center e dispositivi di collaborazione appositamente progettati. Webexl'attenzione alla fornitura di esperienze di collaborazione inclusive alimenta l'innovazione, che sfrutta l'intelligenza artificiale e il Machine Learning, per rimuovere le barriere geografiche, linguistiche, personali e familiari con la tecnologia. Le sue soluzioni si basano sulla sicurezza e sulla privacy fin dalla progettazione. Webex funziona con le app aziendali e di produttività leader a livello mondiale, fornite tramite un'unica applicazione e interfaccia. Ulteriori informazioni sono disponibili in .webex.com.

È possibile utilizzare AWS AppFabric per motivi di sicurezza per controllare i registri e i dati degli utenti da Webex, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF)

e inviali in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Webex

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Webex.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Webex verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un piano Collaboration Flex, Meet Plan, Call Plan o superiore. Per ulteriori informazioni sulla creazione o l'aggiornamento alla versione applicabile Webex tipo di piano, vedere Webex prezzi per tutte le funzionalità di Webex sito web.
- L'account deve disporre della licenza Pro Pack per accedere a Security Audit Events fornita da uno dei Cisco AuditLog APIs.
- È necessario disporre di un utente con il ruolo Amministratore organizzativo > Amministratore completo.
- La configurazione dei ruoli di amministratore per l'amministratore completo deve avere l'opzione Compliance Officer abilitata.

Considerazioni sui limiti di velocità

Webex impone limiti di aliquota al Webex API. Per ulteriori informazioni su Webex Limiti di velocità delle API, vedi Limiti di velocità nel Webex Guida per gli sviluppatori sul Webex sito web. Se la combinazione di AppFabric e quella esistente Webex Le applicazioni API superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle

precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Webex account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Webex. Per trovare le informazioni necessarie per l'autorizzazione Webex con AppFabric, attenersi alla seguente procedura.

Crea un' OAuth applicazione

AppFabric si integra con Webex utilizzando OAuth. Per creare un' OAuthapplicazione in Webex, attenersi alla seguente procedura:

1. Segui le istruzioni nella sezione Registrazione dell'integrazione nella pagina Integrazioni e autorizzazioni del Webex Guida per gli sviluppatori.
2. Utilizza un URL di reindirizzamento con il seguente formato.

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

   In questo URL, *<region>* è presente il codice Regione AWS in cui hai configurato il pacchetto di AppFabric app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`

Ambiti richiesti

È necessario aggiungere i seguenti ambiti al Webex OAuthapplicazione:

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

Autorizzazioni dell'app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant inserito è il tuo AppFabric Webex ID dell'organizzazione. Per informazioni su come trovare il tuo Webex ID dell'organizzazione, consulta

Cerca l'ID della tua organizzazione in CiscoWebex Control Hub sul Webex Sito web del Centro assistenza.

Nome dell'inquilino

Inserisci un nome che identifichi questo univoco Webex istanza. AppFabricutilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà il tuo Webex ID cliente. Per trovare il tuo Webex ID cliente, segui i seguenti passaggi:

1. Accedi al tuo Webex conto presso https://developer.webex.com.
2. Scegli il tuo avatar in alto a destra.
3. Scegli My Webex Apps.
4. Scegliete l' OAuth2 applicazione per cui utilizzate. AppFabric
5. Inserisci l'ID cliente in questa pagina nel campo ID cliente in AppFabric.

Client secret

AppFabric richiederà il tuo Webex segreto del cliente. Webex presenta il segreto del cliente solo una volta quando si crea inizialmente l' OAuth applicazione. Per generare un nuovo client secret se non hai salvato il client secret iniziale, procedi nel seguente modo:

1. Accedi al tuo Webex conto presso https://developer.webex.com.
2. Scegli il tuo avatar in alto a destra.
3. Scegli My Webex Apps.
4. Scegliete l' OAuth2 applicazione per cui utilizzate. AppFabric
5. In questa pagina, genera un nuovo client secret.
6. Inserisci il nuovo segreto del cliente nel campo Segreto del cliente in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app, AppFabric riceverai una finestra pop-up da Webex per approvare l'autorizzazione. Per approvare l' AppFabricautorizzazione, scegli accetta.

Configura Zendesk per AppFabric

Zendesk ha avviato la rivoluzione dell'esperienza del cliente nel 2007, consentendo a qualsiasi azienda in tutto il mondo di offrire il proprio servizio clienti online. Oggi, Zendesk è il paladino di un ottimo servizio ovunque per tutti e dà vita a miliardi di conversazioni, mettendo in contatto più di 100.000 marchi con centinaia di milioni di clienti tramite telefonia, chat, e-mail, messaggistica, canali social, community, siti di recensioni e centri assistenza. Zendesk i prodotti sono costruiti con amore per essere amati. L'azienda è stata concepita a Copenaghen, in Danimarca, costruita e cresciuta in California e oggi impiega più di 6.000 persone in tutto il mondo.

È possibile utilizzare a fini di sicurezza AWS AppFabric per controllare i registri e i dati degli utenti da Zendesk, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Zendesk

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Zendesk.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Zendesk verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un Zendesk Account Suite Enterprise o Enterprise Plus o un Zendesk Account Support Enterprise. Per ulteriori informazioni sulla creazione o l'aggiornamento a un Zendesk Account aziendale, vedi Verifica del tipo di piano Zendesksul Zendesk sito web.
- È necessario disporre di un utente con il ruolo di amministratore nel Zendesk account. Per ulteriori informazioni sui ruoli, vedere Understanding Zendesk Supporta i ruoli utente su Zendesk sito web.

Considerazioni sui limiti di velocità

Zendesk impone limiti di aliquota al Zendesk API. Per ulteriori informazioni su Zendesk Limiti di velocità delle API, consulta Limiti di velocità nel Zendesk Guida per gli sviluppatori su Zendesk sito

web. Se la combinazione di AppFabric e quella esistente Zendesk Le applicazioni API superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo fino a 30 minuti prima che un evento di audit venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati. Tuttavia, questo potrebbe essere personalizzabile a livello di account. Per assistenza, contattare il Supporto.

Connessione al tuo AppFabric Zendesk account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Zendesk. Per trovare le informazioni necessarie per l'autorizzazione Zendesk con AppFabric, attenersi alla seguente procedura.

Crea un' OAuthapplicazione

AppFabric si integra con Zendesk utilizzando OAuth. In Zendesk, è necessario creare un' OAuth applicazione con le seguenti impostazioni:

1. Segui le istruzioni nella sezione Registrazione dell'applicazione con Zendesk dell'articolo Utilizzo dell' OAuth autenticazione con l'applicazione sul Zendesk Sito Web di supporto.
2. Utilizza un URL di reindirizzamento con il seguente formato.

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

   In questo URL, *<region>* è presente il codice Regione AWS in cui hai configurato il pacchetto di AppFabric app. Ad esempio, il codice per la regione Stati Uniti orientali (Virginia settentrionale) è. `us-east-1` Per quella regione, l'URL di reindirizzamento è. `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo Tenant ID. Il Tenant ID inserito è il tuo AppFabric Zendesk sottodominio. Per ulteriori informazioni su come trovare il tuo Zendesk sottodominio, vedi Dove posso trovare il mio Zendesk sottodominio su Zendesk Sito Web di supporto.

Nome dell'inquilino

Inserisci un nome che identifichi questo nome univoco Zendesk organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà un ID cliente. L'ID cliente inserito AppFabric è il tuo Zendesk Identificatore univoco dell'API. Per trovare il tuo identificatore univoco Zendesk, procedi nel seguente modo:

1. Accedi al Centro di amministrazione nel tuo Zendesk account.
2. Scegli App e integrazioni.
3. Scegli APIs, Zendesk APIs.
4. Scegli la scheda OAuth Clienti.
5. Scegli l' OAuth applicazione per cui hai creato AppFabric.
6. Inserisci l'identificatore univoco OAuth del tuo cliente nel AppFabric campo ID cliente di.

Client secret

AppFabric richiederà un segreto per il cliente. Il segreto del cliente AppFabric è tuo Zendesk gettone segreto. Zendesk presenta il tuo token segreto solo una volta quando lo crei per la prima volta Zendesk OAuthapplicazione. Per generare un nuovo token segreto se non hai salvato il token segreto iniziale, usa i seguenti passaggi:

1. Accedi al Centro di amministrazione nel tuo Zendesk account.
2. Scegli App e integrazioni.
3. Scegli APIs, Zendesk APIs.
4. Scegli la scheda OAuth Clienti.
5. Scegli l' OAuth applicazione per cui hai creato AppFabric.
6. Scegli il pulsante Rigenera accanto al campo Token segreto.
7. Inserisci il nuovo token segreto nel campo Segreto del cliente in AppFabric.

Approva l'autorizzazione

Dopo aver creato l'autorizzazione dell'app in AppFabric, riceverai una finestra pop-up da Zendesk per approvare l'autorizzazione. Per approvare l' AppFabric autorizzazione, scegli Consenti.

Configura Zoom per AppFabric

Zoom è una piattaforma di collaborazione all-in-one intelligente che rende la connessione più semplice, coinvolgente e dinamica per aziende e privati. Zoom la tecnologia mette le persone al centro, abilita connessioni significative, facilita la collaborazione moderna e promuove l'innovazione umana attraverso soluzioni come chat di gruppo, telefono, riunioni, contact center cloud omnicanale, registrazioni intelligenti, lavagna e altro ancora, in un'unica offerta.

È possibile utilizzare AWS AppFabric , a fini di sicurezza, per controllare i registri e i dati degli utenti da Zoom, normalizza i dati in formato Open Cybersecurity Schema Framework (OCSF) e invia i dati in un bucket Amazon Simple Storage Service (Amazon S3) o in un flusso Amazon Data Firehose.

Argomenti

AppFabric supporto per Zoom

AppFabric supporta la ricezione di informazioni sugli utenti e registri di controllo da Zoom.

Prerequisiti

Da utilizzare per AppFabric trasferire i registri di controllo da Zoom verso le destinazioni supportate, è necessario soddisfare i seguenti requisiti:

- È necessario disporre di un Zoom Piano Pro, Business, Education o Enterprise.
- Il tuo Zoom Il ruolo di amministratore deve disporre dell'autorizzazione per creare server-to-server OAuth applicazioni. Per informazioni sull'abilitazione server-to-server OAuth delle applicazioni, consulta la sezione Abilitare le autorizzazioni della Server-to-Server OAuthpagina nel Zoom Guida per gli sviluppatori su Zoom sito web.
- Tuo Zoom Il ruolo di amministratore deve disporre dell'autorizzazione per visualizzare i registri delle attività di amministrazione e le attività di controllo di accesso/disconnessione. Per ulteriori informazioni sull'abilitazione dell'autorizzazione alla visualizzazione delle attività di controllo, vedere Utilizzo della gestione dei ruoli e Utilizzo dei registri delle attività di amministrazione su Zoom Sito Web di supporto.

Considerazioni sui limiti di velocità

Zoom impone limiti di aliquota al Zoom API. Per ulteriori informazioni sull' Zoom Limiti di velocità delle API, vedi Limiti di velocità nel Zoom Guida per gli sviluppatori. Se la combinazione di AppFabric e quella esistente Zoom le applicazioni superano il limite, la visualizzazione dei log di controllo AppFabric potrebbe subire ritardi.

Considerazioni sul ritardo dei dati

Potresti riscontrare un ritardo di circa 24 ore prima che un evento di controllo venga consegnato a destinazione. Ciò è dovuto al ritardo negli eventi di controllo resi disponibili dall'applicazione e alle precauzioni adottate per ridurre la perdita di dati.

Connessione AppFabric al tuo Zoom account

Dopo aver creato il pacchetto di app all'interno del AppFabric servizio, devi autorizzare AppFabric con Zoom. Per trovare le informazioni necessarie per l'autorizzazione Zoom con AppFabric, attenersi alla seguente procedura.

Crea un' server-to-server OAuthapplicazione

AppFabric utilizza le credenziali dell'app server-to-server OAuth con cui eseguire l'integrazione Zoom. Per creare un' server-to-server OAuth applicazione in Zoom, segui le istruzioni riportate in Creare un' Server-to-Server OAuth app nel Zoom Guida per gli sviluppatori. AppFabric non supporta Zoom webhook, e puoi saltare la sezione per aggiungere abbonamenti webhook.

Ambiti richiesti

Zoom offre due tipi di ambiti: ambiti granulari (per applicazioni appena create) e ambiti classici (per applicazioni create in precedenza).

È necessario aggiungere i seguenti ambiti granulari al Zoom server-to-server OAuth applicazione:

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

Se si utilizza un'applicazione creata in precedenza, è necessario aggiungere i seguenti ambiti classici:

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

Autorizzazioni delle app

ID tenant

AppFabric richiederà il tuo ID inquilino. L'ID del tenant in è AppFabric Zoom ID dell'account. Per trovare il tuo Zoom ID dell'account, procedi nel seguente modo:

1. Vai al Zoom mercato.
2. Scegli Gestisci.
3. Scegli l' server-to-server OAuth applicazione per cui utilizzi AppFabric.
4. Inserisci l'ID dell'account dalla pagina Credenziali dell'app nel campo ID tenant in. AppFabric

Nome dell'inquilino

Inserisci un nome che identifichi questo nome univoco Zoom organizzazione. AppFabric utilizza il nome del tenant per etichettare le autorizzazioni dell'app e le eventuali acquisizioni create dall'autorizzazione dell'app.

ID client

AppFabric richiederà il tuo ID cliente. Per trovare il tuo Zoom ID cliente, segui i seguenti passaggi:

1. Accedere a Zoom mercato.
2. Scegli Gestisci.
3. Scegli l' server-to-server OAuth applicazione per cui utilizzi AppFabric.
4. Inserisci l'ID client dalla pagina Credenziali dell'app nel campo ID client in AppFabric.

Client secret

AppFabric richiederà il segreto del tuo cliente. Per trovare il tuo Zoom client secret, segui i seguenti passaggi:

1. Vai al Zoom mercato.
2. Scegli Gestisci.

3. Scegli l' server-to-server OAuth applicazione per cui utilizzi AppFabric.
4. Inserisci il segreto del client dalla pagina Credenziali dell'app nel campo Segreto del client in AppFabric.

Controlla la consegna dei log

Zoom rende disponibili i log di controllo accedendo all'API ogni 24 ore. Quando si visualizzano i log di controllo con AppFabric, i dati visualizzati Zoom è per le attività del giorno precedente.

Strumenti e servizi di sicurezza compatibili AppFabric per la sicurezza

AWS AppFabric for security supporta l'integrazione con i seguenti strumenti e servizi di sicurezza. Scegli il nome di un servizio per ulteriori informazioni su come configurare AppFabric la sicurezza della connessione ad esso.

Argomenti

Barracuda XDR

Barracuda Networks è un partner affidabile e fornitore leader di soluzioni di sicurezza incentrate sul cloud, che protegge e-mail, reti, dati e applicazioni con soluzioni innovative che crescono e si adattano al percorso delle aziende. Barracuda XDR è una soluzione aperta e estesa di rilevamento e risposta che combina tecnologie sofisticate con un team di analisti della sicurezza nel nostro centro

operativo di sicurezza (SOC). Il Barracuda XDR la piattaforma analizza miliardi di eventi grezzi ogni giorno da oltre 40 fonti di dati integrate e, insieme a regole complete di rilevamento delle minacce che si adattano al framework MITRE ATT&CK®, è in grado di rilevare le minacce più rapidamente e ridurre i tempi di risposta.

AWS AppFabric verifica: considerazioni sull'ingestione dei log

Le seguenti sezioni descrivono lo schema AppFabric di output, i formati di output e le destinazioni di output da utilizzare con Barracuda XDR.

Schema e formato

Barracuda XDR supporta i seguenti schemi e formati di AppFabric output:

- OCSF - JSON: AppFabric normalizza i dati utilizzando Open Cybersecurity Schema Framework (OCSF) e restituisce i dati in formato JSON.

Posizioni di output

Barracuda XDR supporta la ricezione di registri di controllo da Amazon Security Lake. Per inviare dati da a AppFabric Barracuda XDR, seguendo le istruzioni riportate di seguito:

1. Invio di dati ad Amazon Security Lake: configura AppFabric l'invio di dati ad Amazon Security Lake tramite Amazon Data Firehose. Per ulteriori informazioni, consulta Amazon Security Lake.
2. Invia dati a Barracuda XDR: Configura Barracuda XDR per ricevere i log di controllo da Amazon Security Lake. Per ulteriori informazioni, consulta Configurazione e utilizzo di Amazon Security Lake.

Dynatrace

Il Dynatrace® Platform combina un'osservabilità ampia e approfondita e la sicurezza delle applicazioni a runtime continuo con funzionalità avanzate AIOps per fornire risposte e un'automazione intelligente a partire dai dati. Ciò consente agli innovatori di modernizzare e automatizzare le operazioni cloud, fornire software in modo più rapido e sicuro e garantire esperienze digitali impeccabili.

AWS AppFabric verifica le considerazioni relative all'inserimento dei log

Le sezioni seguenti descrivono lo schema AppFabric di output, i formati di output e le destinazioni di output da utilizzare con Dynatrace Platform.

Schema e formato

Il Dynatrace Platform supporta i seguenti schemi e formati di AppFabric output:

- OCSF - JSON: AppFabric normalizza i dati utilizzando Open Cybersecurity Schema Framework (OCSF) e restituisce i dati in formato JSON.

Posizioni di output

Il Dynatrace Platform supporta la ricezione dei registri di controllo dalle seguenti posizioni AppFabric di output.

- Amazon Simple Storage Service (Amazon S3)
  - Per configurare il Dynatrace Platform per ricevere dati dal bucket Amazon S3 che contiene i log di controllo, segui le istruzioni del progetto S3 Log Forwarder di Dynatrace su GitHub.

Logz.io

Logz.io aiuta le aziende native del cloud a monitorare e proteggere i propri ambienti tramite Logz.ioPiattaforma Open 360: trasforma l'osservabilità e la sicurezza da un onere ad alto costo e di basso valore a un fattore di alto valore ed efficiente in termini di costi che abilita migliori risultati aziendali.

Logz.io Cloud SIEM affronta direttamente le principali sfide di sicurezza odierne, dal sovraccarico di dati all'onnipresente divario di competenze informatiche, tramite interrogazioni rapide, rilevamento multidimensionale e contenuti di sicurezza profondamente personalizzabili per aiutare a monitorare e indagare sull'intera estensione del tuo ambiente cloud, senza alcun degrado delle prestazioni, indipendentemente dai volumi di dati.

Il Logz.io la soluzione è stata creata appositamente per fornire analisi e indagini avanzate sulle minacce con minore complessità e costi. I clienti possono contare sul supporto di analisti di sicurezza dedicati, di content as a service sulle minacce e di funzionalità supportate dall'intelligenza artificiale, create appositamente per contribuire a ridurre il rumore dei dati e concentrarsi sulle informazioni che consentono al team di dare rapidamente priorità alle minacce del mondo reale.

AWS AppFabric verifica: considerazioni sull'ingestione dei log

Le seguenti sezioni descrivono lo schema AppFabric di output, i formati di output e le destinazioni di output da utilizzare con Logz.io.

Schema e formato

Logz.io supporta i seguenti schemi e formati di AppFabric output:

- Raw - JSON
  - AppFabric restituisce i dati nello schema originale utilizzato dall'applicazione sorgente in formato JSON.
- OCSF - JSON
  - AppFabric normalizza i dati utilizzando Open Cybersecurity Schema Framework (OCSF) e li restituisce in formato JSON.

Posizioni di output

Logz.io supporta le seguenti posizioni AppFabric di output:

- Amazon Data Firehose
  - Per configurare il flusso di distribuzione di Firehose in modo che invii dati a Logz.io, segui le istruzioni in Scegli Logz.io per la tua destinazione nella Amazon Data Firehose Developer Guide.
- Amazon Simple Storage Service (Amazon S3)
  - Per configurare Logz.io per ricevere dati dal bucket Amazon S3 che contiene i log di controllo, segui le istruzioni in Configurare un bucket Amazon S3 sul Logz.io sito web.

Netskope

Netskope, leader globale nella sicurezza informatica, sta ridefinendo la sicurezza del cloud, dei dati e della rete per aiutare le organizzazioni ad applicare i principi zero trust per proteggere i dati. Veloce e facile da usare, il Netskope la piattaforma offre un accesso ottimizzato e una sicurezza zero trust per persone, dispositivi e dati ovunque si trovino. Netskope aiuta i clienti a ridurre i rischi, accelerare le prestazioni e ottenere una visibilità senza pari su qualsiasi attività relativa alle applicazioni cloud, web e private. Migliaia di clienti, tra cui oltre 25 delle aziende Fortune 100, si fidano Netskope e la sua potente NewEdge rete per affrontare minacce in evoluzione, nuovi rischi, cambiamenti tecnologici,

cambiamenti organizzativi e di rete e nuovi requisiti normativi. Scopri come Netskope aiuta i clienti a essere pronti a tutto nel loro percorso verso il SASE, visita netskope.com.

AWS AppFabric considerazioni sull'ingestione dei log di controllo

Le seguenti sezioni descrivono lo schema AppFabric di output, i formati di output e le destinazioni di output da utilizzare con Netskope.

Schema e formato

Netskope supporta i seguenti schemi e formati di AppFabric output:

- Raw - JSON
  - AppFabric restituisce i dati nello schema originale utilizzato dall'applicazione sorgente in formato JSON.
- OCSF - JSON
  - AppFabric normalizza i dati utilizzando Open Cybersecurity Schema Framework (OCSF) e li restituisce in formato JSON.

Posizioni di output

Netskope supporta la seguente posizione AppFabric di output:

- Amazon Simple Storage Service (Amazon S3)
  - Per configurare Netskope per ricevere dati dal bucket Amazon S3 che contiene i log di controllo, segui le istruzioni in Data Protection for Amazon Web Services S3 sul Netskope sito web.

NetWitness

NetWitness è uno sviluppatore leader di software XDR (Extended Detection and Response). La loro base globale di clienti altamente attenti alla sicurezza si affida a NetWitness XDR per difendersi da avversari sofisticati e aggressivi. Con la piattaforma più completa, integrata e matura del settore per rilevare, indagare e rispondere agli attacchi digitali, NetWitness XDR è la base unificante di un SOC moderno ed efficace.

Grazie alla sua architettura altamente modulare, NetWitness XDR rileva le minacce ovunque si verifichino: nel cloud, in locale, con lavoratori mobili e remoti o ovunque si trovino. Il NetWitness Platform XDR offre una visibilità completa combinata con l'intelligence applicata sulle minacce e

l'analisi del comportamento degli utenti per rilevare le minacce, dare priorità alle attività, indagare e automatizzare la risposta. Tutto ciò offre agli analisti della sicurezza un'efficienza migliore e più rapida per mantenere le operazioni di sicurezza ben al passo con le minacce che hanno un impatto sull'azienda.

AWS AppFabric verifica le considerazioni relative all'ingestione dei log

Le seguenti sezioni descrivono lo schema AppFabric di output, i formati di output e le destinazioni di output da utilizzare con NetWitness.

Schema e formato

NetWitness supporta i seguenti schemi e formati di AppFabric output:

- Raw - JSON
  - AppFabric restituisce i dati nello schema originale utilizzato dall'applicazione sorgente in formato JSON.
- OCSF - JSON
  - AppFabric normalizza i dati utilizzando Open Cybersecurity Schema Framework (OCSF) e li restituisce in formato JSON.

Posizioni di output

NetWitness supporta la seguente posizione AppFabric di output:

- Amazon Simple Storage Service (Amazon S3)
  - Per configurare NetWitness per ricevere dati dal bucket Amazon S3 che contiene i log di controllo, segui le istruzioni nella Guida alla configurazione del registro di origine degli eventi di S3 Universal Connector sul NetWitness Pagina dedicata alle integrazioni della piattaforma sul NetWitness sito web.

Amazon QuickSight

Amazon QuickSight alimenta le organizzazioni basate sui dati con business intelligence (BI) unificata su larga scala. Con QuickSight, tutti gli utenti possono soddisfare le diverse esigenze analitiche dalla stessa fonte di verità attraverso dashboard interattivi moderni, report impaginati, analisi integrate e query in linguaggio naturale. Puoi analizzare i dati dei log di AWS AppFabric controllo scegliendo

come origine il tuo bucket Amazon Simple Storage Service (Amazon S3) in cui AppFabric sono archiviati i log di sicurezza. QuickSight

AppFabric considerazioni sull'ingestione dei log di controllo

Le sezioni seguenti descrivono lo schema AppFabric di output, i formati di output e le destinazioni di output con cui utilizzare. QuickSight

Schema e formati

QuickSight supporta i seguenti schemi e formati di AppFabric output:

- Raw - JSON
  - AppFabric restituisce i dati nello schema originale utilizzato dall'applicazione sorgente in formato JSON.
- OCSF - JSON-JSON-
  - AppFabric normalizza i dati utilizzando Open Cybersecurity Schema Framework (OCSF) e li restituisce in formato JSON.

Posizioni di output

QuickSight supporta le seguenti posizioni AppFabric di output:

- Amazon S3
  - Puoi importare dati da Amazon S3 direttamente QuickSight in Amazon S3 creando un set di dati utilizzando file Amazon S3. Per verificare che il set di file di destinazione non superi le quote di origine QuickSight dati, consulta la sezione Quote di origine dati nella Guida per l'utente. QuickSight
  - Se il set di file supera le QuickSight quote per un'origine dati Amazon S3, puoi importare i dati in Amazon S3 utilizzando Amazon Athena e tabelle. AWS Glue L'utilizzo di Athena nel QuickSight set di dati comporta costi aggiuntivi. Per ulteriori informazioni sui prezzi di Athena, consulta Prezzi di Athena.

    Per usare Athena:

    1. Segui le istruzioni in Utilizzo AWS Glue per la connessione a sorgenti di dati in Amazon S3 nella Guida per l'utente di Athena.
    2. Segui le istruzioni riportate nella sezione Creazione di un set di dati utilizzando i dati di Athena nella Guida per QuickSight l'utente.

Rapid7

Rapid7, Inc. ha la missione di creare un mondo digitale più sicuro rendendo la sicurezza informatica più semplice e accessibile. Rapid7 consente ai professionisti della sicurezza di gestire una superficie di attacco moderna attraverso la best-in-class tecnologia, la ricerca all'avanguardia e un'ampia esperienza strategica. Rapid7le soluzioni di sicurezza complete aiutano più di 10.000 clienti globali a unire la gestione del rischio nel cloud e il rilevamento delle minacce per ridurre le superfici di attacco ed eliminare le minacce con velocità e precisione.

AWS AppFabric verifica le considerazioni relative all'inserimento dei log

Le seguenti sezioni descrivono lo schema AppFabric di output, il formato di output e le destinazioni di output da utilizzare con Rapid7.

Schema e formato

Rapid7 supporta i seguenti schemi e formati di AppFabric output:

- Raw - JSON
  - AppFabric restituisce i dati nello schema originale utilizzato dall'applicazione sorgente in formato JSON.
- OCSF - JSON
  - AppFabric normalizza i dati utilizzando Open Cybersecurity Schema Framework (OCSF) e li restituisce in formato JSON.

Posizioni di output

Rapid7 supporta la seguente posizione AppFabric di output:

- Amazon Simple Storage Service (Amazon S3)
  - Per configurare Rapid7 per ricevere dati dal bucket Amazon S3 che contiene i log di controllo, segui le istruzioni contenute nel post di blog How to Monitor Your Amazon S3 Activity with InsightIDR sul Rapid7 Sito web del blog.

