Guida all'amministrazione della console

AWS re:Post privato

AWS re:Post privato: Guida all'amministrazione della console

Table of Contents

Cos'è AWS Re:Post Private? 1
Accedi a re:Post Private 1
Prezzi 2
Come iniziare 2
Prerequisiti 3
Sali a bordo di re:POST Private 4
Sicurezza 5
Protezione dei dati 5
Protezione dei dati con la crittografia 7
Crittografia in transito 7
Gestione delle chiavi 7
Come funziona Re:post Private con IAM 7
Politiche basate sull'identità privata di re:POST 7
Politiche basate sulle risorse private di re:POST 9
Autorizzazione basata su tag 9
Ruoli IAM privati re:post 9
Ruoli collegati ai servizi 10
Ruoli di servizio 10
Uso di ruoli collegati ai servizi 10
Esempi di policy basate su identità 14
Policy inline 16
AWS politiche gestite 19
Risoluzione dei problemi 21
Convalida della conformità 23
Resilienza 25
Sicurezza dell'infrastruttura 25
Quote 26
Service Quotas 26
Limiti di limitazione delle API 26
Crea, configura e personalizza il tuo Re:post privato 28
Crea un nuovo Re:post privato 28
Gestione dell'accesso alla creazione e alla gestione dei AWS Support casi in Re:Post Private ... 30
Utilizza una policy AWS gestita o crea una policy gestita dal cliente 31
Policy IAM di esempio 32

Creazione di un ruolo IAM 33
Risoluzione dei problemi 34
Configura e gestisci l'accesso degli utenti 35
Personalizza il tuo Re:post privato 35
Invita gli utenti al tuo re:post privato 36
Gestisci il tuo Re:post privato 37
Aggiungi utenti e gruppi 37
Aggiunta di utenti a un gruppo 38
Invita utenti e gruppi 38
Promuovi un utente ad amministratore 39
Rimuovi utenti e gruppi 39
Aggiungi o rimuovi un dipendente AWS 40
Eliminare un Re:post privato 40
Monitoraggio di Re:Post Private 42
Monitoraggio con CloudWatch 42
Registrazione delle chiamate API private re:POST utilizzando AWS CloudTrail 43
Re:Pubblica informazioni private in CloudTrail 43
Informazioni sulle voci dei file di registro privati di re:POST 45
Risoluzione dei problemi 51
Non riesco a configurare il mio re:Post privato in una regione specifica AWS 51
Non riesco a configurare il re:post privato nel mio account 51
Non puoi gestire utenti o gruppi in un re:POST privato 51
Cronologia dei documenti 52
..... liii

Cos'è AWS Re:Post Private?

AWS re:Post Private è una versione privata di AWS re:Post per aziende con piani Enterprise Support o Enterprise On-Ramp Support. Fornisce accesso a conoscenze ed esperti per accelerare l'adozione del cloud e aumentare la produttività degli sviluppatori. Con Re:POST privato specifico per l'organizzazione, puoi creare una community di sviluppatori specifica per l'organizzazione che promuove l'efficienza su larga scala e fornisce l'accesso a preziose risorse di conoscenza. Inoltre, re:Post Private centralizza contenuti AWS tecnici affidabili e offre forum di discussione privati per migliorare il modo in cui i team collaborano internamente e con AWS per rimuovere gli ostacoli tecnici, accelerare l'innovazione e scalare in modo più efficiente nel cloud.

Per ulteriori informazioni, consulta AWS re:Post Private.

Accedi a re:Post Private

Gli amministratori utilizzano la console AWS re:Post Private per creare un Re:post privato specifico per l'organizzazione. Quando gli amministratori creano un Re:post privato, possono assegnare un nome al proprio re:POST privato e definire un sottodominio sotto. `*.private.repost.aws` Gli amministratori di re:POST privato di un'organizzazione possono configurare l'accesso degli utenti utilizzando AWS IAM Identity Center e specificare una delle seguenti fonti di identità per l'autenticazione: directory Identity Center, Active Directory o un provider di identità esterno. Dopo aver configurato gli utenti, gli amministratori della console possono assegnare un ruolo di amministratore re:POST Private a uno o più utenti. Gli amministratori di re:POST Private possono personalizzare la propria applicazione privata re:POST in base alle esigenze di branding e conoscenza dell'organizzazione. I membri del team addetto all'AWSaccount, come i Technical Account Manager, che conoscono l'architettura e i carichi di lavoro dell'organizzazione vengono automaticamente aggiunti al Re:POST privato dell'organizzazione per consentire la collaborazione.