Amazon Security Lake

Amazon Security Lake centralizza automaticamente i dati di sicurezza provenienti da AWS ambienti, fornitori di software as a service (SaaS), fonti locali e cloud in un data lake appositamente creato e

archiviato nel tuo. Account AWS Con Security Lake, puoi ottenere una comprensione più completa dei tuoi dati di sicurezza in tutta l'organizzazione. Security Lake ha adottato l'Open Cybersecurity Schema Framework (OCSF), uno schema di eventi di sicurezza open source. Con il supporto OCSF, il servizio normalizza e combina i dati di sicurezza provenienti da AWS un'ampia gamma di fonti di dati di sicurezza aziendali.

AppFabric verifica: considerazioni sull'ingestione dei log

Puoi inserire i log di controllo SaaS in Amazon Security Lake direttamente Account AWS da te aggiungendo una fonte personalizzata a Security Lake. Le seguenti sezioni descrivono lo schema AppFabric di output, il formato di output e le destinazioni di output da utilizzare con Security Lake.

Schema e formato

Security Lake supporta lo schema e il formato di AppFabric output seguenti:

- OCSF - JSON
  - AppFabric normalizza i dati utilizzando Open Cybersecurity Schema Framework (OCSF) e li restituisce in formato JSON.

Posizioni di output

Security Lake supporta AppFabric come origine personalizzata l'utilizzo di un flusso di distribuzione Amazon Data Firehose come posizione di output di AppFabric ingestione. Per configurare la AWS Glue tabella e il flusso di distribuzione di Firehose e per configurare un'origine personalizzata in Security Lake, utilizzare le seguenti procedure.

Creare una tabella AWS Glue

1. Accedi ad Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e crea un bucket con un nome a tua scelta.
2. Passa alla console. AWS Glue
3. Per Data Catalog, vai alla sezione Tabelle e scegli Aggiungi tabella.
4. Inserisci un nome a tua scelta per questa tabella.
5. Seleziona il bucket Amazon S3 che hai creato nel passaggio 1.
6. Per il formato dei dati, seleziona JSON e scegli Avanti.
7. Nella pagina Scegli o definisci lo schema, scegli Modifica schema come JSON.
8. Inserisci lo schema seguente e completa il processo di creazione della AWS Glue tabella.

```
[
    {
        "Name": "message",
        "Type": "string"
    },
    {
        "Name": "process",
        "Type":
 "struct<name:string,pid:int,user:struct<name:string,type:string,domain:string,uid:string,t
    },
    {
        "Name": "status",
        "Type": "string"
    },
    {
        "Name": "time",
        "Type": "bigint"
    },
    {
        "Name": "device",
        "Type":
 "struct<name:string,owner:struct<name:string,type:string,uid:string,type_id:int,risk_level
    },
    {
        "Name": "metadata",
        "Type":
 "struct<version:string,product:struct<name:string,version:string,uid:string,data_classific
    },
    {
        "Name": "severity",
        "Type": "string"
    },
    {
        "Name": "duration",
        "Type": "int"
    },
    {
        "Name": "type_name",
        "Type": "string"
    },
    {
        "Name": "activity_id",
        "Type": "int"
```

```
    },
    {
        "Name": "type_uid",
        "Type": "int"
    },
    {
        "Name": "observables",
        "Type": "array<struct<name:string,type:string,type_id:int,value:string>>"
    },
    {
        "Name": "category_name",
        "Type": "string"
    },
    {
        "Name": "class_uid",
        "Type": "int"
    },
    {
        "Name": "category_uid",
        "Type": "int"
    },
    {
        "Name": "class_name",
        "Type": "string"
    },
    {
        "Name": "timezone_offset",
        "Type": "int"
    },
    {
        "Name": "end_time",
        "Type": "bigint"
    },
    {
        "Name": "activity_name",
        "Type": "string"
    },
    {
        "Name": "cloud",
        "Type":
"struct<account:struct<name:string,type:string,uid:string,type_id:int>,project_uid:string,
    },
    {
        "Name": "query_info",
```

```
        "Type": "struct<name:string,uid:string,query_string:string>"
    },
    {
        "Name": "query_result",
        "Type": "string"
    },
    {
        "Name": "query_result_id",
        "Type": "int"
    },
    {
        "Name": "severity_id",
        "Type": "int"
    },
    {
        "Name": "status_code",
        "Type": "string"
    },
    {
        "Name": "status_detail",
        "Type": "string"
    },
    {
        "Name": "status_id",
        "Type": "int"
    },
    {
        "Name": "network_interfaces",
        "Type":
"array<struct<name:string,type:string,hostname:string,mac:string,type_id:int,ip:string>>"
    },
    {
        "Name": "file",
        "Type":
"struct<attributes:int,name:string,type:string,path:string,type_id:int,accessor:struct<nam
    },
    {
        "Name": "actor",
        "Type":
"struct<process:struct<pid:int,file:struct<name:string,size:bigint,type:string,version:str
    },
    {
        "Name": "dst_endpoint",
```

```
        "Type":
"struct<owner:struct<name:string,type:string,uid:string,type_id:int,full_name:string,risk_
    },
    {
        "Name": "src_endpoint",
        "Type":
"struct<name:string,owner:struct<name:string,type:string,domain:string,uid:string,org:stru
    },
    {
        "Name": "user",
        "Type":
"struct<name:string,type:string,groups:array<struct<name:string,uid:string>>,type_id:int>"
    },
    {
        "Name": "resource",
        "Type":
"struct<version:string,uid:string,agent_list:array<struct<name:string,type:string,uid:stri
    },
    {
        "Name": "privileges",
        "Type": "array<string>"
    },
    {
        "Name": "action",
        "Type": "string"
    },
    {
        "Name": "action_id",
        "Type": "int"
    },
    {
        "Name": "protocol_ver",
        "Type": "string"
    },
    {
        "Name": "proxy",
        "Type":
"struct<name:string,port:int,type:string,ip:string,hostname:string,uid:string,type_id:int,
    },
    {
        "Name": "client_hassh",
        "Type":
"struct<algorithm:string,fingerprint:struct<value:string,algorithm:string,algorithm_id:int
    },
```

```
    {
        "Name": "authorizations",
        "Type": "array<string>"
    },
    {
        "Name": "proxy_tls",
        "Type":
"struct<version:string,certificate:struct<version:string,uid:string,subject:string,issuer:
    },
    {
        "Name": "load_balancer",
        "Type":
"struct<name:string,classification:string,dst_endpoint:struct<owner:struct<type:string,dom
    },
    {
        "Name": "disposition_id",
        "Type": "int"
    },
    {
        "Name": "disposition",
        "Type": "string"
    },
    {
        "Name": "proxy_traffic",
        "Type": "struct<bytes:bigint,packets:int>"
    },
    {
        "Name": "auth_type_id",
        "Type": "int"
    },
    {
        "Name": "proxy_http_response",
        "Type": "struct<code:int,message:string,status:string,length:int>"
    },
    {
        "Name": "server_hassh",
        "Type":
"struct<algorithm:string,fingerprint:struct<value:string,algorithm:string,algorithm_id:int
    },
    {
        "Name": "auth_type",
        "Type": "string"
    },
    {
```

```
        "Name": "firewall_rule",
        "Type": "struct<version:string,uid:string>"
    },
    {
        "Name": "proxy_connection_info",
        "Type":
"struct<direction:string,direction_id:int,protocol_num:int,protocol_ver:string>"
    },
    {
        "Name": "connection_info",
        "Type": "struct<direction:string,direction_id:int>"
    },
    {
        "Name": "api",
        "Type":
"struct<request:struct<data:string,uid:string>,response:struct<error:string,code:int,messa
    },
    {
        "Name": "attacks",
        "Type":
"array<struct<version:string,tactics:array<struct<name:string,uid:string>>,technique:struc
    },
    {
        "Name": "raw_data",
        "Type": "string"
    },
    {
        "Name": "email_uid",
        "Type": "string"
    },
    {
        "Name": "malware",
        "Type":
"array<struct<name:string,path:string,uid:string,classification_ids:array<int>,cves:array<
    },
    {
        "Name": "start_time_dt",
        "Type": "string"
    },
    {
        "Name": "direction",
        "Type": "string"
    },
    {
```

```
        "Name": "smtp_hello",
        "Type": "string"
    },
    {
        "Name": "unmapped",
        "Type": "string"
    },
    {
        "Name": "direction_id",
        "Type": "int"
    },
    {
        "Name": "email_auth",
        "Type":
"struct<spf:string,dkim:string,dkim_domain:string,dkim_signature:string,dmarc:string,dmarc
    },
    {
        "Name": "email",
        "Type":
"struct<uid:string,from:string,to:array<string>,data_classification:struct<category:string
    },
    {
        "Name": "impact_id",
        "Type": "int"
    },
    {
        "Name": "resources",
        "Type":
"array<struct<owner:struct<name:string,type:string,uid:string,type_id:int,full_name:string
    },
    {
        "Name": "finding_info",
        "Type":
"struct<title:string,uid:string,attacks:array<struct<version:string,tactics:array<struct<n
    },
    {
        "Name": "evidences",
        "Type":
"array<struct<process:struct<name:string,pid:int,file:struct<name:string,type:string,versi
    },
    {
        "Name": "impact",
        "Type": "string"
    },
```

```
    {
        "Name": "count",
        "Type": "int"
    },
    {
        "Name": "confidence_id",
        "Type": "int"
    },
    {
        "Name": "enrichments",
        "Type":
"array<struct<data:string,name:string,type:string,value:string,provider:string>>"
    },
    {
        "Name": "rcode",
        "Type": "string"
    },
    {
        "Name": "app_name",
        "Type": "string"
    },
    {
        "Name": "rcode_id",
        "Type": "int"
    },
    {
        "Name": "query",
        "Type":
"struct<type:string,hostname:string,class:string,opcode_id:int,packet_uid:int>"
    },
    {
        "Name": "proxy_endpoint",
        "Type":
"struct<name:string,owner:struct<name:string,type:string,domain:string,uid:string,groups:a
    },
    {
        "Name": "response_time",
        "Type": "bigint"
    },
    {
        "Name": "delay",
        "Type": "int"
    },
    {
```

```
        "Name": "start_time",
        "Type": "bigint"
    },
    {
        "Name": "proxy_http_request",
        "Type":
"struct<version:string,url:struct<port:int,scheme:string,path:string,hostname:string,query
    },
    {
        "Name": "version",
        "Type": "string"
    },
    {
        "Name": "stratum",
        "Type": "string"
    },
    {
        "Name": "stratum_id",
        "Type": "int"
    },
    {
        "Name": "dispersion",
        "Type": "int"
    },
    {
        "Name": "traffic",
        "Type":
"struct<bytes_out:int,chunks:bigint,bytes:int,packets:int,packets_in:bigint>"
    },
    {
        "Name": "precision",
        "Type": "int"
    },
    {
        "Name": "size",
        "Type": "int"
    },
    {
        "Name": "actual_permissions",
        "Type": "int"
    },
    {
        "Name": "base_address",
        "Type": "string"
```

```
    },
    {
        "Name": "requested_permissions",
        "Type": "int"
    },
    {
        "Name": "end_time_dt",
        "Type": "string"
    },
    {
        "Name": "compliance",
        "Type":
"struct<control:string,status:string,standards:array<string>,status_id:int>"
    },
    {
        "Name": "remediation",
        "Type": "struct<desc:string>"
    },
    {
        "Name": "kb_article_list",
        "Type":
"array<struct<os:struct<name:string,type:string,type_id:int,cpe_name:string,edition:string
    },
    {
        "Name": "peripheral_device",
        "Type":
"struct<name:string,class:string,uid:string,model:string,serial_number:string,vendor_name:
    },
    {
        "Name": "time_dt",
        "Type": "string"
    },
    {
        "Name": "group",
        "Type": "struct<name:string,type:string,uid:string>"
    },
    {
        "Name": "users",
        "Type":
"array<struct<name:string,type:string,uid:string,type_id:int,risk_level:string,risk_level_
    },
    {
        "Name": "confidence_score",
        "Type": "int"
```

```
    },
    {
        "Name": "state",
        "Type": "string"
    },
    {
        "Name": "state_id",
        "Type": "int"
    },
    {
        "Name": "evidence",
        "Type": "string"
    },
    {
        "Name": "confidence",
        "Type": "string"
    },
    {
        "Name": "risk_level",
        "Type": "string"
    },
    {
        "Name": "risk_score",
        "Type": "int"
    },
    {
        "Name": "impact_score",
        "Type": "int"
    },
    {
        "Name": "risk_level_id",
        "Type": "int"
    },
    {
        "Name": "finding",
        "Type":
"struct<title:string,uid:string,modified_time:bigint,modified_time_dt:string,first_seen_ti
    },
    {
        "Name": "user_result",
        "Type":
"struct<name:string,type:string,uid:string,type_id:int,account:struct<name:string,uid:stri
    },
    {
```

```
        "Name": "codes",
        "Type": "array<int>"
    },
    {
        "Name": "command",
        "Type": "string"
    },
    {
        "Name": "type",
        "Type": "string"
    },
    {
        "Name": "kernel",
        "Type": "struct<name:string,type:string,type_id:int>"
    },
    {
        "Name": "http_response",
        "Type":
"struct<code:int,status:string,http_headers:array<struct<name:string,value:string>>>"
    },
    {
        "Name": "http_request",
        "Type":
"struct<url:struct<scheme:string,path:string,hostname:string,query_string:string,category_
    },
    {
        "Name": "tls",
        "Type":
"struct<version:string,certificate:struct<subject:string,issuer:string,fingerprints:array<
    },
    {
        "Name": "web_resources",
        "Type":
"array<struct<name:string,type:string,data_classification:struct<category:string,category_
    },
    {
        "Name": "http_cookies",
        "Type":
"array<struct<name:string,value:string,is_http_only:boolean,is_secure:boolean,samesite:str
    },
    {
        "Name": "type_id",
        "Type": "int"
    },
```

```
    {
        "Name": "databucket",
        "Type":
"struct<name:string,type:string,file:struct<attributes:int,name:string,owner:struct<name:s
    },
    {
        "Name": "table",
        "Type": "struct<uid:string,created_time_dt:string>"
    },
    {
        "Name": "session",
        "Type":
"struct<count:int,uid:string,uuid:string,issuer:string,created_time:bigint,is_remote:boole
    },
    {
        "Name": "certificate",
        "Type":
"struct<version:string,uid:string,subject:string,issuer:string,fingerprints:array<struct<v
    },
    {
        "Name": "is_mfa",
        "Type": "boolean"
    },
    {
        "Name": "logon_type_id",
        "Type": "int"
    },
    {
        "Name": "auth_protocol_id",
        "Type": "int"
    },
    {
        "Name": "logon_type",
        "Type": "string"
    },
    {
        "Name": "is_remote",
        "Type": "boolean"
    },
    {
        "Name": "is_cleartext",
        "Type": "boolean"
    },
    {
```

```
        "Name": "auth_protocol",
        "Type": "string"
    },
    {
        "Name": "is_renewal",
        "Type": "boolean"
    },
    {
        "Name": "lease_dur",
        "Type": "int"
    },
    {
        "Name": "relay",
        "Type":
"struct<name:string,type:string,ip:string,mac:string,namespace:string,type_id:int>"
    },
    {
        "Name": "transaction_uid",
        "Type": "string"
    },
    {
        "Name": "file_result",
        "Type":
"struct<name:string,size:int,type:string,path:string,desc:string,product:struct<name:strin
    },
    {
        "Name": "file_diff",
        "Type": "string"
    },
    {
        "Name": "create_mask",
        "Type": "string"
    },
    {
        "Name": "web_resources_result",
        "Type":
"array<struct<type:string,data_classification:struct<category:string,category_id:int,confi
    },
    {
        "Name": "app",
        "Type":
"struct<name:string,version:string,uid:string,data_classification:struct<category:string,c
    },
    {
```

```
        "Name": "src_url",
        "Type": "string"
    },
    {
        "Name": "priority_id",
        "Type": "int"
    },
    {
        "Name": "verdict",
        "Type": "string"
    },
    {
        "Name": "desc",
        "Type": "string"
    },
    {
        "Name": "verdict_id",
        "Type": "int"
    },
    {
        "Name": "priority",
        "Type": "string"
    },
    {
        "Name": "finding_info_list",
        "Type":
"array<struct<title:string,uid:string,attacks:array<struct<version:string,tactics:array<st
    },
    {
        "Name": "expiration_time_dt",
        "Type": "string"
    },
    {
        "Name": "expiration_time",
        "Type": "bigint"
    },
    {
        "Name": "comment",
        "Type": "string"
    },
    {
        "Name": "entity",
        "Type": "struct<data:string,name:string,version:string,uid:string>"
    },
```

```
    {
        "Name": "entity_result",
        "Type":
"struct<data:string,name:string,type:string,version:string,uid:string>"
    },
    {
        "Name": "module",
        "Type":
"struct<type:string,file:struct<name:string,type:string,path:string,desc:string,type_id:in
    },
    {
        "Name": "exit_code",
        "Type": "int"
    },
    {
        "Name": "injection_type",
        "Type": "string"
    },
    {
        "Name": "injection_type_id",
        "Type": "int"
    },
    {
        "Name": "request",
        "Type": "struct<uid:string>"
    },
    {
        "Name": "response",
        "Type": "struct<error:string,code:int,message:string,error_message:string>"
    },
    {
        "Name": "driver",
        "Type":
"struct<file:struct<name:string,type:string,version:string,path:string,type_id:int,parent_
    },
    {
        "Name": "prev_security_states",
        "Type": "array<string>"
    },
    {
        "Name": "security_states",
        "Type": "array<string>"
    },
    {
```

```
        "Name": "folder",
        "Type":
"struct<name:string,type:string,path:string,desc:string,type_id:int,mime_type:string,paren
    },
    {
        "Name": "url",
        "Type":
"struct<port:int,scheme:string,path:string,hostname:string,query_string:string,resource_ty
    },
    {
        "Name": "tunnel_type_id",
        "Type": "int"
    },
    {
        "Name": "tunnel_type",
        "Type": "string"
    },
    {
        "Name": "protocol_name",
        "Type": "string"
    },
    {
        "Name": "job",
        "Type":
"struct<name:string,file:struct<name:string,type:string,path:string,signature:struct<certi
    },
    {
        "Name": "num_trusted_items",
        "Type": "int"
    },
    {
        "Name": "command_uid",
        "Type": "string"
    },
    {
        "Name": "num_registry_items",
        "Type": "int"
    },
    {
        "Name": "num_network_items",
        "Type": "int"
    },
    {
        "Name": "schedule_uid",
```

```
        "Type": "string"
    },
    {
        "Name": "num_resolutions",
        "Type": "int"
    },
    {
        "Name": "scan",
        "Type": "struct<name:string,type:string,type_id:int>"
    },
    {
        "Name": "num_detections",
        "Type": "int"
    },
    {
        "Name": "num_processes",
        "Type": "int"
    },
    {
        "Name": "num_files",
        "Type": "int"
    },
    {
        "Name": "total",
        "Type": "int"
    },
    {
        "Name": "num_folders",
        "Type": "int"
    },
    {
        "Name": "dce_rpc",
        "Type":
"struct<command:string,flags:array<string>,command_response:string,opnum:int,rpc_interface
    },
    {
        "Name": "share",
        "Type": "string"
    },
    {
        "Name": "client_dialects",
        "Type": "array<string>"
    },
    {
```

```
        "Name": "open_type",
        "Type": "string"
    },
    {
        "Name": "tree_uid",
        "Type": "string"
    },
    {
        "Name": "share_type_id",
        "Type": "int"
    },
    {
        "Name": "share_type",
        "Type": "string"
    },
    {
        "Name": "dialect",
        "Type": "string"
    },
    {
        "Name": "cis_benchmark_result",
        "Type": "struct<name:string>"
    },
    {
        "Name": "vulnerabilities",
        "Type":
 "array<struct<references:array<string>,severity:string,affected_packages:array<struct<name
    },
    {
        "Name": "service",
        "Type": "struct<name:string,uid:string>"
    },
    {
        "Name": "data_security",
        "Type":
 "struct<category:string,pattern_match:string,category_id:int,confidentiality:string,confid
    },
    {
        "Name": "database",
        "Type":
 "struct<name:string,type:string,uid:string,type_id:int,data_classification:struct<category
    }
]
```

Crea una fonte personalizzata in Security Lake

1. Passa alla console Amazon Security Lake.
2. Seleziona Fonti personalizzate nel riquadro di navigazione.
3. Scegli Crea fonte personalizzata.
4. Inserisci un nome per la tua fonte personalizzata e seleziona una classe di eventi OCSF applicabile.

   > **Note**
   >
   > AppFabric utilizza le classi di eventi Account Change, Authentication, User Access Management, Group Management, Web Resources Activity e Web Resource Access Activity.

5. Sia per Account AWS ID che per ID esterno, inserisci il tuo Account AWS ID. Quindi scegli Create (Crea).
6. Salva la posizione Amazon S3 dell'origine personalizzata. Lo utilizzerai per configurare un flusso di distribuzione di Amazon Data Firehose.

Creare un flusso di distribuzione in Firehose

1. Accedi alla console Amazon Data Firehose.
2. Scegli Crea un flusso di distribuzione.
3. Per Source, seleziona Direct PUT.
4. Per Destinazione, scegli S3.
5. Nella sezione Trasforma e converti i record, scegli Abilita la conversione del formato di record e scegli Apache Parquetcome formato di output.
6. Per AWS Glue tabella, scegliete la AWS Glue tabella creata nella procedura precedente e scegliete la versione più recente.
7. Per le impostazioni di destinazione, scegli il bucket Amazon S3 che hai creato con l'origine personalizzata Security Lake.
8. Per il partizionamento dinamico, scegli Abilitato.
9. Per l'analisi in linea per JSON, scegli Abilitato.

   - Per Keyname, inserisci. `eventDayValue`

- Per JQ Expression, immettere. `(.time/1000)|strftime("%Y%m%d")`

10. Per il prefisso del bucket S3, immettete il seguente valore.

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

Sostituisci *<custom source name>* *<region>* e inserisci *<account_id>* il nome sorgente e l'ID personalizzati di Security Lake. Regione AWS Account AWS

11. Per il prefisso di output degli errori del bucket S3, inserisci il seguente valore.

```
ext/AppFabric/error/
```

12. Per la durata di Riprova, seleziona 300.
13. Per la dimensione del buffer, selezionare 128 MiB.
14. Per l'intervallo Buffer, selezionate 60s.
15. Completa il processo di creazione del flusso di distribuzione di Firehose.

Crea ingestioni AppFabric

Per inviare dati ad Amazon Security Lake, devi creare un'importazione nella AppFabric console che utilizzi il flusso di distribuzione Firehose creato in precedenza come posizione di output. Per ulteriori informazioni sulla configurazione delle AppFabric acquisizioni per utilizzare Firehose come posizione di output, vedere Create an output location.

Singularity Cloud

Il Singularity Cloud la piattaforma protegge la tua azienda dalle minacce di tutte le categorie, in tutte le fasi. La sua IA (Artificial Intelligence) brevettata estende la sicurezza dalle firme e dai modelli noti agli attacchi più sofisticati, come zero-day e ransomware.

AWS AppFabric verifica: considerazioni sull'inserimento dei log

Le seguenti sezioni descrivono lo schema AppFabric di output, i formati di output e le destinazioni di output da utilizzare con Singularity Cloud.

Schema e formato

Singularity Cloud supporta i seguenti schemi e formati di AppFabric output:

OCSF - JSON: AppFabric normalizza i dati utilizzando Open Cybersecurity Schema Framework (OCSF) e restituisce i dati in formato JSON.

Posizioni di output

Singularity Cloud supporta la ricezione dei registri di controllo dalle seguenti posizioni AppFabric di output.

- Amazon Simple Storage Service (Amazon S3)
  - Per configurare Singularity Cloud per ricevere dati dal bucket Amazon S3 che contiene i log di controllo, segui le istruzioni in Singularity Cloud’s documentazione.

Splunk

Splunk aiuta a rendere le organizzazioni più resilienti. Le organizzazioni leader utilizzano Splunkè la piattaforma unificata di sicurezza e osservabilità per mantenere i propri sistemi digitali sicuri e affidabili. Organizzazioni si fidano Splunk per evitare che i problemi relativi alla sicurezza, all'infrastruttura e alle applicazioni diventino gravi, assorbire gli shock causati dalle interruzioni digitali e accelerare la trasformazione digitale.

AWS AppFabric verifica: considerazioni sull'ingestione dei log

Le seguenti sezioni descrivono lo schema AppFabric di output, i formati di output e le destinazioni di output da utilizzare con Splunk.

Schema e formato

Splunk supporta i seguenti schemi e formati di AppFabric output:

- Raw - JSON
  - AppFabric restituisce i dati nello schema originale utilizzato dall'applicazione sorgente in formato JSON.
- OCSF - JSON
  - AppFabric normalizza i dati utilizzando Open Cybersecurity Schema Framework (OCSF) e li restituisce in formato JSON.
- OCSF - Parquet
  - AppFabric normalizza i dati utilizzando l'Open Cybersecurity Schema Framework (OCSF) e restituisce i dati nel Apache Parquet .

Posizioni di output

Splunk supporta le seguenti posizioni AppFabric di output:

- Amazon Data Firehose
  - Per configurare Splunk per ricevere i log di controllo dallo stream Firehose che contiene i log di controllo, segui le istruzioni in Splunk Componente aggiuntivo per Amazon Data Firehose su Splunk sito web.
- Amazon Simple Storage Service (Amazon S3)
  - Per configurare Splunk per ricevere dati dal bucket Amazon S3 che contiene i log di controllo, segui le istruzioni in Configurare gli input S3 basati su SQS per Splunk Componente aggiuntivo per su AWS Splunk sito web.

Elimina AWS AppFabric per risorse di sicurezza

Se non vuoi continuare a utilizzare AWS AppFabric per motivi di sicurezza, assicurati di eliminare i dati nelle posizioni di output che hai creato durante la configurazione e le risorse di sicurezza AppFabric per evitare di incorrere in costi aggiuntivi. Per ripulire le AppFabric risorse, è necessario eliminare le risorse nell'ordine inverso in cui sono state create per ogni applicazione SaaS (Software as a Service): Destinazioni di importazione > Inserimenti > Autorizzazione app > Pacchetti di app

Dopo aver eliminato l'autorizzazione finale dell'app, puoi eliminare il pacchetto dell'app.

Argomenti

- Eliminare una destinazione di importazione
- Eliminare un'ingestione
- Eliminare l'autorizzazione di un'app
- Eliminare un pacchetto di app

Eliminare una destinazione di importazione

Se si seleziona una posizione di output quando si crea un'ingestione, AppFabric per motivi di sicurezza crea le destinazioni di importazione per conto dell'utente. Per eliminare una destinazione di ingestione, effettuate le seguenti operazioni:

1. Apri la AppFabric console all'indirizzo. https://console.aws.amazon.com/appfabric/

2. Dalla pagina Guida introduttiva, espandi il menu a sinistra.
3. Scegli Ingestioni.
4. Scegli un'autorizzazione per l'app.
5. Seleziona il pulsante di opzione accanto alla destinazione che desideri eliminare e scegli Elimina.
6. Scegli Elimina nella finestra di dialogo di eliminazione della destinazione per confermare.
7. Ripeti i passaggi precedenti per tutte le tue destinazioni.

Eliminare un'ingestione

Per eliminare un'ingestione, attenersi alla seguente procedura:

1. Dalla pagina Guida introduttiva, espandi il menu a sinistra.
2. Scegli Ingestioni.
3. Seleziona il pulsante di opzione che si trova accanto all'autorizzazione dell'app.
4. Scegli il menu a discesa Operazione.
5. Scegliere Delete (Elimina).
6. Scegli Elimina nella finestra di dialogo di eliminazione per confermare.

Eliminare l'autorizzazione di un'app

Per eliminare l'autorizzazione di un'app, procedi nel seguente modo:

1. Dalla pagina Guida introduttiva, espandi il menu a sinistra.
2. Scegli Autorizzazioni per le app.
3. Seleziona il pulsante di opzione accanto all'autorizzazione dell'app che desideri eliminare.
4. Scegli il menu a discesa Operazione.
5. Scegliere Delete (Elimina).
6. Scegli Elimina nella finestra di dialogo di eliminazione per confermare.

Eliminare un pacchetto di app

Per eliminare il pacchetto di app, procedi nel seguente modo:

1. Dalla pagina Guida introduttiva, espandi il menu a sinistra.

2. Scegli App bundle.
3. Scegli il pulsante Elimina.
4. Digita `delete` per confermare, quindi scegli Elimina.

A cosa serve AWS AppFabric la produttività?

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

> **Note**
>
> Realizzato da Amazon Bedrock: AWS implementa il rilevamento automatico degli abusi. Poiché AWS AppFabric la produttività si basa su Amazon Bedrock, gli utenti ereditano i controlli implementati in Amazon Bedrock per rafforzare la sicurezza e l'uso responsabile dell'intelligenza artificiale.

AWS AppFabric for productivity (preview) aiuta a reimmaginare la produttività degli utenti finali nelle applicazioni di terze parti generando informazioni e azioni contestualizzate da più applicazioni. Gli sviluppatori di app riconoscono che l'accesso ai dati degli utenti da altre app è importante per creare un'esperienza più produttiva, ma non vogliono creare e gestire integrazioni con ogni applicazione. AppFabric Per la produttività, gli sviluppatori di applicazioni hanno accesso a sistemi di intelligenza artificiale generativa APIs che generano informazioni e azioni sui dati tra le app in modo da fornire esperienze più complete agli utenti finali attraverso assistenti di intelligenza artificiale generativi nuovi o esistenti. AppFabric for productivity integra i dati provenienti da più applicazioni, eliminando la necessità per gli sviluppatori di creare o mantenere integrazioni. point-to-point Gli sviluppatori di applicazioni possono integrare AppFabric la produttività direttamente nell'interfaccia utente dell'applicazione, mantenendo un'esperienza coerente per gli utenti finali e facendo emergere il contesto pertinente da altre applicazioni.

AppFabric per la produttività collega i dati provenienti da applicazioni di uso comune come Asana, Atlassian Jira Suite, Google Workspace, Microsoft 365, Miro, Slack, Smartsheete altro ancora. AppFabric for productivity offre agli sviluppatori di app un modo più semplice per creare esperienze di app più personalizzate che migliorano l'adozione, la soddisfazione e la fidelizzazione degli utenti. Nel frattempo, gli utenti finali traggono vantaggio dall'accesso alle informazioni di cui hanno bisogno da tutte le loro applicazioni senza interrompere il flusso di lavoro.

Argomenti

- Casi d'uso
- Accesso AppFabric per la produttività
- Guida introduttiva AppFabric alla produttività (anteprima) per gli sviluppatori di applicazioni
- Guida introduttiva alla AppFabric produttività (anteprima) per gli utenti finali
- AppFabric per la produttività APIs (anteprima)
- Elaborazione dei dati in AppFabric

Vantaggi

Grazie a AppFabric For Productivity, gli sviluppatori di applicazioni possono accedere a dati APIs che generano informazioni e azioni su più app, in modo da fornire esperienze più complete agli utenti finali attraverso assistenti di intelligenza artificiale generativi nuovi o esistenti.

- Un'unica fonte di dati utente tra app: AppFabric per la produttività integra i dati di più applicazioni eliminando la necessità per gli sviluppatori di creare o mantenere integrazioni. point-to-point I dati delle app SaaS vengono elaborati per essere utilizzati in altre applicazioni normalizzando automaticamente diversi tipi di dati in un formato comprensibile da qualsiasi applicazione, consentendo agli sviluppatori di app di incorporare più dati che migliorano effettivamente la produttività degli utenti finali.
- Controllo completo dell'esperienza utente: gli sviluppatori AppFabric integrano la produttività direttamente nell'interfaccia utente delle loro applicazioni, mantenendo il pieno controllo dell'esperienza utente e fornendo al contempo approfondimenti personalizzati e azioni consigliate agli utenti finali con il contesto di tutte le applicazioni. Ciò rende AppFabric la produttività disponibile nell'applicazione SaaS preferita dagli utenti finali ed è accessibile nell'app che preferiscono per completare le proprie attività. Gli utenti finali dedicano meno tempo a passare da un'app all'altra e possono rimanere concentrati sul flusso del proprio lavoro.
- Accelera il time-to-market: con una singola chiamata API, gli sviluppatori di app possono ricevere informazioni a livello di utente sui dati generati dall'utente senza dover mettere a punto un modello, scrivere un prompt personalizzato o creare integrazioni tra più applicazioni. AppFabric astrae questa complessità per consentire agli sviluppatori di app di creare, incorporare o arricchire più rapidamente le funzionalità di intelligenza artificiale generativa. Ciò consente agli sviluppatori di app di concentrarsi sulle proprie risorse per le attività più importanti.
- Riferimenti agli artefatti per creare la fiducia degli utenti: come parte dell'output AppFabric , per motivi di produttività, verranno evidenziati gli artefatti o i file sorgente pertinenti utilizzati per generare le informazioni necessarie per creare la fiducia dell'utente finale negli output LLM.

- Autorizzazioni utente semplificate: gli artefatti utente utilizzati per generare approfondimenti si basano su ciò a cui l'utente ha accesso. AppFabric per la produttività utilizza l'autorizzazione e il controllo degli accessi di un ISV come fonte di verità.

Casi d'uso

Gli sviluppatori di app possono utilizzare For Productivity AppFabric per reimmaginare la produttività all'interno delle loro applicazioni. AppFabric for productivity ne offre due APIs incentrate sui seguenti casi d'uso per aiutare gli utenti finali a essere più produttivi:

- Dai priorità alla tua giornata
  - L'API Actionable Insights aiuta gli utenti a gestire al meglio la loro giornata facendo emergere informazioni tempestive da tutte le loro applicazioni, tra cui e-mail, calendario, messaggi, attività e altro ancora. Inoltre, gli utenti possono eseguire azioni tra app come la creazione di e-mail, la pianificazione di riunioni e la creazione di azioni dalla loro applicazione preferita. Ad esempio, un dipendente che ha avuto un problema con i clienti durante la notte non solo vedrà un riepilogo delle conversazioni avvenute durante la notte, ma potrà anche visualizzare le azioni consigliate per pianificare un incontro con l'Account Manager del cliente. Le azioni sono precompilate con campi obbligatori (ad esempio nome e proprietario dell'attività o mittente/destinatario dell'e-mail), con la possibilità di modificare il contenuto precompilato prima di eseguire l'azione.
- Preparati per le prossime riunioni
  - L'API per la preparazione delle riunioni aiuta gli utenti a prepararsi al meglio per le riunioni riassumendo lo scopo della riunione e facendo emergere gli elementi pertinenti tra le app come e-mail, messaggi e altro. Gli utenti possono prepararsi rapidamente per le riunioni ora e non perdere tempo a passare da un'app all'altra per trovare contenuti.

Accesso AppFabric per la produttività

AppFabric for productivity è attualmente lanciato in anteprima e disponibile negli Stati Uniti orientali (Virginia settentrionale) Regione AWS. Per ulteriori informazioni su Regioni AWS, consulta AWS AppFabric endpoint e quote in. Riferimenti generali di AWS

In ogni regione, puoi accedere AppFabric alla produttività in uno dei seguenti modi:

- In qualità di sviluppatore di app
  - Guida introduttiva AppFabric alla produttività (anteprima) per gli sviluppatori di applicazioni

- Come utente finale
  - Guida introduttiva alla AppFabric produttività (anteprima) per gli utenti finali

Guida introduttiva AppFabric alla produttività (anteprima) per gli sviluppatori di applicazioni

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Questa sezione aiuta gli sviluppatori di app a integrarsi AWS AppFabric per la produttività (anteprima) nelle loro applicazioni. AWS AppFabric for productivity consente agli sviluppatori di creare esperienze di app più complete per i propri utenti generando informazioni e azioni basate sull'intelligenza artificiale da e-mail, eventi del calendario, attività, messaggi e altro ancora su più applicazioni. Per un elenco delle applicazioni supportate, consulta AWS AppFabric Applicazioni supportate.

AppFabric for productivity offre agli sviluppatori di app la possibilità di creare e sperimentare in un ambiente sicuro e controllato. Quando inizi a utilizzare AppFabric for productivity per la prima volta, crei AppClient e registri un singolo utente di test. Questo approccio è progettato per aiutarti a comprendere e testare il flusso di autenticazione e comunicazione tra l'applicazione e AppFabric. Dopo aver eseguito il test con un singolo utente, puoi inviare la tua applicazione AppFabric per la verifica prima di espandere l'accesso ad altri utenti (vediFase 5. Richiedi AppFabric di verificare la tua candidatura). AppFabric verificherà le informazioni sulle applicazioni prima di consentirne l'adozione su larga scala per proteggere gli sviluppatori di app, gli utenti finali e i relativi dati, aprendo la strada a un'espansione dell'adozione da parte degli utenti in modo responsabile.

Argomenti

- Risolvi i problemi per la AppClients produttività AppFabric

Prerequisiti

Prima di iniziare, devi creare un Account AWS. Per ulteriori informazioni, consulta Registrati per un Account AWS. È inoltre necessario creare almeno un utente con accesso alla policy `"appfabric:CreateAppClient"` IAM elencata di seguito, che consente all'utente di registrare l'applicazione con AppFabric. Per ulteriori informazioni sulla concessione delle autorizzazioni per le funzionalità AppFabric per la produttività, consulta. AppFabric per la produttività, esempi di policy IAM Avere un utente amministrativo è vantaggioso, ma non è obbligatorio per la configurazione iniziale. Per ulteriori informazioni, consulta Crea un utente con accesso amministrativo.

AppFabric for productivity è disponibile solo negli Stati Uniti orientali (Virginia settentrionale) durante l'anteprima. Assicurati di trovarti in questa regione prima di iniziare i passaggi seguenti.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Fase 1: Crea un piano AppFabric per la produttività AppClient

Prima di poter iniziare a raccogliere AppFabric informazioni sulla produttività all'interno della tua applicazione, devi creare un AppFabric AppClient. An AppClient è essenzialmente la porta di accesso AppFabric alla produttività, poiché funge da client OAuth applicativo sicuro che consente una comunicazione sicura tra l'applicazione e AppFabric. Quando ne crei uno AppClient, ti verrà fornito un AppClient ID, un identificatore univoco fondamentale per garantire che AppFabric sappia che funziona con la tua applicazione e con la tua Account AWS.

AppFabric for productivity offre agli sviluppatori di app la possibilità di creare e sperimentare in un ambiente sicuro e controllato. Quando inizi a utilizzare AppFabric for productivity per la prima

volta, crei AppClient e registri un singolo utente di test. Questo approccio è progettato per aiutarti a comprendere e testare il flusso di autenticazione e comunicazione tra l'applicazione e AppFabric. Dopo aver eseguito il test con un singolo utente, puoi inviare la tua applicazione AppFabric per la verifica prima di espandere l'accesso ad altri utenti (vediFase 5. Richiedi AppFabric di verificare la tua candidatura). AppFabric verificherà le informazioni sulle applicazioni prima di consentirne l'adozione su larga scala per proteggere gli sviluppatori di app, gli utenti finali e i relativi dati, aprendo la strada a un'espansione dell'adozione da parte degli utenti in modo responsabile.

Per crearne uno AppClient, utilizza l'operazione AWS AppFabric `CreateAppClient` API. Se è necessario aggiornare il file AppClient after, è possibile utilizzare l'operazione `UpdateAppClient` API per modificare solo gli URL di reindirizzamento. Se devi modificare uno qualsiasi degli altri parametri associati al tuo, AppClient come AppName o description, devi eliminarli AppClient e crearne uno nuovo. Per ulteriori informazioni, consulta CreateAppClient.

È possibile registrare l'applicazione con AWS i servizi utilizzando l'`CreateAppClient`API utilizzando diversi linguaggi di programmazione, tra cui Python, Node.js, Java, C#, Go e Rust. Per ulteriori informazioni, consulta Request signature examples nella IAM User Guide. È necessario utilizzare le credenziali della versione 4 della firma dell'account per eseguire questa operazione API. Per ulteriori informazioni sulla versione 4 della firma, consulta Signing AWS API request nella IAM User Guide.

Campi di richiesta

- `appName`- Il nome dell'applicazione che verrà visualizzato agli utenti nella pagina di consenso del portale AppFabric utenti. La pagina di consenso richiede agli utenti finali l'autorizzazione a visualizzare AppFabric informazioni dettagliate all'interno dell'applicazione. Per i dettagli sulla pagina di consenso, consultaFase 2: Fornisci il consenso affinché l'app mostri approfondimenti.
- `description`- Una descrizione dell'applicazione.
- `redirectUrls`- L'URI a cui reindirizzare gli utenti finali dopo l'autorizzazione. È possibile aggiungere fino a 5 URL di reindirizzamento. Ad esempio, `https://localhost:8080`.
- `starterUserEmails`- Un indirizzo email utente a cui sarà consentito l'accesso per ricevere gli approfondimenti fino alla verifica dell'applicazione. È consentito un solo indirizzo e-mail. Ad esempio, `anyuser@example.com`
- `customerManagedKeyIdentifier`(opzionale) - L'ARN della chiave gestita dal cliente (generata da KMS) da utilizzare per crittografare i dati. Se non specificato, verrà utilizzata la chiave AWS AppFabric gestita. Per ulteriori informazioni sulle chiavi Chiavi di proprietà di AWS gestite dal cliente, consulta Customer keys and AWS keys nella AWS Key Management Service Developer Guide.

Campi di risposta

- `appClientArn`- L'Amazon Resource Name (ARN) che include l' AppClient ID. Ad esempio, l' AppClient ID è`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
- `verificationStatus`- Lo stato AppClient della verifica.
  - `pending_verification`- La verifica di AppClient è ancora in corso con AppFabric. Fino alla AppClient verifica, solo un utente (specificato in`starterUserEmails`) può utilizzare il AppClient. L'utente vedrà una notifica nel portale AppFabric utente, introdotta inFase 3. Aggiungi l'URL del portale AppFabric utente alla tua applicazione, che indica che l'applicazione non è verificata.
  - `verified`- Il processo di verifica è stato completato con successo AppFabric e ora AppClient è completamente verificato.
  - `rejected`- Il processo di verifica per AppClient è stato rifiutato da AppFabric. AppClient Non può essere utilizzato da altri utenti finché il processo di verifica non viene riavviato e completato con successo.

```
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 l'operazione riesce, il servizio restituisce una risposta HTTP 200.

```
{
    "appClientConfigSummary": {
        "appClientArn": "arn:aws:appfabric:<region>:<account>:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "verificationStatus": "pending_verification"
    }
```

```
}
```

Fase 2: Autentica e autorizza la tua applicazione

Consenti alla tua applicazione di integrare in modo sicuro gli AppFabric approfondimenti stabilendo un flusso di autorizzazione OAuth 2.0. Innanzitutto, è necessario creare un codice di autorizzazione che verifichi l'identità dell'applicazione. Per ulteriori informazioni, consulta Autorizza. Quindi scambierai questo codice di autorizzazione con un token di accesso, che concede all'applicazione le autorizzazioni per recuperare e visualizzare AppFabric informazioni all'interno dell'applicazione. Per ulteriori informazioni, consulta Token.

Per ulteriori informazioni sulla concessione dell'autorizzazione all'autorizzazione di un'applicazione, consulta. Consenti l'accesso per autorizzare le applicazioni

1. Per creare un codice di autorizzazione, utilizzate l'operazione AWS AppFabric `oauth2/authorize` API.

   Campi di richiesta

   - `app_client_id`(obbligatorio): l' AppClient ID per il file Account AWS creato nel passaggio 1. Crea un AppClient. Ad esempio, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
   - `redirect_uri`(obbligatorio): l'URI a cui reindirizzare gli utenti finali dopo l'autorizzazione utilizzata nel passaggio 1. Crea un AppClient. Ad esempio, `https://localhost:8080`.
   - `state`(obbligatorio): un valore univoco per mantenere lo stato tra la richiesta e il callback. Ad esempio, `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. Dopo l'autenticazione, verrai reindirizzato all'URI specificato con un codice di autorizzazione restituito come parametro di query. Ad esempio, `dovecode=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`.

   ```
   https://localhost:8080/?code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-
   sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-
   oampc&state=a8904edc-890c-1005-1996-29a757272a44
   ```

3. Scambia questo codice di autorizzazione con un token di accesso utilizzando l'operazione AppFabric `oauth2/token` API.

   Questo token viene utilizzato per le richieste API ed è inizialmente valido `starterUserEmails` fino alla AppClient verifica. Dopo AppClient la verifica, questo token può essere utilizzato per qualsiasi utente. È necessario utilizzare le credenziali della versione 4 della firma dell'account per eseguire questa operazione API. Per ulteriori informazioni sulla versione 4 della firma, consulta Signing AWS API request nella IAM User Guide.

   Campi di richiesta

   - `code`(obbligatorio) - Il codice di autorizzazione che hai ricevuto dopo l'autenticazione nell'ultimo passaggio. Ad esempio, `mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc`.
   - `app_client_id`(obbligatorio) - L' AppClient ID per il file Account AWS creato nel passaggio 1. Crea un AppClient. Ad esempio, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.
   - `grant_type`(obbligatorio): il valore deve essere`authorization_code`.
   - `redirect_uri`(obbligatorio): l'URI a cui reindirizzare gli utenti dopo l'autorizzazione utilizzata nel passaggio 1. Crea un AppClient. Deve essere lo stesso URI di reindirizzamento utilizzato per creare un codice di autorizzazione. Ad esempio, `https://localhost:8080`.

   Campi di risposta

   - `expires_in`- Quanto tempo prima della scadenza del token. Il tempo di scadenza predefinito è di 12 ore.
   - `refresh_token`- Il token di aggiornamento ricevuto dalla richiesta iniziale /token.
   - `token`- Il token ricevuto dalla richiesta iniziale /token.
   - `token_type`- Il valore sarà`Bearer`.
   - `appfabric_user_id`- L'id AppFabric utente. Viene restituito solo per le richieste che utilizzano il tipo di `authorization_code` concessione.

```
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 l'operazione riesce, il servizio restituisce una risposta HTTP 200.

```
{
    "expires_in": 43200,
    "refresh_token": "apkaeibaerjr2example",
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "<userId>"
}
```

Fase 3. Aggiungi l'URL del portale AppFabric utente alla tua applicazione

Gli utenti finali devono autorizzarsi AppFabric ad accedere ai dati delle loro applicazioni che vengono utilizzati per generare approfondimenti. AppFabric elimina la complessità per gli sviluppatori di app di gestire questo processo creando un portale utente dedicato (una schermata pop-up) per consentire agli utenti finali di autorizzare le proprie app. Quando gli utenti saranno pronti a dare AppFabric impulso alla produttività, verranno indirizzati al portale utenti che consente loro di connettersi e gestire le applicazioni utilizzate per generare approfondimenti e azioni tra app. Una volta effettuato l'accesso, gli utenti possono connettere le applicazioni a AppFabric per aumentare la produttività e poi tornare all'applicazione per esplorare le informazioni e le azioni da intraprendere. Per integrare l'applicazione con AppFabric una maggiore produttività, è necessario aggiungere un AppFabric URL specifico all'applicazione. Questo passaggio è fondamentale per consentire agli utenti di accedere al portale AppFabric utenti direttamente dall'applicazione.

1. Accedi alle impostazioni dell'applicazione e individua la sezione per aggiungere il reindirizzamento URLs.
2. Dopo aver trovato l'area appropriata, aggiungi il seguente AppFabric URL come URL di reindirizzamento all'applicazione:

```
https://userportal.appfabric.<region>.amazonaws.com/eup_login
```

Dopo aver aggiunto l'URL, l'applicazione verrà configurata per indirizzare gli utenti al portale AppFabric utenti. Qui, gli utenti possono accedere, connettersi e gestire le applicazioni utilizzate AppFabric per generare informazioni sulla produttività.

Fase 4. Utilizzalo AppFabric per far emergere informazioni e azioni tra app

Dopo che gli utenti hanno collegato le loro applicazioni, puoi utilizzare le informazioni acquisite dagli utenti per migliorarne la produttività riducendo il cambio di app e contesto. AppFabric genera informazioni dettagliate per un utente solo in base a ciò a cui l'utente è autorizzato a accedere. AppFabric archivia i dati dell'utente in un Account AWS file di proprietà di AppFabric. Per informazioni su come vengono AppFabric utilizzati i tuoi dati, consultaElaborazione dei dati in AppFabric.

Puoi utilizzare i seguenti strumenti basati sull'intelligenza artificiale APIs per generare e far emergere informazioni e azioni a livello di utente all'interno delle tue app:

- `ListActionableInsights`— Per ulteriori informazioni, consulta la sezione Actionable Insights di seguito.
- `ListMeetingInsights`— Per ulteriori informazioni, consulta la sezione Preparazione delle riunioni più avanti in questa guida.

Informazioni utilizzabili () **`ListActionableInsights`**

L'`ListActionableInsights`API aiuta gli utenti a gestire al meglio la loro giornata facendo emergere informazioni fruibili basate sulle attività delle loro applicazioni, tra cui e-mail, calendario, messaggi, attività e altro ancora. Gli approfondimenti restituiti mostreranno anche collegamenti incorporati agli artefatti utilizzati per generare le informazioni, aiutando gli utenti a visualizzare rapidamente quali dati sono stati utilizzati per generare le informazioni. Inoltre, l'API può restituire le azioni suggerite in base alle informazioni e consentire agli utenti di eseguire azioni tra app dall'interno dell'applicazione. In particolare, l'API si integra con piattaforme come Asana, Google Workspace, Microsoft 365e Smartsheet per consentire agli utenti di inviare e-mail, creare eventi di calendario e creare attività. I modelli di linguaggio di grandi dimensioni (LLMs) possono precompilare i dettagli relativi a un'azione consigliata (come il corpo dell'e-mail o il nome dell'attività), che gli utenti possono personalizzare prima dell'esecuzione, semplificando il processo decisionale e migliorando la produttività. Analogamente all'esperienza degli utenti finali per l'autorizzazione delle applicazioni,

AppFabric utilizza lo stesso portale dedicato per consentire agli utenti di visualizzare, modificare ed eseguire azioni tra app. Per eseguire azioni, è AppFabric necessario ISVs reindirizzare gli utenti a un portale AppFabric utenti in cui possono visualizzare i dettagli delle azioni ed eseguirle. Ogni azione generata da AppFabric ha un URL univoco. Questo URL è disponibile nella risposta della risposta dell'`ListActionableInsights`API.

Di seguito è riportato un riepilogo delle azioni supportate tra app e in quali app:

- Invia e-mail (Google Workspace, Microsoft 365)
- Crea un evento del calendario (Google Workspace, Microsoft 365)
- Crea attività (Asana, Smartsheet)

Campi di richiesta

- `nextToken`(opzionale) - Il token di impaginazione per recuperare il prossimo set di approfondimenti.
- `includeActionExecutionStatus`- Un filtro che accetta l'elenco degli stati di esecuzione delle azioni. Le azioni vengono filtrate in base ai valori di stato trasmessi. Valori possibili: `NOT_EXECUTED` | `EXECUTED`

Intestazione della richiesta

- L'intestazione di autorizzazione deve essere passata con il `Bearer Token` valore.

Campi di risposta

- `insightId`- L'ID univoco per l'analisi generata.
- `insightContent`- Ciò restituisce un riepilogo dell'analisi e dei collegamenti incorporati agli artefatti utilizzati per generare l'analisi. Nota: si tratterebbe di un contenuto HTML contenente link incorporati (<a>tag).
- `insightTitle`- Il titolo dell'intuizione generata.
- `createdAt`- Quando è stata generata l'intuizione.
- `actions`- Un elenco di azioni consigliate per l'analisi generata. Oggetto d'azione:
  - `actionId`- L'id univoco per l'azione generata.
  - `actionIconUrl`- L'URL dell'icona dell'app in cui si suggerisce di eseguire l'azione.

  - `actionTitle`- Il titolo dell'azione generata.
  - `actionUrl`- L'URL univoco per l'utente finale per visualizzare ed eseguire l'azione nel AppFabric portale utenti. Nota: per l'esecuzione di azioni, le app ISV reindirizzeranno gli utenti al portale AppFabric utenti (schermata pop-up) utilizzando questo URL.
  - `actionExecutionStatus`- Un enum che indica lo stato dell'azione. I valori possibili sono: | `EXECUTED` `NOT_EXECUTED`
- `nextToken`(opzionale) - Il token di impaginazione per recuperare il prossimo set di approfondimenti. È un campo opzionale che, se restituito nullo, significa che non ci sono più approfondimenti da caricare.

Per ulteriori informazioni, consulta ActionableInsights.

```
curl -v --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/actionableInsights" \
  --header "Authorization: Bearer <token>"
```

Se l'operazione riesce, il servizio restituisce una risposta 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
}
```

Preparazione della riunione () **`ListMeetingInsights`**

L'`ListMeetingInsights`API aiuta gli utenti a prepararsi al meglio per le riunioni imminenti riassumendo lo scopo della riunione e facendo emergere elementi pertinenti trasversali alle app come e-mail, messaggi e altro. Gli utenti possono prepararsi rapidamente per le riunioni ora e non perdere tempo a passare da un'app all'altra per trovare contenuti.

Campi di richiesta

- `nextToken`(opzionale) - Il token di impaginazione per recuperare il prossimo set di approfondimenti.

Intestazione della richiesta

- L'intestazione di autorizzazione deve essere passata con il `Bearer Token` valore.

Campi di risposta

- `insightId`- L'ID univoco per l'analisi generata.
- `insightContent`- La descrizione dell'analisi che evidenzia i dettagli in formato stringa. Ad esempio, perché questa intuizione è importante.
- `insightTitle`- Il titolo dell'intuizione generata.
- `createdAt`- Quando è stata generata l'intuizione.
- `calendarEvent`- L'evento o la riunione importante del calendario su cui l'utente dovrebbe concentrarsi. Oggetto Calendar Event:
  - `startTime`- L'ora di inizio dell'evento.
  - `endTime`- L'ora di fine dell'evento.
  - `eventUrl`- L'URL dell'evento del calendario sull'app ISV.
- `resources`- L'elenco contenente le altre risorse relative alla generazione dell'analisi. Oggetto risorsa:
  - `appName`- Il nome dell'app a cui appartiene la risorsa.
  - `resourceTitle`- Il titolo della risorsa.
  - `resourceType`- Il tipo di risorsa. I valori possibili sono: `EMAIL` | `EVENT` | `MESSAGE` | `TASK`
  - `resourceUrl`- L'URL della risorsa nell'app.
  - `appIconUrl`- L'URL dell'immagine dell'app a cui appartiene la risorsa.
- `nextToken`(opzionale) - Il token di impaginazione per recuperare il prossimo set di approfondimenti. È un campo opzionale che, se restituito nullo, significa che non ci sono più approfondimenti da caricare.

Per ulteriori informazioni, consulta MeetingInsights.