Gli amministratori dell'applicazione re:POST Private possono personalizzare il marchio, aggiungere tag per classificare i contenuti e selezionare argomenti di interesse per i propri sviluppatori per inserire automaticamente contenuti tecnici e di formazione. Possono anche invitare gli utenti a partecipare al loro re:POST privato per una maggiore collaborazione. Per ulteriori informazioni, consulta AWS re:Post Private Administration Guide.

Gli utenti non amministrativi utilizzano l'applicazione Re:POST Private per accedere utilizzando credenziali configurate dal loro amministratore. Dopo aver effettuato l'accesso a un Re:post privato, gli utenti possono sfogliare o cercare contenuti esistenti, inclusi contenuti formativi e tecnici

personalizzati relativi agli argomenti di loro interesse. Gli utenti possono anche cercare contenuti tecnici AWS pubblici direttamente dal loro Re:post privato e creare thread privati per discussioni interne su contenuti pubblici. AWS Gli utenti possono risolvere in modo collaborativo problemi AWS tecnici e ottenere assistenza tecnica da altri utenti del re:Post privato ponendo una domanda, fornendo una risposta o pubblicando un articolo. Gli utenti possono anche convertire un thread di discussione in un caso. AWS Support Gli utenti possono scegliere di aggiungere le risposte AWS Support al Re:post privato. Per ulteriori informazioni, consulta AWS re:Post Private User Guide.

Prezzi

Solo i clienti con piani di supporto Enterprise Support (ES) ed Enterprise On-Ramp (EOP) possono abbonarsi al servizio Re:POST Private. Puoi scegliere tra i due livelli di prezzo disponibili: livello gratuito e livello standard. Il piano gratuito ti offre la possibilità di esplorare e provare appieno le funzionalità del livello Standard per sei mesi prima di poter passare senza problemi a un livello a pagamento. Se utilizzi il livello Standard, puoi pagare un abbonamento mensile per utente per utilizzare Re:post Private. Per ulteriori informazioni, consulta la sezione Prezzi di .

Come iniziare

Per iniziare a usare re:Post Private, vedi. Prerequisiti

Prerequisiti

È necessario soddisfare i seguenti prerequisiti prima di poter creare un nuovo re:POST privato o gestire un re:post privato esistente in AWS re:POST Private:

- È necessario sottoscrivere un piano di supporto Enterprise o Enterprise On-Ramp.
- Devi abilitarlo AWS IAM Identity Center nella stessa regione in cui desideri configurare il tuo re:POST privato.
- Devi creare un AWS Identity and Access Management ruolo con le autorizzazioni necessarie per creare, gestire e risolvere i AWS Support casi al posto tuo. Il servizio Re:Post Private utilizza questo ruolo per effettuare chiamate API a. AWS Support Per ulteriori informazioni, consulta Gestione dell'accesso alla creazione e alla gestione dei AWS Support casi in Re:Post Private.

Effettua l'onboarding per re:POST Private tramite IAM Identity Center

Re:post Private si integra con AWS IAM Identity Center per fornire una federazione delle identità alla tua forza lavoro. Tramite IAM Identity Center, gli utenti vengono reindirizzati all'elenco aziendale esistente per accedere con le credenziali esistenti. Quindi, accedono senza problemi al loro re:post privato. In questo modo si assicura che le impostazioni di sicurezza, come le politiche sulle password e l'autenticazione a due fattori, vengano applicate. L'utilizzo di IAM Identity Center non ha alcun impatto sulla configurazione IAM esistente.

Se non disponi di una directory utenti esistente o preferisci non effettuare la federazione, IAM Identity Center offre una directory utenti integrata che puoi utilizzare per creare utenti e gruppi per re:POST Private. re:Post Private non supporta l'uso di utenti e ruoli IAM per assegnare autorizzazioni all'interno di un RE:POST privato. Le autorizzazioni utente all'interno di un Re:post privato sono configurate da un amministratore sulla sua applicazione privata Re:post.

Per ulteriori informazioni su IAM Identity Center, consulta What is AWS IAM Identity Center (successore di AWS Single Sign-On). Per ulteriori informazioni su come iniziare a usare IAM Identity Center, consulta Getting started. Per utilizzare IAM Identity Center, devi aver AWS Organizations attivato anche l'account.

> **Important**
>
> Re:post Private supporta solo le istanze organizzative di IAM Identity Center.

Sicurezza in Re:post Private

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 gestisce AWS i servizi in 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 che si applicano a AWS re:POST Private, consulta AWS Services in Scope by Compliance Program AWS Services in Scope Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda e le leggi e le normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Re:POST Private. I seguenti argomenti mostrano come configurare re:Post Private per soddisfare i tuoi obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse di re:POST Private.