```
curl --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/meetingContexts" \
  --header "Authorization: Bearer <token>"
```

Se l'operazione riesce, il servizio restituisce una risposta 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
}
```

Fornisci feedback per le tue intuizioni o azioni

Utilizza il funzionamento dell' AppFabric `PutFeedback`API per fornire feedback sulle informazioni e sulle azioni generate. Puoi incorporare questa funzionalità nelle tue app per fornire un modo per inviare una valutazione di feedback (da 1 a 5, dove maggiore è la valutazione, migliore è) per un determinato InsightId o ActionId.

Campi di richiesta

- `id`- L'identificatore dell'oggetto per il quale viene inviato il feedback. Può essere il InsightId o il ActionId.
- `feedbackFor`- Il tipo di risorsa per cui viene inviato il feedback. Valori possibili: `ACTIONABLE_INSIGHT` | `MEETING_INSIGHT` | `ACTION`
- `feedbackRating`- Valutazione del feedback da `1` a`5`. Un punteggio più alto è, meglio è.

Campi di risposta

- Non ci sono campi di risposta.

Per ulteriori informazioni, consulta 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 l'operazione riesce, il servizio invia una risposta HTTP 201 con un corpo HTTP vuoto.

Fase 5. Richiedi AppFabric di verificare la tua candidatura

A questo punto, hai aggiornato l'interfaccia utente dell'applicazione per incorporare informazioni e azioni AppFabric tra app e hai ricevuto informazioni dettagliate per un singolo utente. Dopo esserti soddisfatto dei test e aver voluto estendere la tua esperienza AppFabric arricchita ad altri utenti, puoi inviare la tua candidatura AppFabric per la revisione e la verifica. AppFabric verificherà le informazioni sulle applicazioni prima di consentirne l'adozione su larga scala per proteggere gli sviluppatori di app, gli utenti finali e i relativi dati, aprendo la strada a un'espansione dell'adozione da parte degli utenti in modo responsabile.

Avvia il processo di verifica

Inizia il processo di verifica inviando un'email a appfabric-appverification@amazon.com e richiedendo che la tua app venga verificata.

Includi i seguenti dettagli nella tua email:

- Il tuo Account AWS ID
- Il nome dell'applicazione per cui richiedi la verifica
- Il tuo AppClient ID
- Le tue informazioni di contatto

Inoltre, fornisci le seguenti informazioni, se disponibili, per aiutarci a valutare la priorità e l'impatto:

- Numero stimato di utenti a cui intendi concedere l'accesso
- La data di lancio prevista

> **Note**
>
> Se hai un Account AWS manager o un responsabile dello sviluppo dei AWS partner, copiali nella tua email. L'inclusione di questi contatti può aiutare ad accelerare il processo di verifica.

Criteri di verifica

Prima di iniziare il processo di verifica, devi soddisfare i seguenti criteri:

- È necessario utilizzare un valore valido Account AWS per AppFabric la produttività

Inoltre, soddisfi almeno uno di questi criteri:

- La tua organizzazione è un AWS partner AWS Partner Network con almeno un livello «AWS Select». Per ulteriori informazioni, consulta AWS Partner Services Tiers.
- La tua organizzazione avrebbe dovuto spendere almeno 10.000 dollari in AppFabric servizi negli ultimi tre anni.
- La tua candidatura deve essere elencata nel Marketplace AWS. Per ulteriori informazioni, consulta il AWS Marketplace.

Attendi l'aggiornamento dello stato della verifica

Dopo aver esaminato la tua richiesta, risponderemo via e-mail e lo stato della tua richiesta AppClient cambierà da `pending_verification` a `verified`. Se la tua richiesta viene rifiutata, dovrai riavviare la procedura di verifica.

Gestisci AppFabric per la produttività AppClients

> La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

È possibile gestire la produttività AppFabric per AppClients garantire il funzionamento e la manutenzione senza intoppi dei processi di autenticazione e autorizzazione.

Ottieni i dettagli di un AppClient

Utilizza il funzionamento dell' AppFabric `GetAppClient`API per visualizzare i dettagli del tuo AppClient, incluso il controllo dello AppClient stato. Per ulteriori informazioni, consulta GetAppClient.

Per ottenere i dettagli di un AppClient, devi disporre almeno delle autorizzazioni della policy `"appfabric:GetAppClient"` IAM. Per ulteriori informazioni, consulta Consenti l'accesso per ottenere i dettagli di AppClients.

Campi di richiesta

- `appClientId`- L' AppClient ID.

Campi di risposta

- `appName`- Il nome dell'applicazione che verrà visualizzato agli utenti nella pagina di consenso del portale AppFabric utenti.
- `customerManagedKeyIdentifier`(opzionale) - L'ARN della chiave gestita dal cliente (generata da KMS) da utilizzare per crittografare i dati. Se non specificato, verrà utilizzata la chiave AWS AppFabric gestita.
- `description`- Una descrizione dell'applicazione.
- `redirectUrls`- L'URI a cui reindirizzare gli utenti finali dopo l'autorizzazione. È possibile aggiungere fino a 5 URL di reindirizzamento. Ad esempio, `https://localhost:8080`.
- `starterUserEmails`- Un indirizzo email utente a cui sarà consentito l'accesso per ricevere gli approfondimenti fino alla verifica dell'applicazione. È consentito un solo indirizzo e-mail. Ad esempio, `anyuser@example.com`.
- `verificationStatus`- Lo stato AppClient della verifica.
  - `pending_verification`- La verifica di AppClient è ancora in corso con AppFabric. Fino alla AppClient verifica, solo un utente (specificato in`starterUserEmails`) può utilizzare il AppClient.
  - `verified`- Il processo di verifica è stato completato con successo AppFabric e ora AppClient è completamente verificato.
  - `rejected`- Il processo di verifica per AppClient è stato rifiutato da AppFabric. AppClient Non può essere utilizzato da altri utenti finché il processo di verifica non viene riavviato e completato con successo.

```
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 l'operazione riesce, il servizio restituisce una risposta 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"
        }
    }
}
```

Elenco AppClients

Usa l'operazione AppFabric API per visualizzare un elenco dei tuoi AppClients. AppFabric ne consente solo uno AppClient per Account AWS. Questo è soggetto a modifiche in futuro. Per ulteriori informazioni, consulta ListAppClients.

Per poter elencare AppClients, è necessario disporre almeno delle autorizzazioni relative alla policy `"appfabric:ListAppClients"` IAM. Per ulteriori informazioni, consulta Consenti l'accesso all'elenco AppClients.

Campi di richiesta

- Non ci sono campi obbligatori.

Campi di risposta

- `appClientARN`- L'Amazon Resource Name (ARN) che include l' AppClient ID. Ad esempio, l' AppClient ID è`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`.

- `verificationStatus`- Lo stato AppClient della verifica.
  - `pending_verification`- La verifica di AppClient è ancora in corso con AppFabric. Fino alla AppClient verifica, solo un utente (specificato in`starterUserEmails`) può utilizzare il AppClient.
  - `verified`- Il processo di verifica è stato completato con successo AppFabric e ora AppClient è completamente verificato.
  - `rejected`- Il processo di verifica per AppClient è stato rifiutato da AppFabric. AppClient Non può essere utilizzato da altri utenti finché il processo di verifica non viene riavviato e completato con successo.

```
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 l'operazione riesce, il servizio restituisce una risposta HTTP 200.

```
200 OK

{
    "appClientList": [
        {
            "appClientArn": "arn:aws:appfabric:<region>:111122223333:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "verificationStatus": "pending_verification"
        }
    ]
}
```

Aggiorna un AppClient

Utilizza l'operazione AppFabric `UpdateAppClient` API per aggiornare gli URL di reindirizzamento mappati al tuo. AppClient Se è necessario modificare altri parametri, ad esempio, o altro AppName starterUserEmails, è necessario eliminarli AppClient e crearne uno nuovo. Per ulteriori informazioni, consulta UpdateAppClient.

Per aggiornare un AppClient, è necessario disporre almeno delle autorizzazioni della policy `"appfabric:UpdateAppClient"` IAM. Per ulteriori informazioni, consulta Consenti l'accesso all'aggiornamento AppClients.

Campi di richiesta

- `appClientId`(obbligatorio): l' AppClient ID con cui stai aggiornando gli URL di reindirizzamento.
- `redirectUrls`(obbligatorio): l'elenco aggiornato dei redirectURL. Puoi aggiungere fino a 5 redirectURL.

Campi di risposta

- `appName`- Il nome dell'applicazione che verrà visualizzato agli utenti nella pagina di consenso del portale AppFabric utenti.
- `customerManagedKeyIdentifier`(opzionale) - L'ARN della chiave gestita dal cliente (generata da KMS) da utilizzare per crittografare i dati. Se non specificato, verrà utilizzata la chiave AWS AppFabric gestita.
- `description`- Una descrizione dell'applicazione.
- `redirectUrls`- L'URI a cui reindirizzare gli utenti finali dopo l'autorizzazione. Ad esempio, `https://localhost:8080`.
- `starterUserEmails`- Un indirizzo e-mail utente a cui sarà consentito l'accesso per ricevere gli approfondimenti fino alla verifica dell'applicazione. È consentito un solo indirizzo e-mail. Ad esempio, `anyuser@example.com`.
- `verificationStatus`- Lo stato AppClient della verifica.
  - `pending_verification`- La verifica di AppClient è ancora in corso con AppFabric. Fino alla AppClient verifica, solo un utente (specificato in`starterUserEmails`) può utilizzare il AppClient.
  - `verified`- Il processo di verifica è stato completato con successo AppFabric e ora AppClient è completamente verificato.
  - `rejected`- Il processo di verifica per AppClient è stato rifiutato da AppFabric. AppClient Non può essere utilizzato da altri utenti finché il processo di verifica non viene riavviato e completato con successo.

```
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 l'operazione riesce, il servizio restituisce una risposta 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"
        }
    }
}
```

Eliminare un AppClient

Usa l'operazione AppFabric `DeleteAppClient` API per eliminare quelli AppClients che non ti servono più. Per ulteriori informazioni, consulta DeleteAppClient.

Per eliminare un AppClient, devi disporre almeno delle autorizzazioni della policy `"appfabric:DeleteAppClient"` IAM. Per ulteriori informazioni, consulta Consenti l'accesso per l'eliminazione AppClients.

Campi di richiesta

- `appClientId`- L' AppClient ID.

Campi di risposta

- Non ci sono campi di risposta.

```
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 l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

Token di aggiornamento per gli utenti finali

I token AppClient acquisiti per gli utenti finali possono essere aggiornati alla scadenza. Questo può essere fatto utilizzando l'TokenAPI con grant_type. `refresh_token` L'oggetto `refresh_token` da utilizzare viene restituito come parte della risposta dell'API del token quando grant_type è. `authorization_code` Le scadenze predefinite sono 12 ore. Per chiamare l'API di aggiornamento, devi disporre dell'autorizzazione della `"appfabric:Token"` policy IAM. Per ulteriori informazioni, consultare Token e Consenti l'accesso all'aggiornamento AppClients.

Campi di richiesta

- `refresh_token`(obbligatorio): il token di aggiornamento ricevuto dalla `/token` richiesta iniziale.
- `app_client_id`(obbligatorio) - L'ID della AppClient risorsa creata per. Account AWS
- `grant_type`(obbligatorio) - Deve essere`refresh_token`.

Campi di risposta

- `expires_in`- Quanto tempo prima della scadenza del token. Il tempo di scadenza predefinito è di 12 ore.
- `refresh_token`- Il token di aggiornamento ricevuto dalla richiesta iniziale /token.

- `token`- Il token ricevuto dalla richiesta iniziale /token.
- `token_type`- Il valore saràBearer.
- `appfabric_user_id`- L'id AppFabric utente. Viene restituito solo per le richieste che utilizzano il tipo di `authorization_code` concessione.

```
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 l'operazione riesce, il servizio restituisce una risposta HTTP 200.

```
200 OK

{
    "expires_in": 43200,
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "${UserID}"
}
```

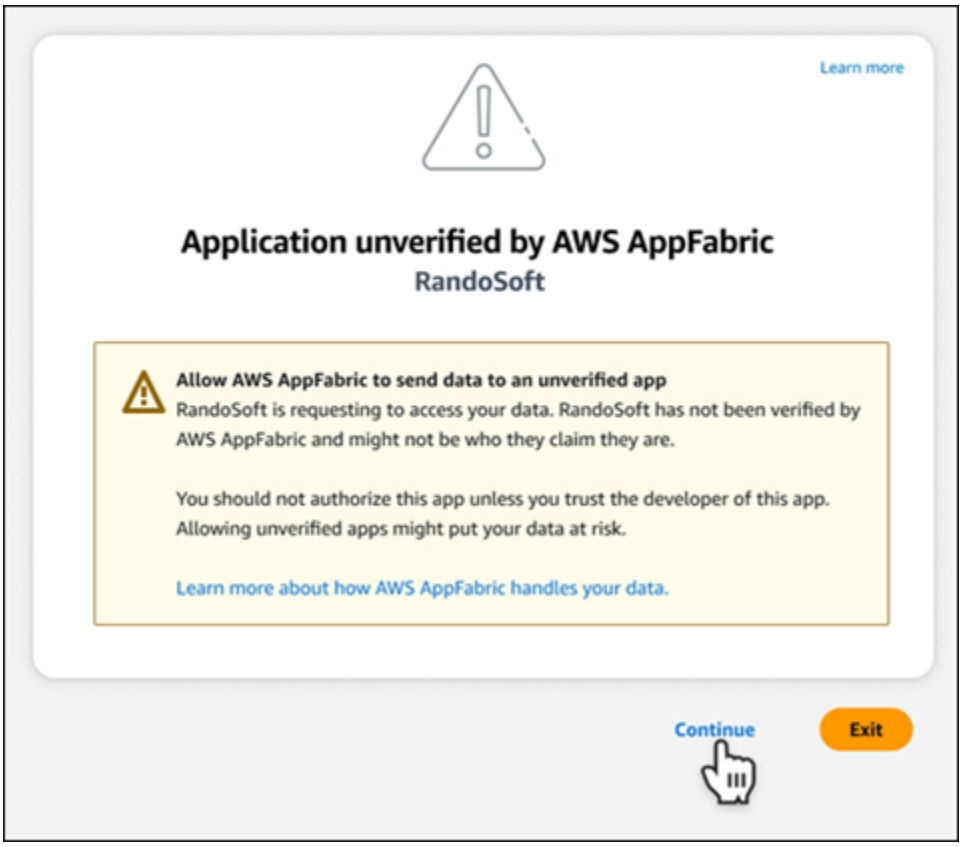
Risolvi i problemi per la AppClients produttività AppFabric

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Questa sezione descrive gli errori comuni e la risoluzione dei problemi relativi AppFabric alla produttività.

Applicazione non verificata

Gli sviluppatori di app che utilizzano AppFabric le app per la produttività per arricchire le proprie esperienze con le app passeranno attraverso un processo di verifica prima di lanciare le funzionalità agli utenti finali. Tutte le applicazioni iniziano come non verificate e passano a verificate solo quando il processo di verifica è completo. Ciò significa che il file che `starterUserEmails` hai usato durante la creazione AppClient vedrà questo messaggio.



Errori **`CreateAppClient`**

ServiceQuotaExceededException

Se ricevi la seguente eccezione durante la creazione di un AppClient, significa che hai superato il numero di eccezioni AppClients che puoi creare per Account AWS. Il limite è 1. Codice di stato 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
```

Errori **`GetAppClient`**

ResourceNotFoundException

Se ricevi la seguente eccezione quando ricevi i dettagli di un AppClient, assicurati di aver inserito l' AppClient identificatore corretto. Questo errore indica che l'oggetto specificato non AppClient è stato trovato.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you’ve entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Errori **`DeleteAppClient`**

ConflictException

Se si riceve la seguente eccezione quando si elimina un AppClient, è in corso un'altra richiesta di eliminazione. Attendi il completamento, quindi riprova. Codice di stato HTTP: 409

```
ConflictException
Another delete request is in progress. Wait until it completes then try again.
HTTP Status Code: 409
```

ResourceNotFoundException

Se ricevi la seguente eccezione quando elimini un AppClient, assicurati di aver inserito l'identificatore corretto AppClient . Questo errore indica che l'oggetto specificato non AppClient è stato trovato.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you’ve entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Errori **`UpdateAppClient`**

ResourceNotFoundException

Se ricevi la seguente eccezione durante l'aggiornamento di un AppClient, assicurati di aver inserito l' AppClient identificatore corretto. Questo errore indica che l'oggetto specificato non AppClient è stato trovato.

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

Errori **`Authorize`**

ValidationException

Potresti ricevere la seguente eccezione se uno qualsiasi dei parametri dell'API non soddisfa i vincoli definiti nelle specifiche dell'API.

```
ValidationException
HTTP Status Code: 400
```

Motivo 1: quando l' AppClient ID non è specificato

`app_client_id`Manca nei parametri della richiesta. Crea il AppClient file se non è ancora stato creato o usa quello esistente `app_client_id` e riprova. Per trovare l' AppClient ID, usa l'operazione ListAppClientAPI.

Motivo 2: AppFabric When non ha accesso alla chiave gestita dal cliente

```
Message: AppFabric couldn't access the customer managed key configured for AppClient.
```

AppFabric al momento non è in grado di accedere alle chiavi gestite dal cliente, probabilmente a causa delle recenti modifiche alle sue autorizzazioni. Verifica che la chiave specificata esista e assicurati che AppFabric siano concesse le autorizzazioni di accesso appropriate.

Motivo 3: l'URL di reindirizzamento specificato non è valido

```
Message: Redirect url invalid
```

Assicurati che l'URL di reindirizzamento nella richiesta sia corretto. Deve corrispondere a uno dei reindirizzamenti URLs specificati al momento della creazione o dell'aggiornamento di. AppClient Per visualizzare l'elenco dei reindirizzamenti consentiti URLs, utilizza l'operazione GetAppClientAPI.

Errori **Token**

TokenException

Potresti ricevere la seguente eccezione per alcuni motivi.

```
TokenException
HTTP Status Code: 400
```

Motivo 1: quando viene specificata un'e-mail non valida

```
Message: Invalid Email used
```

Assicurati che l'indirizzo email che stai utilizzando corrisponda a quello elencato per l'`starterUserEmails`attributo quando hai creato il AppClient. Se le email non corrispondono, passa all'indirizzo e-mail corrispondente e riprova. Per visualizzare l'e-mail utilizzata, utilizza l'operazione GetAppClientAPI.

Motivo 2: per grant_type come refresh_token quando il token non è specificato.

```
Message: refresh_token must be non-null for Refresh Token Grant-type
```

Il token di aggiornamento specificato nella richiesta è nullo o vuoto. Specificare un valore attivo `refresh_token` ricevuto nella risposta alla chiamata dell'API Token.

ThrottlingException

Potresti ricevere la seguente eccezione se l'API viene chiamata a una frequenza superiore alla quota consentita.

```
ThrottlingException
HTTP Status Code: 429
```

ListActionableInsightsListMeetingInsights, ed **PutFeedback** errori

ValidationException

Potresti ricevere la seguente eccezione se uno qualsiasi dei parametri dell'API non soddisfa il vincolo definito nelle specifiche dell'API.

```
ValidationException
HTTP Status Code: 400
```

ThrottlingException

Potresti ricevere la seguente eccezione se l'API viene chiamata a una frequenza superiore alla quota consentita.

```
ThrottlingException
HTTP Status Code: 429
```

Guida introduttiva alla AppFabric produttività (anteprima) per gli utenti finali

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Questa sezione è destinata agli utenti finali di applicazioni SaaS che desiderano abilitare la produttività (anteprima) AWS AppFabric per migliorare la gestione delle attività e l'efficienza del flusso di lavoro. Segui questi passaggi per connettere le tue applicazioni e autorizzarle AppFabric a far emergere informazioni trasversali tra app e aiutarti a completare azioni (come inviare un'e-mail o pianificare una riunione) dalle tue applicazioni preferite. Puoi connettere applicazioni come Asana, Atlassian Jira Suite, Google Workspace, Microsoft 365, Miro, Slack, Smartsheete molto altro ancora. Dopo aver autorizzato l'accesso AppFabric ai tuoi contenuti, AppFabric offre informazioni e azioni tra app direttamente all'interno delle tue app preferite, aiutandoti a lavorare in modo più efficiente e a rimanere all'interno dei flussi di lavoro correnti.

AppFabric per la produttività utilizza l'intelligenza artificiale generativa basata su Amazon Bedrock. AppFabric genererà informazioni e azioni solo dopo aver ricevuto la tua autorizzazione esplicita. Autorizzi ogni singola applicazione a mantenere il pieno controllo del contenuto utilizzato. AppFabric non utilizzerà i tuoi dati per addestrare o migliorare i modelli linguistici di grandi dimensioni sottostanti utilizzati per generare approfondimenti. Per ulteriori informazioni, consulta Amazon Bedrock FAQs.

Argomenti

Prerequisiti

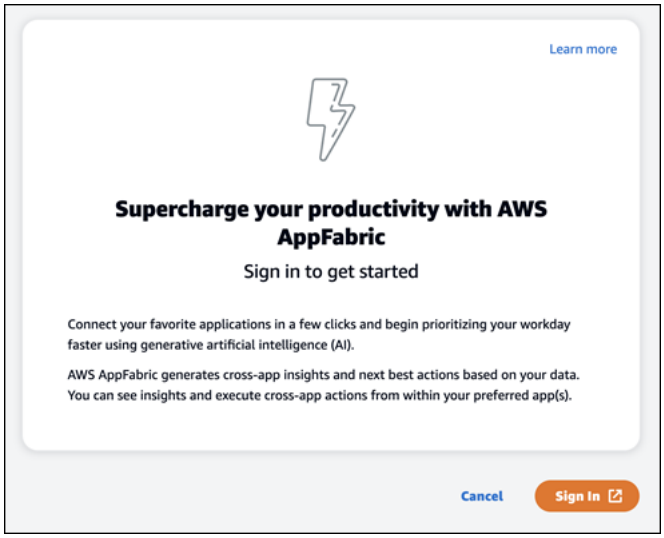
Prima di iniziare, assicurati di avere quanto segue:

- Credenziali di accesso AppFabric: per iniziare a utilizzarle AppFabric per la produttività, avrai bisogno di credenziali di accesso federate (nome utente e password) per uno dei seguenti provider: Asana, Google Workspace, Microsoft 365, oppure Slack. L'accesso a ci AppFabric aiuta a identificarti come utente in ogni applicazione che attivi AppFabric per la produttività. Dopo aver effettuato l'accesso, puoi connettere le tue applicazioni per iniziare a generare approfondimenti.
- Credenziali per connettere le tue applicazioni: le informazioni e le azioni tra app vengono generate solo in base alle applicazioni che autorizzi. Avrai bisogno delle credenziali di accesso (nome utente e password) per ciascuna delle applicazioni che desideri autorizzare. Le applicazioni supportate includono Asana, Atlassian Jira Suite, Google Workspace, Microsoft 365, Miro, Slacke Smartsheet.

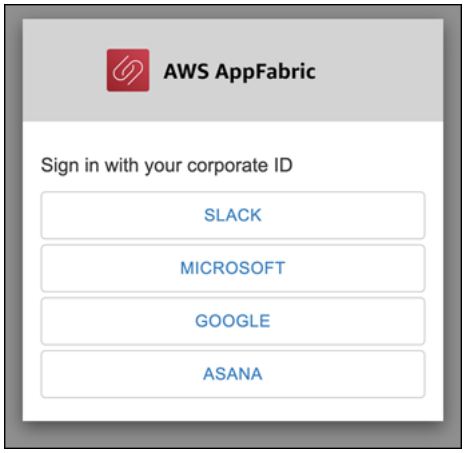
Fase 1: Accedi a AppFabric

Connect le applicazioni AppFabric per portare contenuti e approfondimenti direttamente all'interno delle applicazioni preferite.

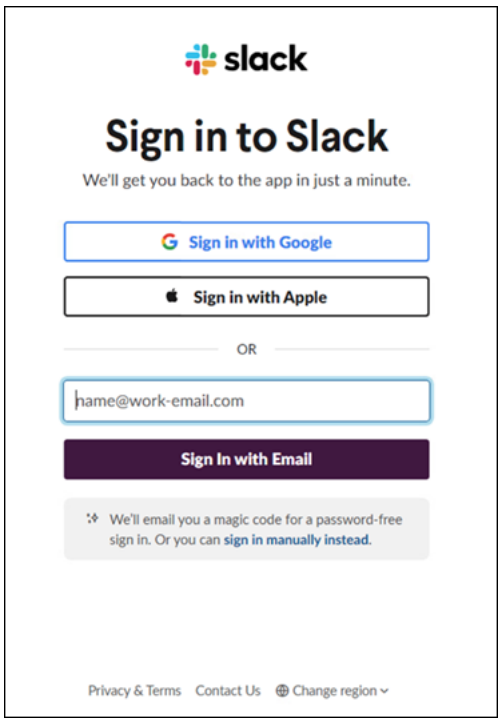
1. Ogni applicazione verrà utilizzata AppFabric per la produttività in modi diversi per offrirti esperienze di app più ricche. Per questo motivo, ogni applicazione avrà un punto di accesso diverso AppFabric per accedere alla home page dedicata alla produttività riportata di seguito. La home page fornisce un contesto relativo al processo da abilitare AppFabric e richiede innanzitutto di effettuare l'accesso. Ogni applicazione che desideri abilitare accederà AppFabric a questa schermata.

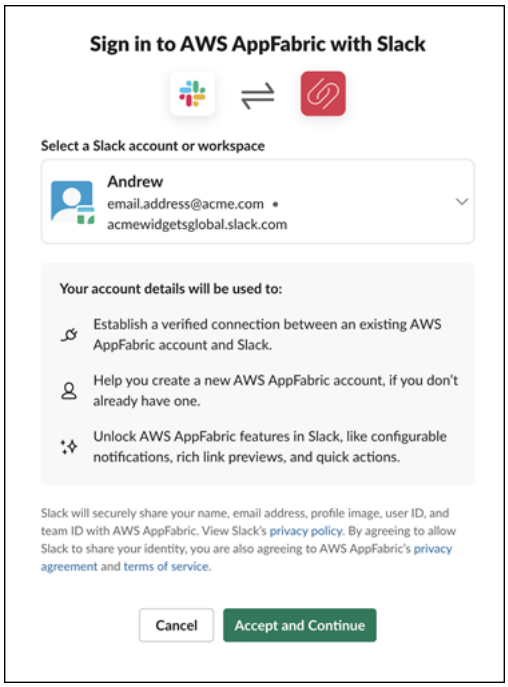


2. Accedi con le tue credenziali di uno di questi provider: Asana, Google Workspace, Microsoft 365, oppure Slack. Per un'esperienza ottimale, ti consigliamo di accedere utilizzando lo stesso provider per ogni applicazione AppFabric abilitata. Ad esempio, se scegli le credenziali di Google Workspace in App1, ti consigliamo di scegliere Google Workspace in App2, così come ogni altra volta che devi accedere nuovamente. Se accedi con un altro provider, dovrai riavviare il processo di connessione delle applicazioni.



3. Se richiesto, inserisci le tue credenziali di accesso e accetta l'accesso AppFabric da questo provider.

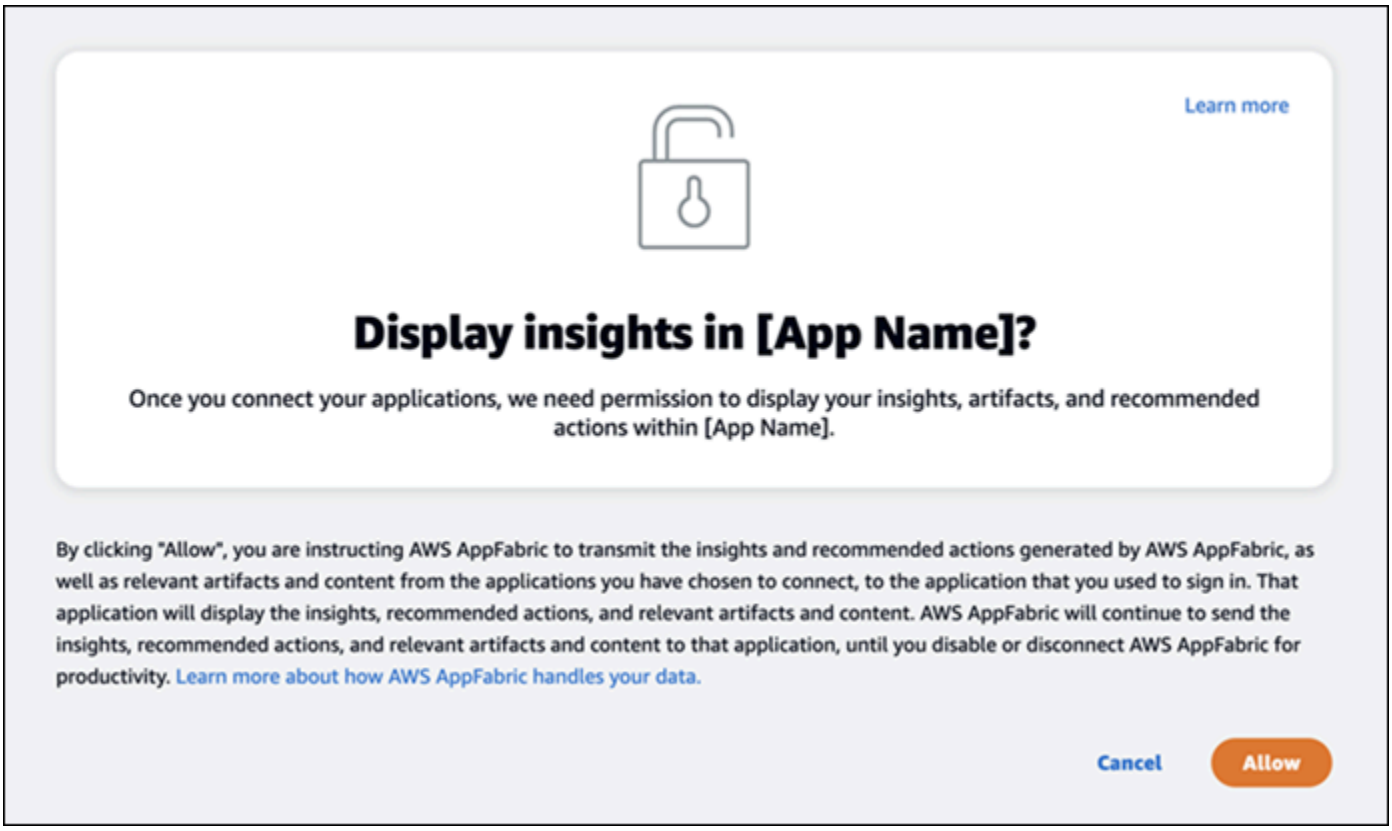




Fase 2: Fornisci il consenso affinché l'app mostri approfondimenti

Dopo l'accesso, AppFabric verrà visualizzata una pagina di consenso che ti chiederà se consenti di AppFabric visualizzare informazioni e azioni tra app all'interno dell'applicazione in cui stai abilitando AppFabric la produttività. Ad esempio, consentite di AppFabric prendere le vostre Google Workspace

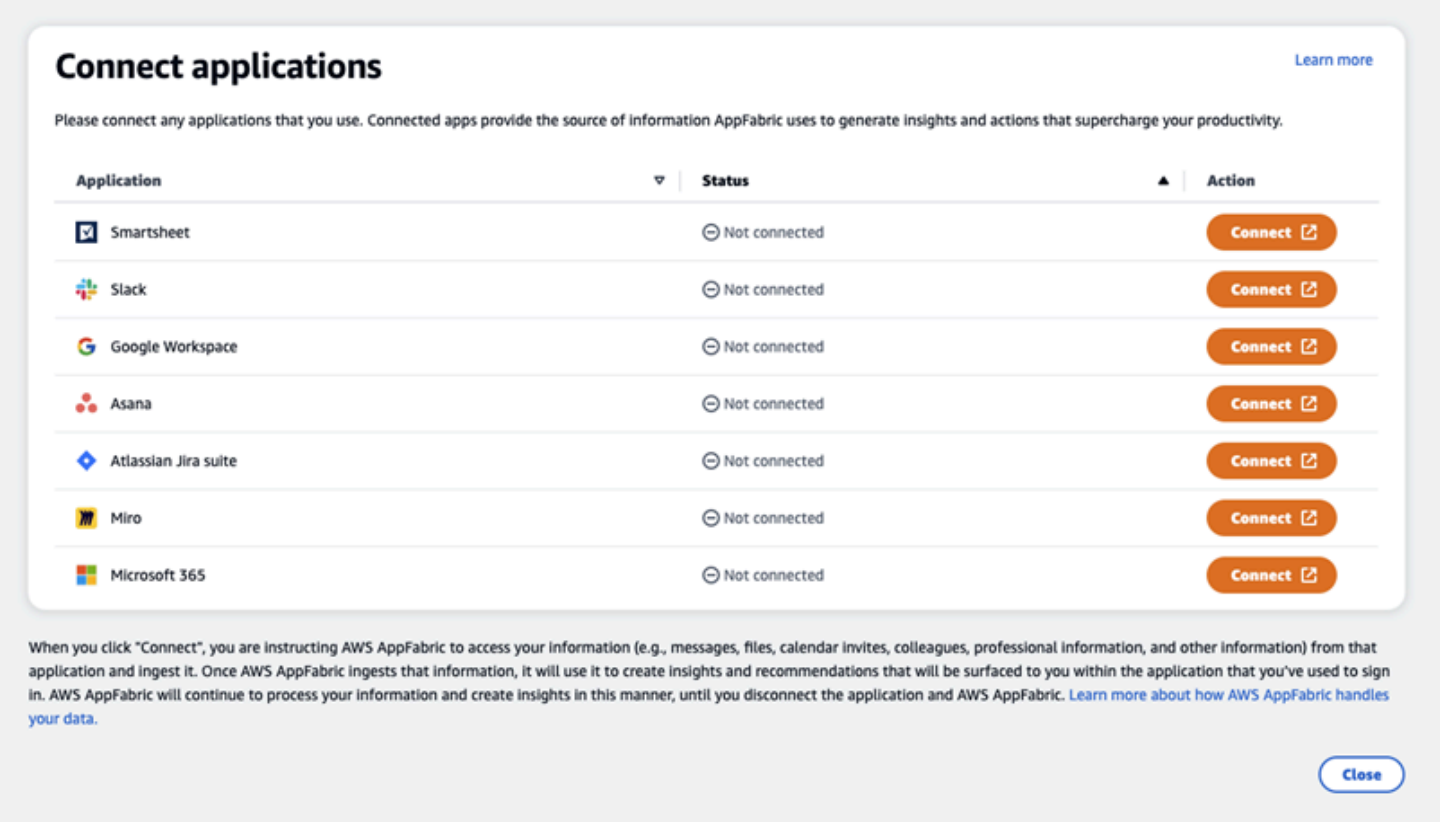
e-mail ed eventi del calendario e visualizzarli in Asana. Devi completare questa fase di consenso solo una volta per applicazione AppFabric in cui abiliti.



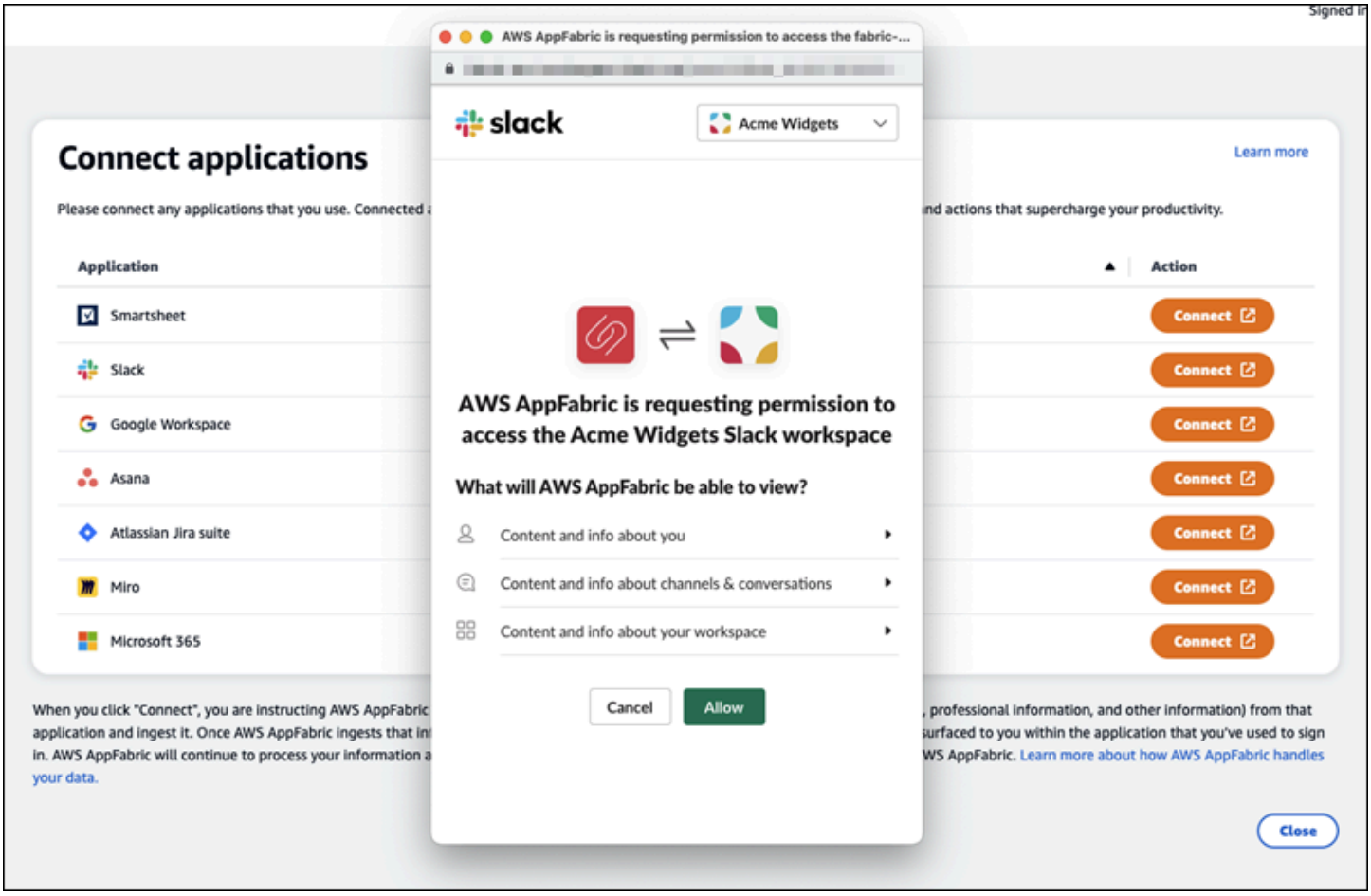
Fase 3. Connect le tue applicazioni per generare informazioni e azioni

Dopo aver completato la pagina di consenso, verrai indirizzato alla pagina Connect applications dove puoi connettere, disconnettere o ricollegare singole applicazioni che vengono utilizzate in ultima analisi per generare informazioni e azioni tra app. Nella maggior parte dei casi, dopo aver effettuato l'accesso e fornito il consenso, continuerai a utilizzare questa pagina per gestire le applicazioni connesse.

Per connettere un'applicazione, scegli il pulsante Connetti accanto a qualsiasi applicazione che usi.



Dovrai fornire le tue credenziali di accesso per l'applicazione e consentire l' AppFabricautorizzazione ad accedere ai tuoi dati per generare approfondimenti e completare azioni.

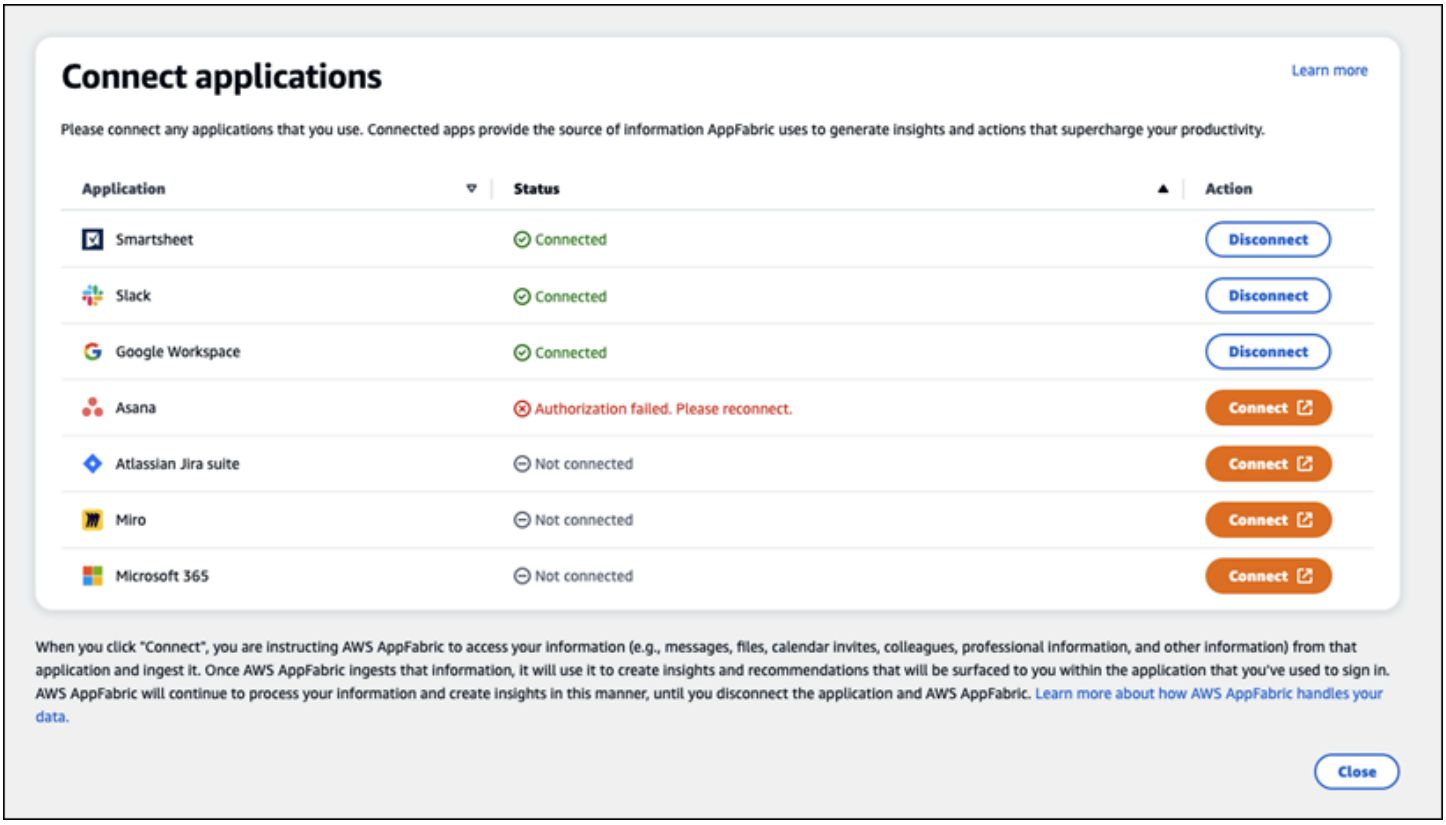


Dopo aver collegato correttamente un'applicazione, lo stato dell'applicazione cambierà da «Non connessa» a «Connessa». Promemoria: è necessario completare questa fase di autorizzazione per ogni applicazione che si desidera utilizzare per generare informazioni e azioni.

Dopo aver connesso un'applicazione, questa non è connessa per sempre. Dovrai riconnettere periodicamente le applicazioni. Lo facciamo per assicurarci di avere ancora la tua autorizzazione a generare approfondimenti.

I possibili stati dell'applicazione sono:

- Connesso: AppFabric è autorizzato e genera approfondimenti utilizzando i dati dell'utente provenienti da questa applicazione.
- Non connesso: AppFabric non genera approfondimenti utilizzando i dati di questa applicazione. Puoi connetterti per iniziare a generare approfondimenti.
- Autorizzazione fallita. Riconnettiti, per favore. - Potrebbe esserci un errore di autorizzazione con un'applicazione specifica. Se vedi questo errore, prova a ricollegare l'applicazione usando il pulsante Connect.



La configurazione è completa e puoi tornare alla tua applicazione. Potrebbero essere necessarie almeno alcune ore per iniziare a visualizzare informazioni dettagliate all'interno delle applicazioni.

Se necessario, puoi tornare a questa pagina per gestire le applicazioni connesse. Se scegli di disconnettere un'applicazione, AppFabric smetterà di utilizzare i dati di quell'applicazione o di raccogliere nuovi dati per generare nuove informazioni. I dati delle applicazioni disconnesse verranno automaticamente eliminati entro 7 giorni se si sceglie di non ricollegare l'applicazione in quel lasso di tempo.

Fase 4. Inizia a visualizzare informazioni dettagliate ed esegui azioni tra app nella tua applicazione

Dopo aver collegato le applicazioni AppFabric, avrai accesso a informazioni preziose e la possibilità di eseguire azioni tra app direttamente dalla tua applicazione preferita. Nota: questa funzionalità non è garantita in ogni app e dipende interamente dalle funzionalità AppFabric di produttività che lo sviluppatore dell'applicazione ha scelto di abilitare.

Informazioni su più app

AppFabric for productivity offre due tipi di approfondimenti:

- Informazioni fruibili: AppFabric analizza le informazioni provenienti da e-mail, eventi del calendario, attività e messaggi tra le app connesse e genera informazioni chiave a cui potrebbe essere importante dare priorità. Inoltre, AppFabric può generare azioni consigliate (come inviare e-mail, pianificare riunioni e creare attività) che è possibile modificare ed eseguire rimanendo nella propria applicazione preferita. Ad esempio, potresti ricevere un messaggio che ti dice che c'è un'escalation di clienti da affrontare e ti suggeriamo un'azione successiva per pianificare un incontro con il cliente.
- Informazioni sulla preparazione delle riunioni: questa funzione ti aiuta a prepararti al meglio per le riunioni imminenti. AppFabric analizzerà le riunioni imminenti e genererà un breve riepilogo dello scopo della riunione. Inoltre, mostrerà elementi pertinenti (come e-mail, messaggi e attività) dalle applicazioni connesse che saranno utili per prepararsi in modo efficiente alla riunione senza dover passare da un'app all'altra per trovare contenuti.

Azioni tra app

Per alcune informazioni, AppFabric può anche generare azioni consigliate come l'invio di un'e-mail, la pianificazione di una riunione o la creazione di un'attività. Durante la generazione di azioni, AppFabric può precompilare determinati campi in base al contenuto e al contesto delle applicazioni connesse. Ad esempio, AppFabric può generare una risposta e-mail suggerita o il nome dell'attività in base alle informazioni. Quando fai clic su un'azione suggerita, verrai indirizzato a un'interfaccia utente AppFabric proprietaria in cui puoi modificare il contenuto precompilato prima di eseguire l'azione. AppFabric non eseguirà azioni senza prima aver prima esaminato e inserito l'utente, poiché l'IA generativa e i modelli di linguaggio di grandi dimensioni (LLM) sottostanti possono avere allucinazioni di tanto in tanto.

> **Note**
>
> Hai la responsabilità di convalidare e confermare gli output LLM. AppFabric AppFabric non garantisce l'accuratezza o la qualità delle sue uscite LLM. Per ulteriori informazioni, consulta la Politica sull'IA AWS responsabile.

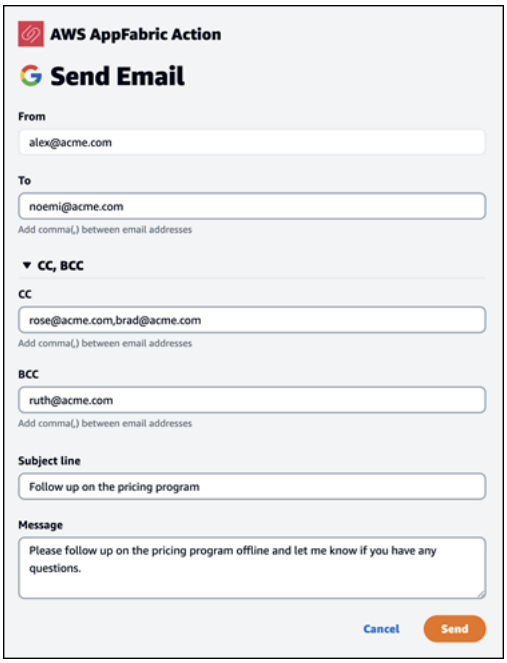
Crea email (Google Workspace, Microsoft 365)

AppFabric consente di modificare e inviare un'e-mail dall'applicazione preferita. Supportiamo i campi e-mail di base, tra cui From, To, Cc/Bcc, Email Subject Line e Email Body Message. AppFabric può

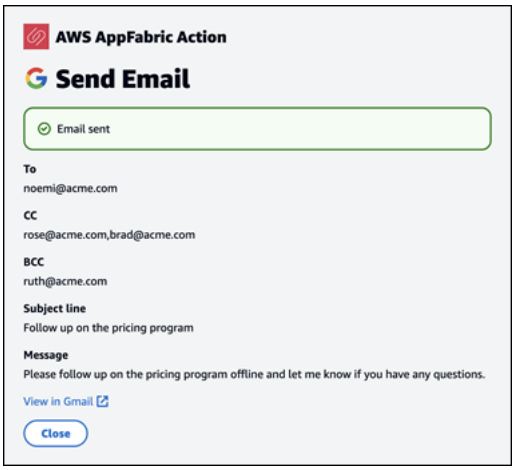
generare contenuti in questi campi per aiutarti a ridurre i tempi di completamento dell'attività. Dopo aver modificato l'e-mail, scegli Invia per inviare l'e-mail.

I seguenti campi sono obbligatori per inviare un'email:

- Almeno uno dei messaggi di posta elettronica dei destinatari (To, CC e BCC) è obbligatorio e deve essere un indirizzo e-mail valido.
- Riga dell'oggetto e campi del messaggio.



Dopo l'invio dell'email, vedrai una conferma che l'email è stata inviata. Inoltre, vedrai un link per visualizzare l'e-mail nell'applicazione designata. Puoi utilizzare questo link per accedere rapidamente all'applicazione e verificare che l'e-mail sia stata inviata.

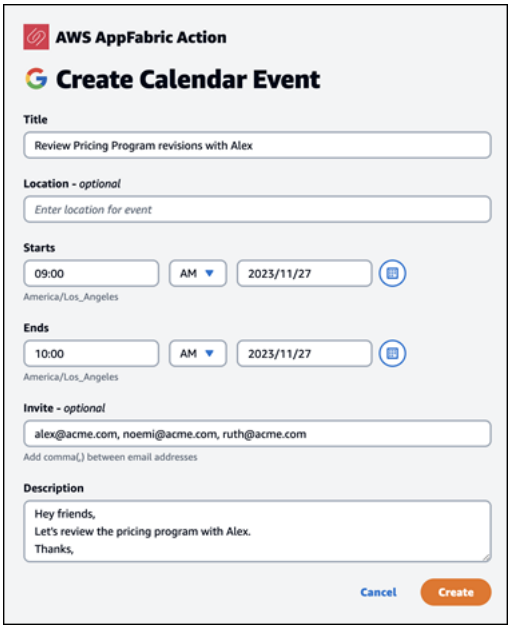


Crea eventi in calendario (Google Workspace, Microsoft 365)

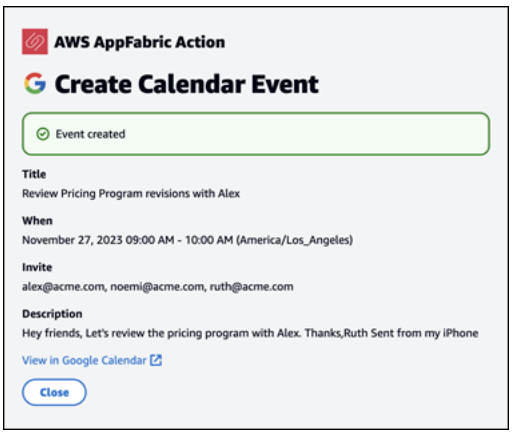
AppFabric consente di modificare e creare un evento del calendario dall'interno dell'applicazione preferita. Supportiamo i campi di base degli eventi del calendario, tra cui il titolo dell'evento, il luogo, l'ora e la data di inizio/fine, l'elenco degli invitati e i dettagli dell'evento. AppFabric può generare contenuti in questi campi per aiutarti a ridurre i tempi di completamento dell'attività. Dopo aver modificato l'evento del calendario, scegli Crea per creare l'evento.

I seguenti campi sono obbligatori per creare un evento del calendario:

- Campi Titolo, Inizio, Fine e Descrizione.
- L'ora e la data di inizio non devono essere precedenti all'ora e alla data di fine.
- Il campo di invito è facoltativo, ma richiede indirizzi e-mail validi, se forniti.



Dopo l'invio dell'evento del calendario, vedrai una conferma che l'evento è stato creato. Inoltre, vedrai un link per visualizzare l'evento nell'applicazione designata. È possibile utilizzare questo collegamento per accedere rapidamente all'applicazione e verificare che l'evento sia stato creato.

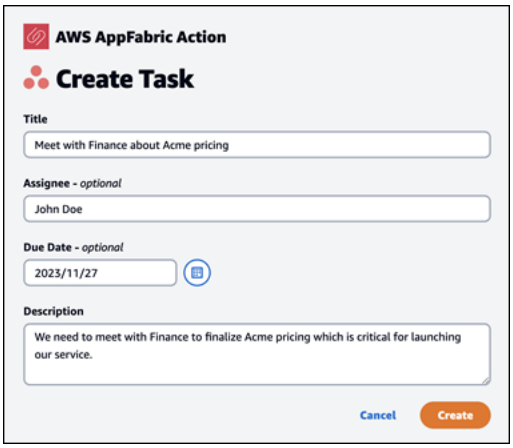


Crea attività (Asana)

AppFabric consente di modificare e creare un'attività in Asana dall'interno dell'applicazione preferita. Supportiamo campi di attività di base come Nome dell'attività, Proprietario dell'attività, Data di scadenza e Descrizione dell'attività. AppFabric può generare contenuti in questi campi per aiutarti a ridurre i tempi di creazione dell'attività. Dopo aver modificato l'attività, scegli Crea per creare l'attività. Le attività vengono create nell'apposito Asana spazio di lavoro o progetto o attività, come suggerito dal LLM.

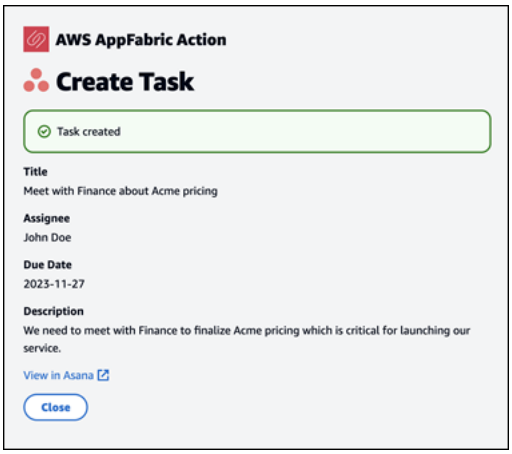
I seguenti campi sono obbligatori per creare un Asana attività:

- Campi del titolo e della descrizione.
- L'assegnatario deve avere un indirizzo e-mail valido se modificato.