Argomenti

- Protezione dei dati in AWS Re:Post Private
- Come funziona Re:post Private con IAM
- Convalida della conformità per AWS re:Post Private
- Resilienza in AWS Re:Post Private
- Sicurezza dell'infrastruttura in AWS Re:Post Private

Protezione dei dati in AWS Re:Post Private

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS Re:post Private. 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 AWS servizi 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.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS servizi.
- 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 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente 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 con Re:Post Private o altro AWS servizi utilizzando la console, l'API o gli SDK. AWS CLI AWS 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.

Protezione dei dati con la crittografia

Crittografia a riposo

re:POST Private utilizza bucket Amazon Simple Storage Service, database Amazon DynamoDB, database Amazon Neptune OpenSearch e domini Amazon Service crittografati a riposo utilizzando chiavi gestite da Amazon o chiavi gestite dal cliente.

Crittografia in transito

re:Post Private utilizza il protocollo HTTPS per comunicare con l'applicazione client. Utilizza HTTPS e AWS firme per comunicare con altri servizi per conto dell'applicazione.

Gestione delle chiavi

Re:post Private è integrato AWS Key Management Service e supporta le chiavi. AWS KMS Puoi personalizzare le impostazioni di crittografia dei dati per il tuo re:post privato al momento della creazione. A tale scopo, puoi scegliere una AWS KMS chiave esistente o crearne una nuova AWS KMS.

Come funziona Re:post Private con IAM

Prima di utilizzare IAM per gestire l'accesso ad AWS re:Post Private, devi capire quali funzionalità IAM sono disponibili per l'uso con RE:post Private. Per avere una visione di alto livello di come re:post Private e altri AWS servizi funzionano con IAM, consulta i AWS servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità privata di re:POST

Con le policy basate sull'identità IAM, puoi specificare azioni consentite o negate. re:Post Private supporta azioni specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta la Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Azioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni 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 azioni 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.

Le azioni politiche in Re:post Private utilizzano il seguente prefisso prima dell'azione:. `repostspace:` Ad esempio, per concedere a qualcuno l'autorizzazione a eseguire l'operazione dell'`CreateSpace`API re:Post Private, includi l'azione nella `repostspace:CreateSpace` sua politica. Le dichiarazioni politiche devono includere un `NotAction` elemento `Action` or. re:Post Private definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più azioni in una sola istruzione, separa ciascuna di esse con una virgola come mostrato di seguito:

```
"Action": [
      "repostspace:CreateSpace",
      "repostspace:DeleteSpace"
```

È possibile specificare più azioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola `Describe`, includi la seguente azione:

```
"Action": "repostspace:Describe*"
```

Per visualizzare un elenco delle azioni private di re:POST, consulta Actions defined by re:POST Private nella IAM User Guide.

Risorse

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, 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).