Dopo aver creato l'attività, vedrai una conferma che l'attività è stata creata in Asana. Inoltre, vedrai un link per visualizzare l'attività in Asana. È possibile utilizzare questo collegamento per accedere

rapidamente all'applicazione e verificare che l'attività sia stata creata o spostarla nella posizione appropriata Asana spazio di lavoro o progetto o attività.

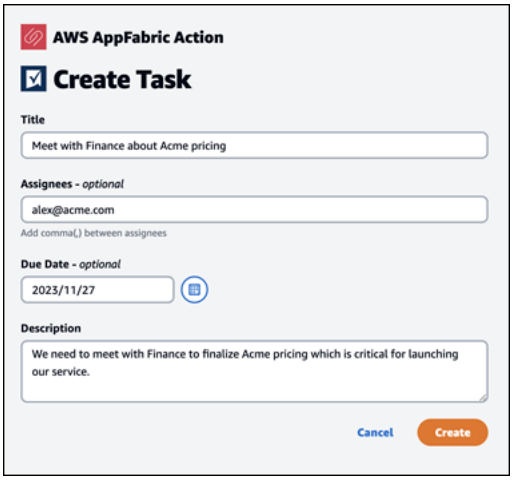


Crea attività (Smartsheet)

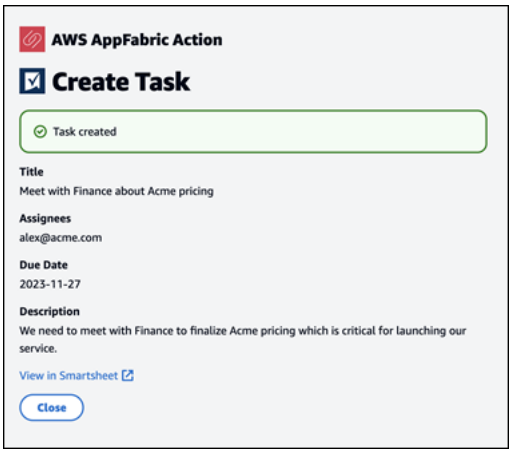
AppFabric consente di modificare e creare un'attività in Smartsheet dall'interno dell'applicazione preferita. Supportiamo campi di attività di base come Nome dell'attività, Proprietario dell'attività, Data di scadenza e Descrizione dell'attività. AppFabric può generare contenuti in questi campi per aiutarti a ridurre i tempi di creazione dell'attività. Dopo aver modificato l'attività, scegli Crea per creare l'attività. In Smartsheet attività, AppFabric ne creerà una nuova privata Smartsheet elenca e compila tutte le attività create. Questo viene fatto per aiutare a centralizzare le azioni AppFabric generate in un unico posto in modo strutturato.

I seguenti campi sono necessari per creare un Smartsheet attività:

- Campi del titolo e della descrizione.
- L'assegnatario deve avere un indirizzo e-mail valido, se fornito.



Dopo aver creato l'attività, vedrai una conferma che l'attività è stata creata in Smartsheet. Inoltre, vedrai un link per visualizzare l'attività in Smartsheet. È possibile utilizzare questo collegamento per accedere rapidamente all'applicazione e visualizzare l'attività nel file creato Smartsheet foglio. Tutte le future Smartsheet le attività verranno compilate in questo foglio. Se il foglio viene eliminato, AppFabric ne creerà uno nuovo.



Gestisci l'accesso alle AppFabric funzionalità di produttività (anteprima) per gli amministratori IT e di sicurezza

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Il portale AppFabric per gli utenti di for productivity è accessibile pubblicamente a tutti gli utenti di applicazioni SaaS che hanno integrato le funzionalità di AppFabric for productivity (anteprima). Se

sei un amministratore IT che desidera gestire l'accesso a queste funzionalità di intelligenza artificiale generativa all'interno della tua organizzazione, prendi in considerazione queste opzioni:

- Limita l'accesso all'Identity Provider (IdP): puoi bloccare l'accesso tramite il tuo Identity Provider per controllare l'accesso degli utenti alle funzionalità di intelligenza artificiale generativa.
- Disattiva OAuth per applicazioni specifiche: implementa le restrizioni a valle disabilitando. OAuth Questa azione impedisce agli utenti di connettere le applicazioni che richiedono OAuth l'autenticazione all'area di lavoro dell'azienda.

Risolvi gli errori degli utenti finali in AppFabric termini di produttività

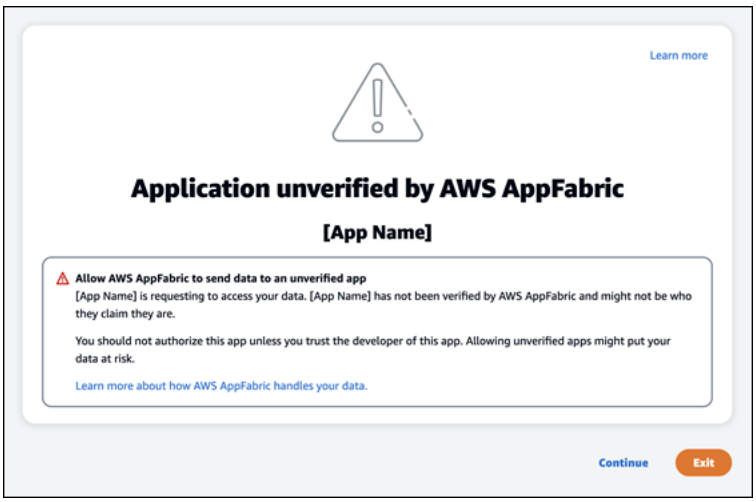
La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Questa sezione descrive gli errori comuni e la risoluzione dei problemi relativi AppFabric alla produttività.

Applicazione non verificata

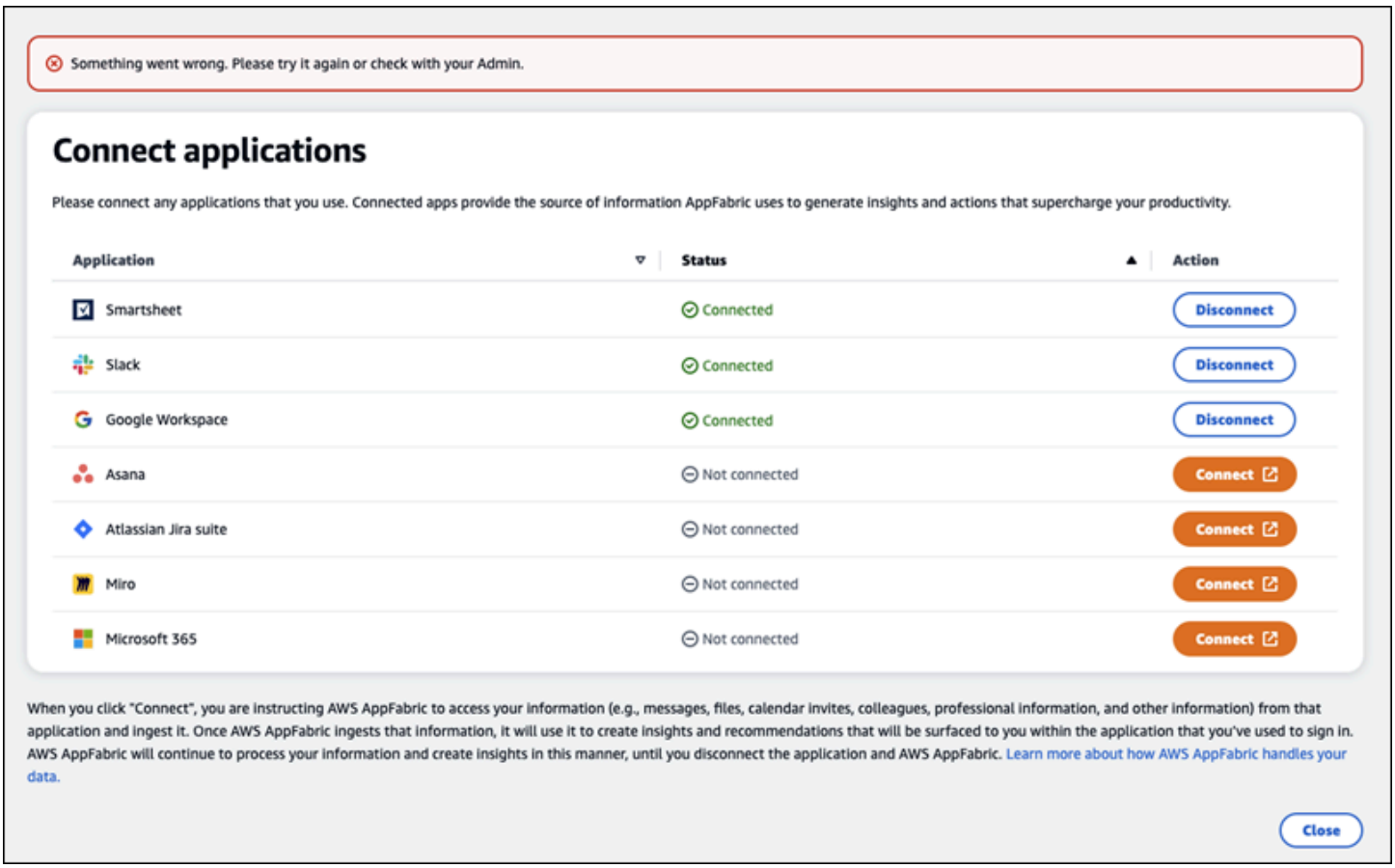
Le applicazioni che utilizzano la produttività AppFabric per arricchire l'esperienza delle app verranno sottoposte a un processo di verifica prima di rilasciare le funzionalità agli utenti finali. Se compare un banner «non verificato» quando provi ad accedere AppFabric, significa che l'applicazione non è stata sottoposta AppFabric al processo di verifica che confermi l'identità dello sviluppatore dell'app e l'accuratezza delle informazioni di registrazione dell'applicazione. Tutte le applicazioni iniziano come non verificate e passano a verificate solo quando il processo di verifica è completo.

Fai attenzione quando usi un'applicazione non verificata. Se non sei sicuro degli sviluppatori dell'app, puoi attendere che l'applicazione raggiunga lo stato di verifica prima di procedere.



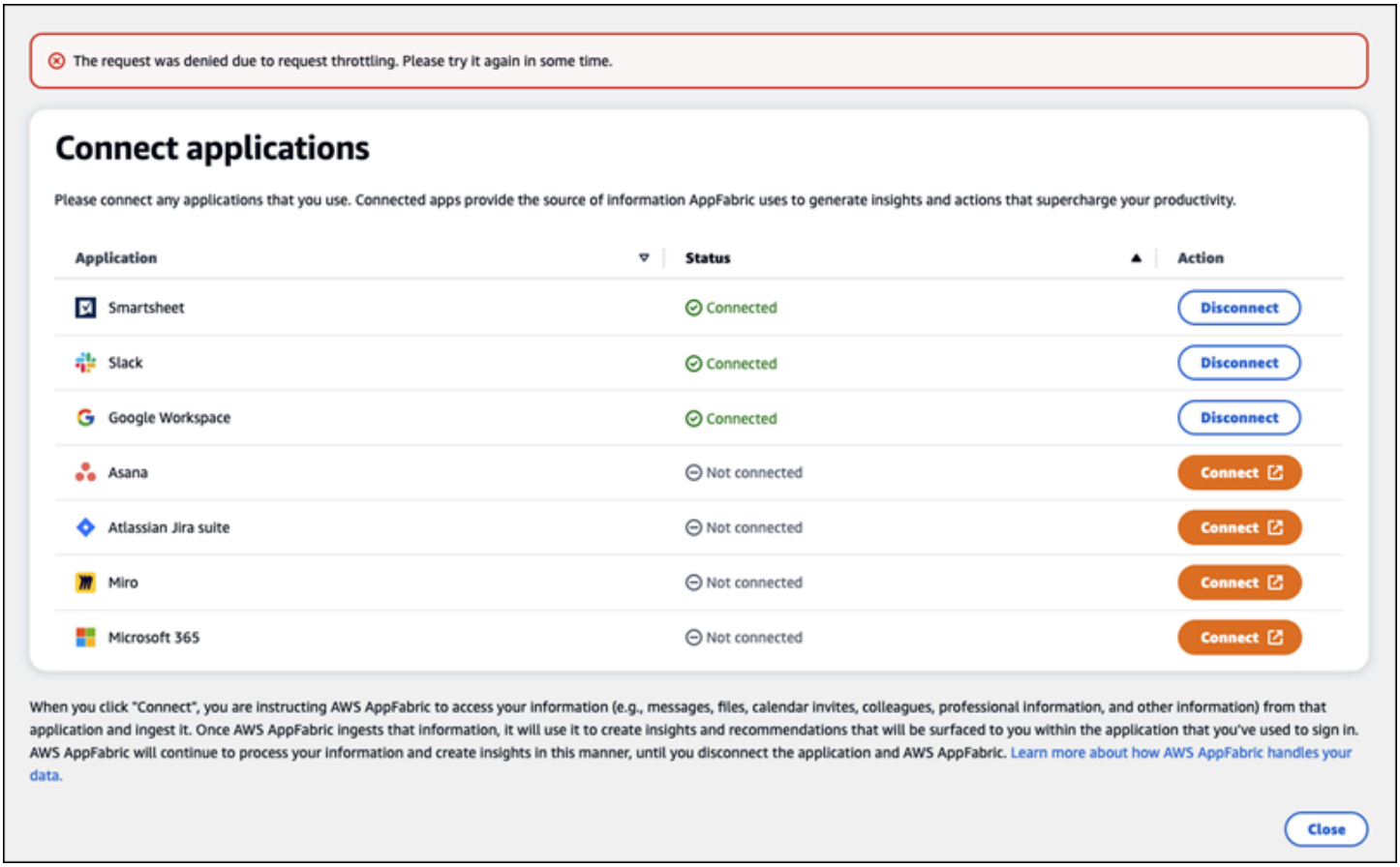
Qualcosa è andato storto. Riprova o verifica con il tuo amministratore (`InternalServerException`)

Potresti ricevere questo messaggio quando il portale AppFabric utente non riesce a elencare le applicazioni o disconnette un'applicazione a causa di un errore, un'eccezione o un errore sconosciuto. Riprova più tardi.



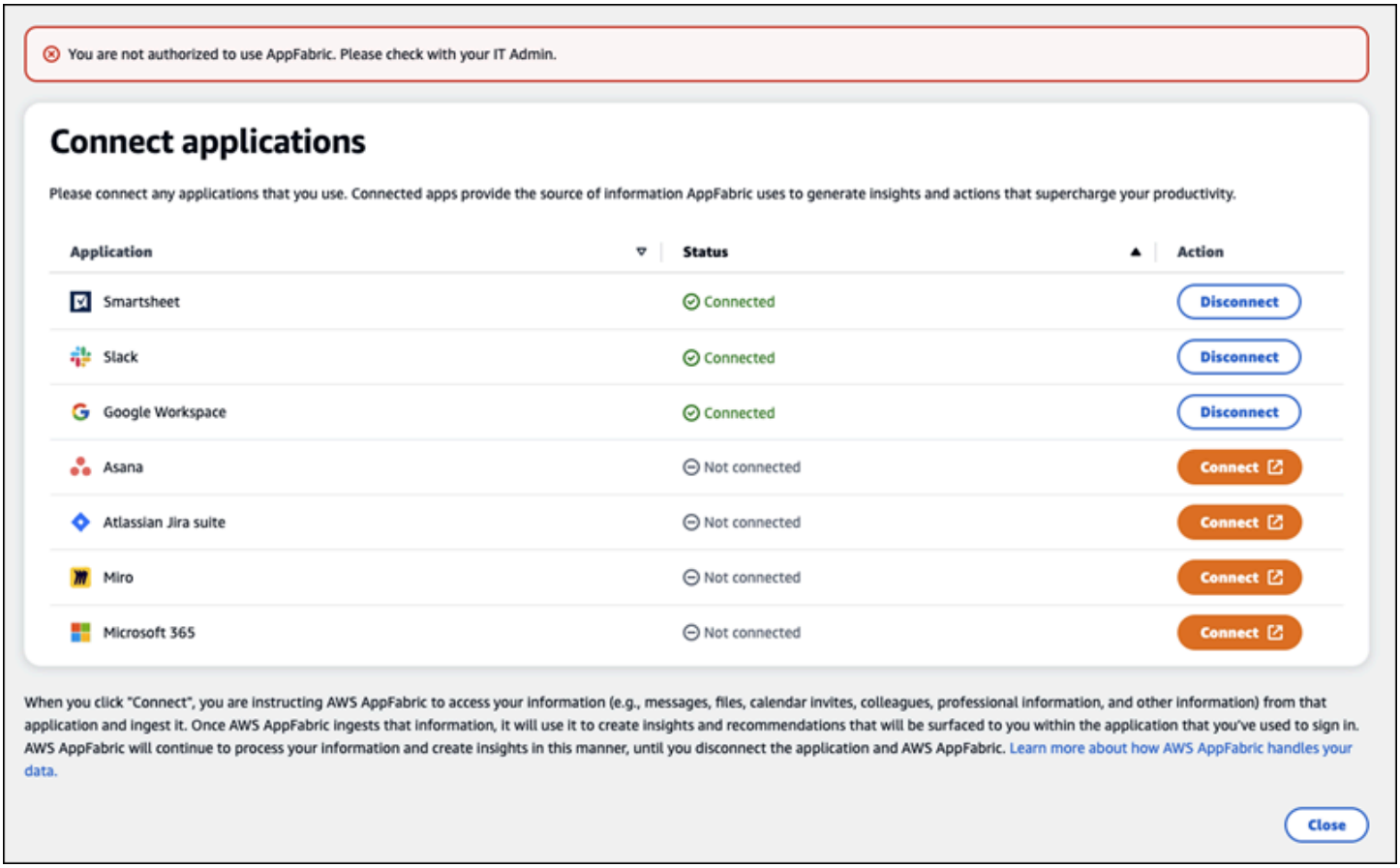
La richiesta è stata negata a causa del throttling della richiesta. Riprova tra qualche tempo () **`ThrottlingException`**

Potresti ricevere questo messaggio quando il portale AppFabric utente non riesce a elencare le applicazioni o disconnette un'applicazione a causa di un problema di limitazione. Riprova più tardi.



Non sei autorizzato a utilizzare. AppFabric Effettua AppFabric nuovamente il login a (**`AccessDeniedException`**)

Potresti ricevere questo messaggio quando il portale AppFabric utente non riesce a elencare le applicazioni o disconnette un'applicazione a causa di un'eccezione di accesso negato. Effettua AppFabric nuovamente l'accesso a.



AppFabric per la produttività APIs (anteprima)

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Questa sezione fornisce le operazioni dell'API, i tipi di dati e gli errori comuni per le funzionalità di AWS AppFabric produttività.

> **Note**
>
> Per tutte le altre AppFabric APIs, consulta l'AWS AppFabric API Reference.

Argomenti

- Azioni API AppFabric per la produttività (anteprima)
- Tipi di dati API AppFabric per la produttività (anteprima)

- Errori API comuni AppFabric per la produttività (anteprima)

Azioni API AppFabric per la produttività (anteprima)

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Le seguenti azioni sono supportate AppFabric per le funzionalità di produttività.

Per tutte le altre azioni AppFabric API, consulta la sezione Azioni AWS AppFabric API.

Argomenti

- Autorizza
- CreateAppClient
- DeleteAppClient
- GetAppClient
- ListActionableInsights
- ListAppClients
- ListMeetingInsights
- PutFeedback
- Token
- UpdateAppClient

Autorizza

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Autorizza un AppClient.

Argomenti

- Corpo della richiesta

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Parametro	Descrizione
app_client_id	L'ID del da autorizzare. AppClient
redirect_uri	L'URI a cui reindirizzare gli utenti finali dopo l'autorizzazione.
state	Un valore unico per mantenere lo stato tra la richiesta e il callback.

CreateAppClient

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Crea un AppClient.

Argomenti

- Corpo della richiesta
- Elementi di risposta

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Parametro	Descrizione
AppName	Il nome dell'app. Tipo: stringa Limitazioni di lunghezza: lunghezza minima di 1. Lunghezza massima di 255.

Parametro	Descrizione
	Campo obbligatorio: sì
Token client	Specifica un identificatore univoco con distinzione tra maiuscole e minuscole fornito per garantire l'idempotenza della richiesta . Ciò consente di riprovare la richiesta in tutta sicurezza senza eseguire accidentalmente la stessa operazione una seconda volta. Per passare lo stesso valore a una chiamata successiva a un'operazione è necessario passare lo stesso valore anche per tutti gli altri parametri. Si consiglia di utilizzare un tipo di valore UUID. Se non fornisci questo valore, ne AWS genera uno casuale per te. Se si riprova l'operazione con gli stessi parametri`ClientToken` , ma con parametri diversi, il tentativo fallisce e viene restituito un `IdempotentParameterMismatch` errore. Tipo: stringa Modello: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Campo obbligatorio: no

Parametro	Descrizione
customerManagedKeyIdentifier (Identificatore)	L'ARN del file chiave gestita dal cliente generato da. AWS Key Management Service La chiave viene utilizzata per crittografare i dati. Se non viene specificata alcuna chiave, Chiave gestita da AWS viene utilizzata una. Una mappa delle coppie chiave-valore del tag o dei tag da assegnare alla risorsa. Per ulteriori informazioni sulle chiavi gestite Chiavi di proprietà di AWS dai clienti, consulta Customer keys and AWS keys nella Developer Guide.AWS Key Management Service Tipo: stringa Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1011. Modello: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Campo obbligatorio: no
description	Una descrizione dell'app. Tipo: stringa Campo obbligatorio: sì
IconUrl	L'URL dell'icona o del logo di AppClient. Tipo: string Campo obbligatorio: no

Parametro	Descrizione
URL di reindirizzamento	L'URI a cui reindirizzare gli utenti finali dopo l'autorizzazione. Puoi aggiungere fino a 5 URL di reindirizzamento. Ad esempio, `https://localhost:8080` . Tipo: matrice di stringhe Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi. Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 2048 caratteri. Modello: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+` Campo obbligatorio: sì
starterUserEmails	Indirizzi email iniziali per gli utenti a cui è consentito l'accesso alla ricezione di informazioni dettagliate fino alla verifica. AppClient Tipo: matrice di stringhe Membri dell'array: numero minimo di 1 elemento. Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 320. Modello: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Campo obbligatorio: sì

Parametro	Descrizione
tags	Una mappa delle coppie chiave-valore del tag o dei tag da assegnare alla risorsa. Tipo: matrice di oggetti Tag Membri dell'array: numero minimo di 0 elementi. Numero massimo di 50 item. Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 201.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Parametro	Descrizione
appClientSummary	Contiene un riepilogo di AppClient. Tipo: oggetto AppClientSummary

DeleteAppClient

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Elimina un client applicativo.

Argomenti

- Corpo della richiesta
- Elementi di risposta

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Parametro	Descrizione
appClientIdentifier	L'Amazon Resource Name (ARN) o l'Universal Unique Identifier (UUID) da utilizzare AppClient per la richiesta. Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1011. Modello: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 204 con un corpo HTTP vuoto.

GetAppClient

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Restituisce informazioni su un AppClient.

Argomenti

- Corpo della richiesta
- Elementi di risposta

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Parametro	Descrizione
appClientIdentifier	L'Amazon Resource Name (ARN) o l'Universal Unique Identifier (UUID) da utilizzare AppClient per la richiesta. Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1011. Modello: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Campo obbligatorio: sì

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Parametro	Descrizione
AppClient	Contiene informazioni su un AppClient. Tipo: oggetto AppClient

ListActionableInsights

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Elenca i messaggi e-mail, le attività e gli altri aggiornamenti utilizzabili più importanti.

Argomenti

- Corpo della richiesta
- Elementi di risposta

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Parametro	Descrizione
nextToken	Se `nextToken` viene restituito, ci sono altri risultati disponibili. Il valore di `nextToken` è un token di impaginazione unico per ogni pagina. Effettua nuovamente la chiamata utilizzando il token restituito per recuperare la pagina successiva. Mantieni invariati tutti gli altri argomenti. Ogni token di impaginazione scade dopo 24 ore. L'utilizzo di un token di impaginazione scaduto restituirà un errore HTTP 400. InvalidToken

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 201.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Parametro	Descrizione
ActionableInsightsList	Elenca le informazioni utili, tra cui titolo, descrizione, azioni e data e ora di creazione. Per ulteriori informazioni, consulta ActionableInsights.
nextToken	Se `nextToken` viene restituito, ci sono più risultati disponibili. Il valore di `nextToken` è un token di impaginazione unico per ogni pagina. Effettua nuovamente la chiamata utilizzando il token restituito per recuperare la pagina successiva. Mantieni invariati tutti gli altri argomenti. Ogni token di impaginazione scade dopo 24 ore. L'utilizzo di un token di impaginazione scaduto restituirà un errore HTTP 400. InvalidToken Tipo: stringa

ListAppClients

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Restituisce un elenco di tutti AppClients.

Argomenti

- Corpo della richiesta
- Elementi di risposta

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Parametro	Descrizione
maxResults	Il numero massimo di risultati restituiti per chiamata. È possibile utilizzare `nextToken` per ottenere ulteriori pagine di risultati. Questo è solo un limite superiore. Il numero effettivo di risultati restituiti per chiamata potrebbe essere inferiore al massimo specificato. Intervallo valido: valore minimo di 1. valore massimo pari a 100.
nextToken	Se `nextToken` viene restituito, ci sono più risultati disponibili. Il valore di `nextToken` è un token di impaginazione unico per ogni pagina. Effettua nuovamente la chiamata utilizzando il token restituito per recuperare la pagina successiva. Mantieni invariati tutti gli altri argomenti. Ogni token di impaginazione scade dopo 24 ore. L'utilizzo di un token di impaginazione scaduto restituirà un errore HTTP 400. InvalidToken

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Parametro	Descrizione
appClientList	Contiene un elenco di risultati. AppClient Tipo: matrice di oggetti AppClientSummary
nextToken	Se `nextToken` viene restituito, ci sono altri risultati disponibili. Il valore di `nextToken` è un token di impaginazione unico per ogni pagina. Effettua nuovamente la chiamata utilizzando il token restituito per recuperare la pagina successiva. Mantieni invariati tutti gli altri argomenti. Ogni token di impaginazione scade dopo 24 ore. L'utilizzo di un token di impaginazione scaduto restituirà un errore HTTP 400. InvalidToken Tipo: stringa

ListMeetingInsights

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Elenca gli eventi più importanti del calendario su cui è possibile intervenire.

Argomenti

- Corpo della richiesta
- Elementi di risposta

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Parametro	Descrizione
nextToken	Se `nextToken` viene restituito, ci sono altri risultati disponibili. Il valore di `nextToken` è un token di impaginazione unico per ogni pagina. Effettua nuovamente la chiamata utilizzando il token restituito per recuperare la pagina successiva. Mantieni invariati tutti gli altri argomenti. Ogni token di impaginazione scade dopo 24 ore. L'utilizzo di un token di impaginazione scaduto restituirà un errore HTTP 400. InvalidToken

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 201.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Parametro	Descrizione
MeetingInsightList	Elenca le informazioni utili sulla riunione. Per ulteriori informazioni, consulta MeetingInsights.
nextToken	Se `nextToken` viene restituito, ci sono più risultati disponibili. Il valore di `nextToken` è un token di impaginazione unico per ogni pagina. Effettua nuovamente la chiamata utilizzando il token restituito per recuperare la pagina successiva. Mantieni invariati tutti gli altri argomenti. Ogni token di impaginazione scade dopo 24 ore. L'utilizzo di un token di impaginazione scaduto restituirà un errore HTTP 400. InvalidToken Tipo: stringa

PutFeedback

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Consente agli utenti di inviare feedback per una determinata analisi o azione.

Argomenti

- Corpo della richiesta
- Elementi di risposta

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Parametro	Descrizione
id	L'ID dell'oggetto per il quale viene inviato il feedback. Può essere il InsightId o il ActionId.
Feedback per	Il tipo di approfondimento per il quale viene inviato il feedback. Valori possibili: `ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION`
Valutazione del feedback	Valutazione del feedback da a1. 5 Più alto è il punteggio, meglio è.

Elementi di risposta

Se l'operazione riesce, il servizio invia una risposta HTTP 201 con un corpo HTTP vuoto.

Token

> La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Contiene informazioni che consentono di AppClients scambiare un codice di autorizzazione con un token di accesso.

Argomenti

- Corpo della richiesta
- Elementi di risposta

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Parametro	Descrizione
code	Il codice di autorizzazione ricevuto dall'endpoint di autorizzazione. Tipo: stringa Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 2048 caratteri. Campo obbligatorio: no
grant_type	Il tipo di concessione per il token. Deve essere `authorization_code` o `refresh_token`. Tipo: stringa Campo obbligatorio: sì
app_client_id	L'ID del AppClient. Tipo: stringa Modello: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Campo obbligatorio: sì
redirect_uri	L'URI di reindirizzamento passato all'endpoint di autorizzazione. Tipo: string Campo obbligatorio: no

Parametro	Descrizione
refresh_token	Il token di aggiornamento ricevuto dalla richiesta iniziale del token. Tipo: stringa Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 4096. Campo obbligatorio: no

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Parametro	Descrizione
appfabric_user_id	L'ID dell'utente per il token. Viene restituito solo per le richieste che utilizzano il tipo di `authorization_code` concessione. Tipo: stringa
expires_in	Il numero di secondi che mancano alla scadenza del token. Tipo: long
refresh_token	Il token di aggiornamento da utilizzare per una richiesta successiva. Tipo: stringa Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 2048 caratteri.
token	Il token di accesso. Tipo: stringa

Parametro	Descrizione
	Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 2048 caratteri.
token_type	Il tipo di token. Tipo: stringa

UpdateAppClient

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Aggiorna un AppClient.

Argomenti

- Corpo della richiesta
- Elementi di risposta

Corpo della richiesta

La richiesta accetta i seguenti dati in formato JSON.

Parametro	Descrizione
appClientIdentifier	L'Amazon Resource Name (ARN) o l'Universal Unique Identifier (UUID) da utilizzare AppClient per la richiesta. Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1011. Modello: `arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Campo obbligatorio: sì

Parametro	Descrizione
URL di reindirizzamento	L'URI a cui reindirizzare gli utenti finali dopo l'autorizzazione. Puoi aggiungere fino a 5 URL di reindirizzamento. Ad esempio, `https://localhost:8080` . Tipo: matrice di stringhe Membri dell'array: numero minimo di 1 elemento. Numero massimo 5 elementi. Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 2048 caratteri. Modello: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200.

I dati seguenti vengono restituiti in formato JSON mediante il servizio.

Parametro	Descrizione
AppClient	Contiene informazioni su un AppClient. Tipo: oggetto AppClient

Tipi di dati API AppFabric per la produttività (anteprima)

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

L' AppFabric API contiene diversi tipi di dati utilizzati da varie azioni. Questa sezione descrive in dettaglio i tipi di dati AppFabric per le funzionalità di produttività.

Per tutti gli altri tipi di dati AppFabric API, consulta Tipi di dati AWS AppFabric API.

> **Important**
>
> L'ordine di ogni elemento in una struttura di tipi di dati non è garantito. Le applicazioni non devono assumere un determinato ordine.

Argomenti

ActionableInsights

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Contiene un riepilogo delle azioni importanti e adatte per un utente in base a e-mail, inviti al calendario, messaggi e attività dal portafoglio di app. Gli utenti possono visualizzare informazioni proattive provenienti da tutte le loro applicazioni per aiutarli a orientare al meglio la giornata. Queste informazioni giustificano il motivo per cui un utente dovrebbe interessarsi al riepilogo delle informazioni, oltre a riferimenti, come i link incorporati, alle singole app e agli artefatti che hanno generato le informazioni.

Parametro	Descrizione
InsightID	L'ID univoco per l'analisi generata.
Insight Content	Ciò restituisce un riepilogo delle informazioni e dei collegamenti incorporati agli artefatti utilizzati per generare l'analisi.

Parametro	Descrizione
	Si tratterebbe di un contenuto HTML contenente link incorporati (<a>tag).
Titolo approfondito	Il titolo dell'intuizione generata.
CreatedAt	Quando è stata generata l'intuizione.
azioni	Un elenco di azioni consigliate per l'analisi generata. L'oggetto azione contiene i seguenti parametri: • `actionId`— L'id univoco per l'azione generata. • `actionIconUrl` — L'URL dell'icona dell'app in cui si suggerisce di eseguire l'azione. • `actionTitle` — Il titolo dell'azione generata. • `actionUrl` — L'URL univoco per l'utente finale per visualizzare ed eseguire l'azione nel AppFabric portale utenti. Per eseguire azioni, le app ISV reindirizzeranno gli utenti al portale AppFabric utenti (schermata pop-up) utilizzando questo URL. • `actionExecutionStatus` — Un enum che indica lo stato dell'azione. I valori possibili sono: `EXECUTED | NOT_EXECUTED`

AppClient

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Contiene informazioni su un AppClient.

Parametro	Descrizione
AppName	Il nome dell'applicazione. Tipo: stringa Campo obbligatorio: sì
arn	L'Amazon Resource Name (ARN) del AppClient. Tipo: stringa Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1011. Modello: `arn:.+` Campo obbligatorio: sì
description	Una descrizione dell'applicazione. Tipo: stringa Campo obbligatorio: sì
IconUrl	L'URL dell'icona o del logo di AppClient. Tipo: string Campo obbligatorio: no
URL di reindirizzamento	Il reindirizzamento consentito per URLs . AppClient Tipo: matrice di stringhe Membri dell’array: numero minimo di 1 elemento. Numero massimo 5 elementi. Limitazioni di lunghezza: lunghezza minima di 1. La lunghezza massima è 2048 caratteri. Modello: `(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

Parametro	Descrizione
	Campo obbligatorio: sì
starterUserEmails	Indirizzi email iniziali per gli utenti a cui AppClient è consentito l'accesso per ricevere approfondimenti fino alla verifica. Tipo: matrice di stringhe Membri dell'array: numero minimo di 1 elemento. Limitazioni di lunghezza: lunghezza minima di 0. Lunghezza massima di 320. Modello: `[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` Campo obbligatorio: sì
Dettagli di verifica	Contiene lo stato e il motivo della AppClient verifica. Tipo: oggetto VerificationDetails Campo obbligatorio: sì
customerManagedKeyArn	L'Amazon Resource Name (ARN) del file chiave gestita dal cliente generato da AWS Key Management Service per. AppClient Tipo: stringa Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1011. Modello: `arn:.+` Campo obbligatorio: no

Parametro	Descrizione
appClientId	L'ID del AppClient. Pensato per essere usato nei flussi o-auth per l'app-client. Tipo: stringa Modello: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Campo obbligatorio: no

AppClientSummary

La funzione AWS AppFabric per la produttività è in anteprima ed è soggetta a modifiche.

Contiene informazioni su un AppClient.

Parametro	Descrizione
fienile	L'Amazon Resource Name (ARN) del AppClient. Tipo: stringa Limitazioni di lunghezza: lunghezza minima pari a 1. Lunghezza massima di 1011. Modello: `arn:.+` Campo obbligatorio: sì
Stato della verifica	Lo stato della AppClient verifica. Tipo: stringa Valori validi: `pending_verification | verified | rejected`

Parametro	Descrizione
	Campo obbligatorio: sì
appClientId	L'ID del AppClient. Pensato per essere usato nei flussi o-auth per l'app-client. Tipo: stringa Modello: `[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` Campo obbligatorio: no

MeetingInsights

La funzione AWS AppFabric per la produttività è in anteprima ed è soggetta a modifiche.

Contiene un riepilogo delle 3 riunioni principali insieme allo scopo della riunione, agli elementi correlati tra le app e alle attività relative a attività, e-mail, messaggi ed eventi del calendario.

Parametro	Descrizione
InsightID	L'ID univoco per l'analisi generata.
Insight Content	La descrizione dell'analisi che evidenzia i dettagli in formato stringa. Ad esempio, perché questa intuizione è importante.
Titolo di approfondimento	Il titolo dell'intuizione generata.
CreatedAt	Quando è stata generata l'intuizione.
Evento del calendario	L'evento o la riunione importante del calendario su cui l'utente dovrebbe concentrarsi. Oggetto Calendar Event: • `startTime` — L'ora di inizio dell'evento.

Parametro	Descrizione
	• `endTime`— L'ora di fine dell'evento. • `eventUrl`— L'URL dell'evento del calendario sull'app ISV.
resources	L'elenco contenente le altre risorse relative alla generazione dell'analisi. Oggetto risorsa: • `appName`— Il nome dell'app a cui appartiene la risorsa. • `resourceTitle` — Il titolo della risorsa. • `resourceType` — Il tipo di risorsa. I valori possibili sono: `EMAIL | EVENT | MESSAGE | TASK` • `resourceUrl` — L'URL della risorsa nell'app. • `appIconUrl` — L'URL dell'immagine dell'app a cui appartien e la risorsa.
nextToken	Il token di impaginazione per recuperare il prossimo set di approfondimenti. È un campo opzionale che, se restituito nullo, significa che non ci sono più approfondimenti da caricare.

VerificationDetails

La funzione AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Contiene lo stato e il motivo della AppClient verifica.

Parametro	Descrizione
Stato della verifica	Lo stato della AppClient verifica. Tipo: stringa

Parametro	Descrizione
	Valori validi: `pending_verification | verified | rejected` Campo obbligatorio: sì
Status/Motivo	Il motivo dello stato AppClient della verifica. Tipo: stringa Limitazioni di lunghezza: lunghezza minima pari a 1. La lunghezza massima è 1024 caratteri. Campo obbligatorio: no

Errori API comuni AppFabric per la produttività (anteprima)

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Questa sezione elenca gli errori comuni alle azioni API per le funzionalità di AWS AppFabric produttività.

Per tutti gli altri errori AppFabric comuni delle API, consulta Risolvi i problemi per la AppClients produttività AppFabric gli AWS AppFabric errori comuni delle AWS AppFabric API nel riferimento API.

Nome dell'eccezione	Descrizione
TokenException	La richiesta del token non è valida. Codice di stato HTTP: 400

Elaborazione dei dati in AppFabric

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

AppFabric adotta misure per archiviare i contenuti degli utenti individualmente, in un bucket Amazon S3 gestito da AppFabric e separatamente; il che aiuta a garantire la generazione di informazioni specifiche per l'utente. Utilizziamo misure di sicurezza ragionevoli per proteggere i tuoi contenuti, che possono includere la crittografia in archivio e in transito. Abbiamo configurato i nostri sistemi per eliminare automaticamente i contenuti dei clienti entro 30 giorni dall'inserimento. AppFabric non genera approfondimenti utilizzando artefatti di dati a cui un utente non ha più accesso. Ad esempio, quando un utente disconnette una fonte di dati (un'app), AppFabric smette di raccogliere dati da quell'app e non utilizza alcun artefatto persistente delle app disconnesse per generare approfondimenti. AppFabrici sistemi sono configurati per eliminare tali dati entro 30 giorni.

AppFabric non utilizza i contenuti degli utenti per addestrare o migliorare i modelli linguistici di grandi dimensioni sottostanti utilizzati per generare approfondimenti. Per ulteriori informazioni sulla funzionalità AppFabric di intelligenza artificiale generativa, consulta Amazon FAQs Bedrock.

Crittografia a riposo

AWS AppFabric supporta la crittografia a riposo, una funzionalità di crittografia lato server in cui crittografa in AppFabric modo trasparente tutti i dati relativi agli utenti quando vengono salvati su disco e li decrittografa quando accedi ai dati.

Crittografia in transito

AppFabric protegge tutti i contenuti in transito utilizzando TLS 1.2 e firma le richieste API per i AWS servizi con AWS Signature Version 4.

Terminologia e concetti in AppFabric

Questo argomento descrive la terminologia e i concetti chiave AWS AppFabric per aiutarti a iniziare.

Pacchetto di app

Un pacchetto di AppFabric app memorizza tutte le autorizzazioni e le acquisizioni delle AppFabric app (vedi la seguente definizione di ingestioni). Puoi creare un pacchetto di app per ogni app. Account AWS Regione AWS

AppClient (anche client di app e client di applicazioni)

E OAuth AppClient per l'app per il destinatario dei dati. Ogni app destinataria dei dati deve registrarsi e accedere AppClient ai AppFabric dati. Un utente sviluppatore deve disporre di un AWS account per registrarsi AppClient. Ogni AWS account può registrarne solo uno AppClient. AppFabric venderà token di accesso basati su. AppClient AppClient conterrà informazioni sull'app di ricezione dei dati che accederà ai AppFabric dati tramite questa. AppClient

Autorizzazione dell'app

L'autorizzazione dell'app concede AppFabric l'autorizzazione a connettersi e interagire con le applicazioni. Consente l'inserimento dei log di controllo dalle applicazioni, con credenziali OAuth (Open Authorization, uno standard aperto per la delega di accesso per concedere l'accesso alle applicazioni) o un token di accesso personale (PAT). È possibile configurare più autorizzazioni di app (fino a 50) per pacchetto di app. Ciò consente di AppFabric inserire i registri di controllo da più tenant delle applicazioni, ripetendo la fase di creazione dell'autorizzazione dell'app secondo necessità per ogni tenant dell'applicazione. Le credenziali condivise vengono crittografate con una Chiave di proprietà di AWS o una chiave gestita dal cliente fornita da AWS Key Management Service (AWS KMS) e vengono archiviate in. AppFabric

Ingestione

Un' AppFabric ingestione utilizza l'autorizzazione di un'app per estrarre i registri di controllo da un'applicazione rendendoli pubblici dell'applicazione. APIs Quindi invia i log di controllo a una o più (fino a cinque) destinazioni.

ID client

Quando crei un'autorizzazione per la connessione a un'applicazione che utilizza il OAuth flusso, AppFabric potrebbe chiederti l'ID client e il segreto del client. L'ID client e il segreto del client sono

disponibili nell'app di autenticazione dell'applicazione. Per istruzioni su dove trovare l'ID client in una determinata app di autenticazione, consulta Applicazioni supportate. L'ID client e il client secret condivisi vengono crittografati con una chiave Chiave di proprietà di AWS o una AWS KMS chiave gestita dal cliente e archiviati in AppFabric.

Client secret

Quando crei un'app, l'autorizzazione per la connessione a un'applicazione che utilizza il OAuth flusso, AppFabric potrebbe chiederti l'ID client e il segreto del client. L'ID client e il segreto del client sono disponibili nell'app di autenticazione dell'applicazione. Per istruzioni su dove trovare il client secret in una determinata app di autenticazione, consulta Applicazioni supportate. L'ID client e il segreto client condivisi vengono crittografati con una chiave Chiave di proprietà di AWS o una AWS KMS chiave gestita dal cliente e archiviati in AppFabric.

Destinazione di ingestione

Una destinazione di ingestione definisce dove devono essere conservati i registri di controllo estratti da un'ingestione. Ogni ingestione può fornire log di controllo a una o più destinazioni (fino a cinque), che sono un bucket Amazon Simple Storage Service (Amazon S3) o un Amazon Data Firehose nel tuo. Account AWS Per ogni destinazione, puoi definire se desideri che i log siano in forma grezza o normalizzati in uno schema Open Cybersecurity Schema Framework (OCSF). Quando si seleziona lo schema OCSF, è possibile definire il formato dei log (JSON o Apache Parquet). La Apache Parquet il formato può essere utilizzato solo se Amazon S3 è selezionato come destinazione.

app per i destinatari dei dati

App da cui richiameranno AppFabric per ottenere informazioni generate AppFabric.

OAuth

OAuth è un protocollo aperto che consente l'autorizzazione sicura con un metodo semplice e standard da applicazioni web, mobili e desktop. AppFabric utilizza OAuth per creare alcune autorizzazioni per le app.

Open Cybersecurity Schema Framework (OCSF)

L'Open Cybersecurity Schema Framework (OCSF) è un progetto open source che fornisce un framework estensibile per lo sviluppo di schemi, insieme a uno schema di sicurezza di base indipendente dal fornitore. I fornitori e gli altri produttori di dati possono adottare ed estendere lo schema per i loro domini specifici. L'obiettivo è fornire uno standard aperto, adottato in qualsiasi

ambiente, applicazione o soluzione, integrando al contempo gli standard e i processi di sicurezza esistenti. AppFabric ha esteso questo schema per creare una struttura di eventi incentrata sul software as a service (SaaS) su cui verranno normalizzati tutti i log di controllo delle app SaaS supportati. AppFabric Per ulteriori informazioni, consulta Open Cybersecurity Schema Framework per AWS AppFabric.

Token di accesso personale (PAT)

Un token di accesso personale (PAT) è una stringa di caratteri che può essere utilizzata per accedere a un sistema informatico anziché la normale password. Quando crei l'autorizzazione di un'app per la connessione a un'applicazione che utilizza il flusso PAT, AppFabric potrebbe chiederti un PAT. Il PAT è disponibile nell'app di autenticazione dell'applicazione. Per istruzioni su dove trovare il PAT in un'app di autenticazione specifica, consulta Applicazioni supportate. I token dell'account di servizio condivisi sono crittografati con una chiave Chiave di proprietà di AWS o una AWS KMS chiave gestita dal cliente e archiviati in. AppFabric

Token dell'account di servizio

Quando si crea un' AppFabric autorizzazione per connettersi a un'applicazione, alcune applicazioni richiedono la creazione di un account di servizio per l'autenticazione dell'applicazione. AppFabric potrebbe richiedere il token dell'account di servizio come parte del processo di autorizzazione dell'app. Per istruzioni su dove trovare il token dell'account di servizio in una determinata app di autenticazione, consulta Applicazioni supportate. I token dell'account di servizio condivisi sono crittografati con una chiave Chiave di proprietà di AWS o una AWS KMS chiave gestita dal cliente e archiviati in AppFabric.

ID tenant

Quando crei un'autorizzazione per l'app, AppFabric potrebbe chiederti l'ID del tenant e il nome del tenant della tua app. L'ID tenant è un identificatore univoco per il tenant dell'applicazione. Ogni applicazione potrebbe avere termini diversi per un tenant, ad esempio Workspace ID for Slack o ID di dominio per Asana. Per istruzioni su dove trovare l'ID del tenant in un'applicazione specifica, consulta Applicazioni supportate.

Nome del tenant

Quando crei un'autorizzazione per l'app, AppFabric potrebbe chiederti l'ID del tenant e il nome del tenant della tua app. Il nome del tenant è un nome univoco che dai all'ID del tenant, da utilizzare all'interno di un pacchetto di app. Questo valore viene utilizzato per etichettare l'autorizzazione dell'app e qualsiasi relativa ingestione.

Sicurezza in AWS AppFabric

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gira Servizi AWS su Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili AWS AppFabric, consulta AWS Servizi nell'ambito del programma di conformitàAWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dall'uso Servizio AWS che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AppFabric. Negli argomenti seguenti viene illustrato come eseguire la configurazione AppFabric per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzarne altri Servizi AWS che ti aiutano a monitorare e proteggere AppFabric le tue risorse.

Argomenti

Protezione dei dati in AWS AppFabric

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS AppFabric. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori AppFabric o Servizi AWS utilizzi la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo

vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

> **Note**
>
> Per ulteriori informazioni sulla protezione dei dati applicata AppFabric alla sicurezza, consultaElaborazione dei dati in AppFabric.

Crittografia a riposo

AWS AppFabric supporta la crittografia a riposo, una funzionalità di crittografia lato server in cui crittografa in AppFabric modo trasparente tutti i dati relativi ai bundle di app quando vengono salvati su disco e li decrittografa quando si accede ai dati. Per impostazione predefinita, AppFabric crittografa i dati utilizzando an from (). Chiave di proprietà di AWS AWS Key Management Service AWS KMS Puoi anche scegliere di crittografare i tuoi dati utilizzando la tua chiave gestita dal cliente di. AWS KMS

Quando elimini un pacchetto di app, tutti i relativi metadati vengono eliminati definitivamente.

Crittografia in transito

Quando configuri un app bundle, puoi scegliere una chiave Chiave di proprietà di AWS o una chiave gestita dal cliente. Durante la raccolta e la normalizzazione dei dati per l'inserimento di un log di controllo, AppFabric archivia temporaneamente i dati in un bucket Amazon Simple Storage Service (Amazon S3) intermedio e li crittografa utilizzando questa chiave. Questo bucket intermedio viene eliminato dopo 30 giorni, utilizzando una politica del ciclo di vita del bucket.

AppFabric protegge tutti i dati in transito utilizzando TLS 1.2 e firma le richieste API con Signature V4. Servizi AWS AWS

Gestione delle chiavi

AppFabric supporta la crittografia dei dati con una Chiave di proprietà di AWS o una chiave gestita dal cliente. Ti consigliamo di utilizzare una chiave gestita dal cliente perché ti dà il pieno controllo dei tuoi dati crittografati. Quando scegli una chiave gestita dal cliente, AppFabric associa una politica delle risorse alla chiave gestita dal cliente che le consente l'accesso alla chiave gestita dal cliente.

Chiave gestita dal cliente

Per creare una chiave gestita dal cliente, segui i passaggi per la creazione di chiavi KMS con crittografia simmetrica nella Guida per gli sviluppatori.AWS KMS

Policy della chiave

Le politiche chiave controllano l'accesso alle chiavi gestite dai clienti. Ogni chiave gestita dal cliente deve avere esattamente una policy della chiave, che contiene istruzioni che determinano chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, puoi specificare una policy della chiave. Per informazioni sulla creazione di una policy chiave, consulta Creating a key policy nella AWS KMS Developer Guide.

Per utilizzare una chiave gestita dal cliente con AppFabric, l'utente o il ruolo AWS Identity and Access Management (IAM) che crea le AppFabric risorse deve disporre dell'autorizzazione a utilizzare la chiave gestita dal cliente. Ti consigliamo di creare una chiave da utilizzare solo con AppFabric e di aggiungere gli AppFabric utenti come utenti della chiave. Questo approccio limita l'ambito di accesso ai dati. Le autorizzazioni richieste dagli utenti sono le seguenti:

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Decrypt`

La AWS KMS console guida l'utente nella creazione di una chiave con la policy chiave appropriata. Per ulteriori informazioni sulle politiche chiave, consulta le politiche chiave AWS KMS nella Guida per gli AWS KMS sviluppatori.

Di seguito è riportato un esempio di policy chiave che consente:

- Il Utente root dell'account AWS pieno controllo della chiave.
- Utenti autorizzati AppFabric a utilizzare la chiave gestita dal cliente con AppFabric.
- Una politica chiave per la configurazione di un pacchetto di app in`us-east-1`.

```
{
    "Id": "key-consolepolicy-3",
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key_ID"
        },
        {
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow access to principals authorized to use AWS AppFabric",
            "Effect": "Allow",
            "Principal": {"AWS": "IAM-role/user-creating-appfabric-resources"},
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "appfabric.us-east-1.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        }
    ]
}
```

Come AppFabric utilizza le sovvenzioni in AWS KMS

AppFabric richiede una concessione per utilizzare la chiave gestita dal cliente. Per ulteriori informazioni, consulta Grants AWS KMS nella AWS KMS Developer Guide.

Quando crei un pacchetto di app, AppFabric crea una sovvenzione per tuo conto inviando una `CreateGrant` richiesta a. AWS KMS Le sovvenzioni AWS KMS vengono utilizzate per AppFabric consentire l'accesso a una AWS KMS chiave in un account cliente. AppFabric richiede la concessione dell'utilizzo della chiave gestita dal cliente per le seguenti operazioni interne:

- Invia `GenerateDataKey` richieste per AWS KMS generare chiavi dati crittografate dalla chiave gestita dal cliente.
- Invia `Decrypt` richieste per AWS KMS decrittografare le chiavi di dati crittografate in modo che possano essere utilizzate per crittografare i dati e per decrittografare i token di accesso alle applicazioni in transito.
- Invia `Encrypt` richieste a per crittografare i token di accesso AWS KMS alle applicazioni in transito.

Di seguito è riportato un esempio di sovvenzione.

```
{
  "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 elimini un pacchetto di app, AppFabric ritira le sovvenzioni emesse sulla chiave gestita dal cliente.

Monitoraggio delle chiavi di crittografia per AppFabric

Quando utilizzi chiavi gestite AWS KMS dal cliente con AppFabric, puoi utilizzare AWS CloudTrail i log per tenere traccia delle richieste AppFabric inviate a AWS KMS.

Di seguito è riportato un esempio di CloudTrail evento registrato quando viene AppFabric utilizzato `CreateGrant` per la chiave gestita dal 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"
    }
```

```
}
```

Gestione delle identità e degli accessi per AWS AppFabric

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AppFabric IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AppFabric svolgi.

Utente del servizio: se utilizzi il AppFabric servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AppFabric funzionalità per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AppFabric, consulta Risoluzione dei problemi di AWS AppFabric identità e accesso.

Amministratore del servizio: se sei responsabile delle AppFabric risorse della tua azienda, probabilmente hai pieno accesso a AppFabric. È tuo compito determinare a quali AppFabric

funzionalità e risorse devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con AppFabric, consultaCome AWS AppFabric funziona con IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AppFabric. Per visualizzare esempi di policy AppFabric basate sull'identità che puoi utilizzare in IAM, consulta. Esempi di policy basate su identità per AWS AppFabric

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA)AWS in IAM nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti

alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni.

AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi

possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Elenchi di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.
- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.

- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

Come AWS AppFabric funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AppFabric, scopri con quali funzionalità IAM è disponibile l'uso AppFabric.

Funzionalità IAM che puoi utilizzare con AWS AppFabric

Funzionalità IAM	AppFabric supporto
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì

Funzionalità IAM	AppFabric supporto
Chiavi di condizione delle policy	No
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	No
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una panoramica generale di come AppFabric e altri Servizi AWS utilizzi la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per AppFabric

Supporta le policy basate su identità: sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di politiche basate sull'identità per AppFabric

Per visualizzare esempi di politiche basate sull' AppFabric identità, vedere. Esempi di policy basate su identità per AWS AppFabric

Politiche basate sulle risorse all'interno AppFabric

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per AppFabric

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di AppFabric azioni, vedere Azioni definite da AWS AppFabric nel Service Authorization Reference.

Le azioni politiche in AppFabric uso utilizzano il seguente prefisso prima dell'azione:

```
appfabric
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "appfabric:action1",
      "appfabric:action2"
         ]
```

È possibile specificare più azioni utilizzando caratteri jolly ()*. Ad esempio, per specificare tutte le operazioni che iniziano con la parola `List`, includi la seguente operazione.

```
"Action": "appfabric:List*"
```

Per visualizzare esempi di politiche AppFabric basate sull'identità, vedere. Esempi di policy basate su identità per AWS AppFabric

Risorse politiche per AppFabric

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di AppFabric risorse e relativi ARNs, vedere Tipi di risorse definiti da AWS AppFabric nel Service Authorization Reference. Per informazioni con quali azioni è possibile specificare l'ARN di ciascuna risorsa, vedere Azioni definite da. AWS AppFabric

Per visualizzare esempi di politiche basate sull' AppFabric identità, vedere. Esempi di policy basate su identità per AWS AppFabric

Chiavi relative alle condizioni delle politiche per AppFabric

Supporta le chiavi delle condizioni delle politiche specifiche del servizio: No

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di AppFabric condizione, consulta Condition keys for AWS AppFabric nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, vedi Azioni definite da AWS AppFabric.

Per visualizzare esempi di politiche AppFabric basate sull'identità, vedere. Esempi di policy basate su identità per AWS AppFabric

ACLs in AppFabric

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AppFabric

Supporta ABAC (tag nelle policy): sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con AppFabric

Supporta credenziali temporanee: No

Alcune Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-On (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali multiservizio per AppFabric

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per AppFabric

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità. AppFabric Modifica i ruoli di servizio solo quando viene AppFabric fornita una guida in tal senso.

Ruoli collegati ai servizi per AppFabric

Supporta ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli AppFabric collegati ai servizi, consulta. Utilizzo di ruoli collegati ai servizi per AppFabric

Esempi di policy basate su identità per AWS AppFabric

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AppFabric. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da AppFabric, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione AWS AppFabric nel Service Authorization Reference.

Indice

- Consenti l'accesso alla creazione AppClients
- Consenti l'accesso per ottenere i dettagli di AppClients
- Consenti l'accesso all'elenco AppClients
- Consenti l'accesso all'aggiornamento AppClients
- Consenti l'accesso per l'eliminazione AppClients
- Consenti l'accesso per autorizzare le applicazioni

- Altri esempi di policy IAM
  - Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare AppFabric risorse nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla

sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.

- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console di AppFabric

Allega la policy `AWSAppFabricReadOnlyAccess` AWS gestita alle tue identità IAM per concedere loro l'autorizzazione di sola lettura al AppFabric servizio, inclusa la console in. AppFabric AWS Management Console In alternativa, puoi allegare la policy `AWSAppFabricFullAccess` AWS gestita alle tue identità IAM per concedere loro l'autorizzazione amministrativa completa al servizio. AppFabric Per ulteriori informazioni, consulta AWS politiche gestite per AWS AppFabric.

AppFabric per esempi di policy IAM sulla sicurezza

I seguenti esempi di policy si applicano alle funzionalità di sicurezza di AppFabric for.

Consenti l'accesso ai pacchetti di app

Il seguente esempio di policy concede l'accesso ai pacchetti di app del servizio. AppFabric

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
```

```
}
```

Limita l'accesso ai pacchetti di app

Il seguente esempio di policy limita l'accesso ai pacchetti di app del servizio. AppFabric

```
{
    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Limita l'eliminazione o l'interruzione delle acquisizioni

Il seguente esempio di policy limita l'eliminazione o l'interruzione delle acquisizioni nel servizio. 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 per la produttività, esempi di policy IAM

La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

I seguenti esempi di policy si applicano alle funzionalità AppFabric per la produttività.

Consenti l'accesso (accesso in sola lettura) alle funzionalità di produttività

Il seguente esempio di policy concede l'accesso in sola lettura alle funzionalità per la produttività. AppFabric

> **Important**
>
> Potresti visualizzare un errore di azione non valida quando aggiungi questa policy nell'editor di policy JSON della console IAM. Questo perché le funzionalità AppFabric per la produttività sono attualmente disponibili in anteprima. È necessario ignorare l'errore e procedere con la creazione della politica.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppClient",
                "appfabric:ListActionableInsights",
                "appfabric:ListAppClients",
                "appfabric:ListMeetingInsights"
            ],
            "Resource": "*"
        }
    ],
```

```
    "Version": "2012-10-17"
}
```

Consenti l'accesso completo alle funzionalità di produttività

Il seguente esempio di policy garantisce l'accesso completo alle funzionalità AppFabric per la produttività.

> **Important**
>
> Potresti visualizzare un errore di azione non valido quando aggiungi questa policy nell'editor di policy JSON della console IAM. Questo perché le funzionalità AppFabric per la produttività sono attualmente disponibili in anteprima. È necessario ignorare l'errore e procedere con la creazione della politica.

```
{
    "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"
}
```

Consenti l'accesso alla creazione AppClients

Il seguente esempio di policy concede l'accesso alla creazione AppClients. Per ulteriori informazioni, consulta Creare un uomo AppFabric per la produttività AppClient.

> **Important**
>
> Potresti visualizzare un errore di azione non valida quando aggiungi questa policy nell'editor di policy JSON della console IAM. Questo perché le funzionalità AppFabric per la produttività sono attualmente disponibili in anteprima. È necessario ignorare l'errore e procedere con la creazione della politica.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:CreateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Consenti l'accesso per ottenere i dettagli di AppClients

Il seguente esempio di policy consente l'accesso per ottenere i dettagli di AppClients. Per ulteriori informazioni, consulta Ottenere i dettagli di un AppClient.

> **Important**
>
> Potresti visualizzare un errore di azione non valida quando aggiungi questa policy nell'editor di policy JSON della console IAM. Questo perché le funzionalità AppFabric per la produttività sono attualmente disponibili in anteprima. È necessario ignorare l'errore e procedere con la creazione della politica.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "appfabric:GetAppClient",
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Consenti l'accesso all'elenco AppClients

Il seguente esempio di policy concede l'accesso all'elenco AppClients. Per ulteriori informazioni, consulta Ottenere i dettagli di un AppClient.

> **Important**
>
> Potresti visualizzare un errore di azione non valida quando aggiungi questa policy nell'editor di policy JSON della console IAM. Questo perché le funzionalità AppFabric per la produttività sono attualmente disponibili in anteprima. È necessario ignorare l'errore e procedere con la creazione della politica.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:ListAppClients"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Consenti l'accesso all'aggiornamento AppClients

Il seguente esempio di policy concede l'accesso all'aggiornamento AppClients. Per ulteriori informazioni, vedere Update an AppClient.

> **Important**
>
> Potresti visualizzare un errore di azione non valida quando aggiungi questa policy nell'editor di policy JSON della console IAM. Questo perché le funzionalità AppFabric per la produttività sono attualmente disponibili in anteprima. È necessario ignorare l'errore e procedere con la creazione della politica.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:UpdateAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Consenti l'accesso per l'eliminazione AppClients

Il seguente esempio di policy concede l'accesso all'eliminazione AppClients. Per ulteriori informazioni, vedere Aggiornare un AppClient.

> **Important**
>
> Potresti visualizzare un errore di azione non valida quando aggiungi questa policy nell'editor di policy JSON della console IAM. Questo perché le funzionalità AppFabric per la produttività sono attualmente disponibili in anteprima. È necessario ignorare l'errore e procedere con la creazione della politica.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
```

```
                "appfabric:DeleteAppClient"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Consenti l'accesso per autorizzare le applicazioni

Il seguente esempio di policy concede l'accesso per autorizzare le applicazioni utilizzando l'API Token. Per ulteriori informazioni, consulta Autenticare e autorizzare l'applicazione.

> **Important**
>
> Potresti visualizzare un errore di azione non valida quando aggiungi questa policy nell'editor di policy JSON della console IAM. Questo perché le funzionalità AppFabric per la produttività sono attualmente disponibili in anteprima. È necessario ignorare l'errore e procedere con la creazione della politica.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:Token"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appclient/*"]
        }
    ],
    "Version": "2012-10-17"
}
```

Altri esempi di policy IAM

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente.

Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l' AWS CLI API o. AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Utilizzo di ruoli collegati ai servizi per AppFabric

AWS AppFabric utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AppFabric I ruoli

collegati ai servizi sono predefiniti AppFabric e includono tutte le autorizzazioni richieste dal servizio per chiamare altri utenti per tuo conto. Servizi AWS

Un ruolo collegato al servizio semplifica la configurazione AppFabric perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AppFabric definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AppFabric Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi AppFabric le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta AWS i servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per AppFabric

AppFabric utilizza il ruolo collegato al servizio denominato`AWSServiceRoleForAppFabric`: consente di AppFabric inserire dati in una risorsa di destinazione di importazione, come un bucket Amazon S3 o un flusso di distribuzione Amazon Data Firehose. Consente inoltre di inserire dati metrici nel AppFabric namespace. CloudWatch `AWS/AppFabric`

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForAppFabric` considera attendibili i seguenti servizi:

- `appfabric.amazonaws.com`

La politica di autorizzazione dei ruoli denominata `AWSAppFabricServiceRolePolicy` consente di AppFabric completare le seguenti azioni sulle risorse specificate:

- Azione: `cloudwatch:PutMetricData` nello `AWS/AppFabric` spazio dei nomi. Questa azione concede l'autorizzazione per AppFabric inserire dati metrici nello spazio dei nomi Amazon CloudWatch`AWS/AppFabric`. Per ulteriori informazioni sulle AppFabric metriche disponibili in, consulta. CloudWatch Monitoraggio AWS AppFabric con Amazon CloudWatch
- Azione: `s3:PutObject` in un bucket Amazon S3. Questa azione concede l'autorizzazione AppFabric a inserire i dati importati in un bucket Amazon S3 specificato.

- Azione: `firehose:PutRecordBatch` in un flusso di distribuzione di Amazon Data Firehose. Questa azione concede l'autorizzazione AppFabric a inserire i dati importati in un flusso di distribuzione Amazon Data Firehose specificato.

Per ulteriori informazioni, consulta Policy gestite da AWS per AppFabric.

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per AppFabric

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un pacchetto di AppFabric app in AWS Management Console, l'o l' AWS API AWS CLI, AppFabric crea automaticamente il ruolo collegato al servizio.

Modifica di un ruolo collegato ai servizi per AppFabric

AppFabric non ti consente di modificare il ruolo collegato al `AWSServiceRoleForAppFabric` servizio. Dopo aver creato un ruolo collegato al servizio, non è possibile modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AppFabric

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, devi eliminare tutti i pacchetti di AppFabric app prima di poter eliminare il ruolo collegato al servizio.

Pulizia di un ruolo collegato ai servizi

Prima di utilizzare IAM; per eliminare un ruolo collegato al servizio, è necessario prima rimuovere qualsiasi risorsa utilizzata dal ruolo. I bundle di app in cui crei AppFabric vengono utilizzati dal ruolo. Per ulteriori informazioni, consulta Elimina AWS AppFabric per risorse di sicurezza.

> **Note**
>
> Se il AppFabric servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Eliminazione manuale del ruolo collegato ai servizi

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo `AWSServiceRoleForAppFabric` collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi AppFabric

AppFabric supporta l'utilizzo di ruoli collegati al servizio in tutti i paesi in Regioni AWS cui il servizio è disponibile. Per ulteriori informazioni, consulta Endpoint e quote AppFabric nella Riferimenti generali di AWS.

AWS politiche gestite per AWS AppFabric

Per aggiungere autorizzazioni a utenti, gruppi e ruoli, è più facile utilizzare le politiche AWS gestite che scrivere le politiche da soli. Creare policy gestite dal cliente IAM per fornire al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Per iniziare rapidamente, puoi utilizzare le nostre politiche AWS gestite. Queste policy coprono i casi d'uso comuni e sono disponibili nel tuo Account AWS. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

Servizi AWS mantenere e aggiornare le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi occasionalmente aggiungono altre autorizzazioni a una policy gestita da AWS per supportare nuove funzionalità. Questo tipo di aggiornamento interessa tutte le identità (utenti, gruppi e ruoli) a cui è collegata la policy. È più probabile che i servizi aggiornino una policy gestita da AWS quando viene avviata una nuova funzionalità o quando diventano disponibili nuove operazioni. I servizi non rimuovono le autorizzazioni da una policy AWS gestita, quindi gli aggiornamenti delle policy non comprometteranno le autorizzazioni esistenti.

Inoltre, AWS supporta politiche gestite per le funzioni lavorative che si estendono su più servizi. Ad esempio, la policy ReadOnlyAccess AWS gestita fornisce l'accesso in sola lettura a tutte le Servizi AWS risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per l'elenco e la descrizione delle policy di funzione dei

processi, consulta la sezione Policy gestite da AWS per funzioni di processi nella Guida per l'utente di IAM.

AWS politica gestita: AWSAppFabricReadOnlyAccess

È possibile allegare la policy `AWSAppFabricReadOnlyAccess` alle identità IAM. Questa politica concede autorizzazioni di sola lettura al servizio. AppFabric

> **Note**
>
> La `AWSAppFabricReadOnlyAccess` policy non concede l'accesso in sola lettura alle funzionalità per la produttività. AppFabric

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `appfabric`— Concede l'autorizzazione a creare un pacchetto di app, elencare pacchetti di app, ottenere l'autorizzazione di un'app, elencare le autorizzazioni delle app, ottenere un'importazione, elencare le acquisizioni, ottenere una destinazione di importazione, elencare le destinazioni di importazione ed elencare i tag delle risorse.

```
{
    "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 politica gestita: AWSAppFabricFullAccess

È possibile allegare la policy `AWSAppFabricFullAccess` alle identità IAM. Questa politica concede autorizzazioni amministrative al AppFabric servizio.

> **Important**
>
> La `AWSAppFabricFullAccess` politica non concede l'accesso alle funzionalità AppFabric per la produttività perché sono attualmente in anteprima. Per ulteriori informazioni sulla concessione dell'accesso alle funzionalità AppFabric per la produttività, consultaAppFabric per la produttività, esempi di policy IAM.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `appfabric`— Concede l'autorizzazione amministrativa completa a. AppFabric
- `kms`— Concede l'autorizzazione a elencare gli alias.
- `s3`— Concede l'autorizzazione a elencare tutti i bucket Amazon S3 e a ottenere la posizione dei bucket.
- `firehose`— Concede l'autorizzazione a elencare i flussi di consegna di Amazon Data Firehose e a descrivere i flussi di consegna.
- `iam`— Concede l'autorizzazione a creare il ruolo collegato al servizio per. `AWSServiceRoleForAppFabric` AppFabric Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per 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 politica gestita: AWSAppFabricServiceRolePolicy

Non è possibile allegare la policy `AWSAppFabricServiceRolePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente di eseguire azioni AppFabric per conto dell'utente. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per AppFabric.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `cloudwatch`— Concede l'autorizzazione AppFabric a inserire dati metrici nello spazio dei nomi Amazon CloudWatch `AWS/AppFabric`. Per ulteriori informazioni sulle AppFabric metriche disponibili in, consulta. CloudWatch Monitoraggio AWS AppFabric con Amazon CloudWatch
- `s3`— Concede l'autorizzazione AppFabric a inserire i dati acquisiti in un bucket Amazon S3 specificato dall'utente.
- `firehose`— Concede l'autorizzazione AppFabric a inserire i dati importati in un flusso di distribuzione Amazon Data Firehose da te specificato.

```
{
    "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 aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AppFabric da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivi il feed RSS nella pagina della cronologia dei documenti AppFabric .

Modifica	Descrizione	Data
AWSAppFabricReadOnlyAccess: nuova policy	AppFabric ha aggiunto una nuova politica per concedere autorizzazioni di sola lettura al servizio. AppFabric	27 giugno 2023
AWSAppFabricFullAccess: nuova policy	AppFabric ha aggiunto una nuova politica per concedere autorizzazioni amministrative al servizio. AppFabric	27 giugno 2023
AWSAppFabricServiceRolePolicy: nuova policy	AppFabric ha aggiunto una nuova politica per il ruolo collegato al `AWSServiceRoleForAppFabric` servizio.	27 giugno 2023
AppFabric ha iniziato a tenere traccia delle modifiche	AppFabric ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	27 giugno 2023

Risoluzione dei problemi di AWS AppFabric identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con un AppFabric IAM.

Argomenti

Non sono autorizzato a eseguire alcuna azione in AppFabric

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `appfabric:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 appfabric:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `appfabric:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam:PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a AppFabric.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio anziché creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AppFabric. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie AppFabric risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AppFabric supporta queste funzionalità, consulta. Come AWS AppFabric funziona con IAM
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Convalida della conformità per AWS AppFabric

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Le migliori pratiche di sicurezza per AWS AppFabric

AWS AppFabric offre diverse funzionalità di sicurezza da considerare durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida

generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni.

Monitora le applicazioni senza accesso da amministratore

Con l'autorizzazione di sola lettura AWS Identity and Access Management (IAM), chiunque può integrarsi con AppFabric Amazon QuickSight e altri strumenti di gestione delle informazioni e degli eventi di sicurezza (SIEM), come. Splunk Per monitorare la sicurezza delle applicazioni, i dati vengono inviati a un bucket Amazon Simple Storage Service (Amazon S3) o a un flusso di distribuzione Amazon Data Firehose.

Monitora gli eventi AppFabric

Puoi monitorare AppFabric utilizzando i CloudWatch parametri di Amazon. CloudWatch raccoglie dati AppFabric ogni minuto e li elabora in metriche. Puoi impostare allarmi che attivano le notifiche quando le metriche soddisfano le soglie specificate. Per ulteriori informazioni, consulta Monitoraggio AWS AppFabric con Amazon CloudWatch.

Resilienza in AWS AppFabric

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Sicurezza dell'infrastruttura in AWS AppFabric

In quanto servizio gestito, AWS AppFabric è protetto dalle procedure di sicurezza della rete AWS globale descritte nel white paper Amazon Web Services: Overview of Security Processes.

Utilizzi chiamate API AWS pubblicate per accedere AppFabric attraverso la rete. I client devono supportare TLS 1.0 o versioni successive. È consigliabile TLS 1.2 o versioni successive. I client devono, inoltre, supportare le suite di cifratura con PFS (Perfect Forward Secrecy), ad esempio

Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, per generare credenziali di sicurezza temporanee per firmare le richieste, puoi utilizzare AWS Security Token Service()AWS STS.

Analisi della configurazione e della vulnerabilità in AWS AppFabric

La configurazione e i controlli IT sono una responsabilità condivisa tra voi AWS e voi, nostri clienti. Per ulteriori informazioni, consulta il modello di responsabilità AWS condivisa.

Monitoraggio AWS AppFabric

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS AppFabric altre AWS soluzioni esistenti. AWS fornisce i seguenti strumenti di monitoraggio per osservare AppFabric, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon CloudWatch monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere i parametri e tenerne traccia, creare pannelli di controllo personalizzati e impostare allarmi per inviare una notifica o intraprendere azioni quando un parametro specificato raggiunge una determinata soglia. Ad esempio, puoi tenere CloudWatch traccia dell'utilizzo della CPU o di altri parametri delle tue EC2 istanze Amazon e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.
- Amazon CloudWatch Logs ti consente di monitorare, archiviare e accedere ai tuoi file di registro da EC2 istanze Amazon e altre fonti. AWS CloudTrail CloudWatch I log possono monitorare le informazioni nei file di registro e avvisarti quando vengono raggiunte determinate soglie. Puoi inoltre archiviare i dati del log in storage estremamente durevole. Per ulteriori informazioni, consulta la Amazon CloudWatch Logs User Guide.
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per conto tuo Account AWS e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

Monitoraggio AWS AppFabric con Amazon CloudWatch

Puoi monitorare AWS AppFabric l'utilizzo CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili e quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, per permettere l'accesso alle informazioni storiche e offrire una prospettiva migliore sulle prestazioni del servizio o dell'applicazione web. È anche possibile impostare allarmi che controllano determinate soglie e inviare notifiche o intraprendere azioni quando queste soglie vengono raggiunte. Per ulteriori informazioni, consulta la Amazon CloudWatch User Guide.

Il AppFabric servizio riporta le seguenti metriche nel `AWS/AppFabric` namespace.

Parametro	Descrizione
AppFabric Stato di autorizzazione dell'app	Lo stato dell'autorizzazione dell'app (1per le app connesse, 0 per qualsiasi altra).
AppFabric Latenza di consegna dei dati	Il tempo impiegato (in secondi) AppFabric per raccogliere i log di controllo dall'applicazione SaaS e consegnarli alla destinazione configura ta (Amazon S3 o Amazon Data Firehose).
Stato della destinazione di importazione	Lo stato della destinazione di ingestione (1per attiva; 0 per qualsiasi altra).
Ritardo complessivo dei dati	La differenza di tempo (in secondi) tra il momento in cui si sono verificati gli eventi sull'applicazione SaaS e il momento in cui i log di controllo corrispondenti sono stati consegnat i alla destinazione configurata (Amazon S3 o Amazon Data Firehose) entro. AppFabric
Volume di dati ingeriti	La dimensione dei dati forniti ad Amazon Simple Storage Service (Amazon S3) o Amazon Data Firehose.

La seguente dimensione è supportata per AppFabric le metriche.

Dimensione	Descrizione
Arn di destinazione di importazione	L'Amazon Resource Name (ARN) della destinazione di ingestione.

Registrazione delle chiamate AWS AppFabric API utilizzando AWS CloudTrail

AWS AppFabric è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un membro Servizio AWS . AppFabric CloudTrail

acquisisce tutte le chiamate API AppFabric come eventi. Le chiamate acquisite includono chiamate dalla AppFabric console e chiamate di codice alle operazioni AppFabric API. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AppFabric Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviata AppFabric, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni in merito CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

AppFabric informazioni in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in AppFabric, tale attività viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella Cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti in Account AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi nella Guida AWS CloudTrail per l'utente.

Per una registrazione continua degli eventi del tuo sito Account AWS, inclusi gli eventi di AppFabric, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurarne altri Servizi AWS per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di AWS CloudTrail :

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte AppFabric le azioni vengono registrate CloudTrail e documentate nell'AWS AppFabric API Reference. Ad esempio, le chiamate a `CreateAppBundle`, `UpdateAppBundle`, e `GetAppBundle` le azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

Per ulteriori informazioni, consulta CloudTrail userIdentity elemento nella Guida per l'AWS CloudTrail utente.

Comprendere AppFabric le voci dei file di registro

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`CreateAppBundle`azione.


```
{
    "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"
    }
}
```

Quote per AppFabric

Hai Account AWS delle quote predefinite, precedentemente denominate limiti, per ciascuno di essi. Servizio AWS Salvo diversa indicazione, ogni quota si applica a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Per visualizzare le quote per AppFabric, apri la console Service Quotas. Nel riquadro di navigazione, scegliere Servizi AWS , quindi selezionare AppFabric.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida dell'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il modulo di incremento dei limiti.

Le quote correlate presenti nella tua Account AWS sono mostrate nella tabella seguente. AppFabric

Nome	Predefinita	Adattabile	Descrizione
Pacchetti di applicazioni	Ogni regione supportata: 1	No	Il numero massimo di pacchetti di applicazioni che è possibile creare in un account nella regione corrente AWS .
Autorizzazioni dell'applicazione	Ogni Regione supportata: 50	No	Il numero massimo di autorizzazioni dell'applicazione che è possibile creare in un account nella regione corrente AWS .
Ingestioni	Ogni Regione supportata: 50	No	Il numero massimo di acquisizioni che è possibile creare in un account nella regione corrente. AWS
Destinazioni di importazione	Ogni Regione supportata: 5	No	Il numero massimo di destinazioni di importazi

Nome	Predefinita	Adatta e	Descrizione
			one che è possibile creare per ogni ingestion e in un account nella regione corrente. AWS
AppClient	Ogni regione supportata: 1	No	Il numero massimo di file AppClients che puoi creare in un account nella regione corrente. AWS La funzionalità AWS AppFabric per la produttività è disponibile in anteprima ed è soggetta a modifiche.

Cronologia dei documenti per la Guida AppFabric amministrativa

La tabella seguente descrive le versioni della documentazione per AWS AppFabric.

Modifica	Descrizione	Data
Nuova applicazione supportata	Aggiunto JumpCloud come applicazione supportata. Per ulteriori informazioni, consulta Applicazioni supportate in AWS AppFabric.	5 giugno 2024
Nuove applicazioni e strumenti di sicurezza supportati	Aggiunto Azure Monitor e Google Analytics come applicazioni supportate. Per ulteriori informazioni, consulta Applicazioni supportate in AWS AppFabric. Aggiunto Singularity Cloud come strumento di sicurezza supportato. Per ulteriori informazioni, consulta Strumenti di sicurezza compatibili.	30 aprile 2024
Nuova applicazione supportata	Aggiunto SentinelOne come applicazione supportata. Per ulteriori informazioni, consulta Applicazioni supportate in AWS AppFabric.	25 aprile 2024
Nuova applicazione supportata	Aggiunto 1Password come applicazione supportata. Per ulteriori informazioni, consulta	23 aprile 2024

	Applicazioni supportate in AWS AppFabric.	
Nuovo strumento di sicurezza supportato	Aggiunto Dynatrace come strumento di sicurezza compatibile. Per ulteriori informazioni, consulta Strumenti di sicurezza compatibili.	26 marzo 2024
Nuova metrica	È stata aggiunta la metrica dello stato di autorizzazione dell' AppFabric app. Per ulteriori informazioni, consulta Monitoraggio AWS AppFabric con Amazon CloudWatch Logs.	8 marzo 2024
Nuova applicazione supportata	Aggiunto IBM Security® Verify come applicazione supportat a. Per ulteriori informazi oni, consulta Applicazioni supportate in AWS AppFabric.	6 marzo 2024
Nuova applicazione supportata	Aggiunto Box come applicazi one supportata. Per ulteriori informazioni, consulta Applicazioni supportate in AWS AppFabric.	28 febbraio 2024

Nuove applicazioni e metriche supportate	Aggiunto Cisco Duo, Salesforcee Terraform Cloud come applicazioni supportate. Per ulteriori informazioni su di esse, consulta Applicazioni supportate in AWS AppFabric. Sono state aggiunte le metriche AppFabric Data Delivery Latency e Overall Data Delay. Per ulteriori informazioni, consulta Monitoraggio AWS AppFabric con Amazon CloudWatch Logs.	1 febbraio 2024
Aggiunto Atlassian Confluence, Genesys Cloud, HubSpot, OneLogin by One Identity, PagerDutye Ping Identity come applicazioni supportate e Barracuda XDR come strumento di sicurezza compatibile	Per ulteriori informazioni sulle nuove applicazioni supportate, consulta Applicazioni supportate in AWS AppFabric e Strumenti di sicurezza compatibili.	15 dicembre 2023
Aggiunto Atlassian Confluence, Genesys Cloud, HubSpot, OneLogin by One Identity, PagerDutye Ping Identity come applicazioni supportate e Barracuda XDR come strumento di sicurezza compatibile	Per ulteriori informazioni sulle nuove applicazioni supportate, consulta Applicazioni supportate in AWS AppFabric e Strumenti di sicurezza compatibili.	15 dicembre 2023
È stata aggiunta la documentazione di anteprima AWS AppFabric per la produttività	Per ulteriori informazioni sulla AppFabric produttività, consulta What is AWS AppFabric for productivity?	27 novembre 2023

Aggiunto GitHub e ServiceNow come applicazioni supportate	Per ulteriori informazioni sulle nuove applicazioni supportate, vedere Applicazioni supportate.	31 ottobre 2023
Ha iniziato a tenere traccia delle politiche AWS gestite per AWS AppFabric	Per ulteriori informazioni sulle politiche AWS gestite per AppFabric, consulta le politiche AWS gestite per AWS AppFabric.	27 giugno 2023
Versione iniziale	Versione iniziale della Guida all' AWS AppFabric amministrazione.	27 giugno 2023

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.