Puoi eseguire questa operazione per azioni 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": "*"
```

Chiavi di condizione

Re:Post Private non fornisce chiavi di condizione specifiche del servizio, ma supporta l'utilizzo di chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Esempi

Per visualizzare esempi di politiche basate sull'identità privata di re:POST, consulta. Esempi di policy basate sull'identità privata di AWS re:Post

Politiche basate sulle risorse private di re:POST

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su 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 azioni 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.

Re:post Private non supporta le politiche basate sulle risorse.

Autorizzazione basata su tag

Re:Post Private supporta l'etichettatura delle risorse o il controllo dell'accesso in base ai tag. Per ulteriori informazioni, consulta Controllare l'accesso alle risorse AWS tramite tag.

Ruoli IAM privati re:post

Un ruolo IAM è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con re:Post Private

Consigliamo vivamente di utilizzare credenziali temporanee per accedere con la federazione, assumere un ruolo IAM o assumere un ruolo tra account. È possibile ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come o. AssumeRoleGetFederationToken

Re:post Private supporta l'utilizzo di credenziali temporanee.

Ruoli collegati ai servizi

I ruoli collegati ai AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione al posto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

Ruoli di servizio

Questa funzionalità consente a un servizio di assumere un ruolo di servizio al posto dell'utente. Questo ruolo consente al servizio di accedere alle risorse di altri servizi per completare un'azione al posto tuo. Per ulteriori informazioni, consulta Creazione di un ruolo per delegare le autorizzazioni a un servizio AWS. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore IAM può modificare le autorizzazioni per questo ruolo. Tuttavia, questo potrebbe pregiudicare la funzionalità del servizio.

Utilizzo di ruoli collegati ai servizi per Re:POST Private

AWS re:Post Private utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a re:POST Private. I ruoli collegati ai servizi sono predefiniti da Re:POST Private e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato ai servizi semplifica la configurazione di re:POST Private perché non è necessario aggiungere manualmente le autorizzazioni necessarie. re:POST Private definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo re:POST Private può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consultare Servizi AWS che funzionano con IAM e cercare i servizi che riportano Yes (Sì) nella colonna Service-linked roles

(Ruoli collegati ai servizi). Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Autorizzazioni relative ai ruoli collegati al servizio per Re:post Private

re:Post Private utilizza il ruolo collegato al servizio denominato AWSServiceRoleForrePostPrivate. re:Post Private utilizza questo ruolo collegato al servizio su cui pubblicare i dati. CloudWatch

Il ruolo AWSServiceRoleForrePostPrivate collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `repostspace.amazonaws.com`

La politica di autorizzazione dei ruoli denominata `AWSrePostPrivateCloudWatchAccess` consente a Re:Post Private di completare le seguenti azioni sulle risorse specificate:

- Azione su: `cloudwatch PutMetricData`

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.

Per ulteriori informazioni, consulta AWSrePostPrivateCloudWatchAccess.

Creazione di un ruolo collegato al servizio per Re:Post Private

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei il tuo primo re:POST privato nell' AWS Management Console, the AWS CLI o nell' AWS API, Re:post Private crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato al servizio può apparire nell'account, se è stata completata un'operazione in un altro servizio che utilizza le caratteristiche supportate da questo ruolo. Inoltre, se utilizzavi il servizio re:POST Private prima del 1° dicembre 2023, quando ha iniziato a supportare i ruoli collegati al servizio, Re:post Private ha creato il ruolo nel tuo account. `AWSServiceRoleForrePostPrivate` Per ulteriori informazioni, vedi A new role appeared in my. Account AWS

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei il tuo primo re:post privato, re:post Private crea nuovamente il ruolo collegato al servizio per te.

Nella AWS CLI o nell' AWS API, crea un ruolo collegato al servizio con il nome del servizio. `repostspace.amazonaws.com` Per ulteriori informazioni, consulta Creazione di un ruolo collegato ai servizi nella Guida per l'utente di IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Modifica di un ruolo collegato al servizio per Re:Post Private

re:Post Private non ti consente di modificare il ruolo collegato al servizio. `AWSServiceRoleForrePostPrivate` Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi 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 al servizio per Re:Post Private

Non è necessario eliminare manualmente il ruolo `AWSServiceRoleForrePostPrivate`. Quando elimini il tuo Re:post privato nell' AWS Management Console, the AWS CLI o nell' AWS API, re:post Private elimina automaticamente il ruolo collegato al servizio.

Puoi anche utilizzare la console IAM, l'o l' AWS API per eliminare manualmente AWS CLI il ruolo collegato al servizio.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, l'o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForrePostPrivate 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 di Re:POST Private

re:Post Private supporta l'utilizzo di ruoli collegati ai servizi nelle regioni in cui il servizio è disponibile. AWS

Nome Regione	Identità della regione	Support in re:Post Private
US East (N. Virginia)	us-east-1	Sì

Nome Regione	Identità della regione	Support in re:Post Private
Stati Uniti orientali (Ohio)	us-east-2	No
US West (N. California)	us-west-1	No
US West (Oregon)	us-west-2	Sì
Africa (Cape Town)	af-south-1	No
Asia Pacifico (Hong Kong)	ap-east-1	No
Asia Pacifico (Giacarta)	ap-southeast-3	No
Asia Pacific (Mumbai)	ap-south-1	No
Asia Pacifico (Osaka-Locale)	ap-northeast-3	No
Asia Pacifico (Seul)	ap-northeast-2	No
Asia Pacific (Singapore)	ap-southeast-1	Sì
Asia Pacifico (Sydney)	ap-southeast-2	Sì
Asia Pacifico (Tokyo)	ap-northeast-1	No
Canada (Central)	ca-central-1	Sì
Europe (Frankfurt)	eu-central-1	Sì
Europa (Irlanda)	eu-west-1	Sì
Europe (London)	eu-west-2	No
Europa (Milano)	eu-south-1	No
Europe (Paris)	eu-west-3	No
Europa (Stoccolma)	eu-north-1	No
Medio Oriente (Bahrein)	me-south-1	No

Nome Regione	Identità della regione	Support in re:Post Private
Medio Oriente (Emirati Arabi Uniti)	me-central-1	No
Sud America (São Paulo)	sa-east-1	No

Esempi di policy basate sull'identità privata di AWS re:Post

> **Note**
>
> Per una maggiore sicurezza, crea utenti federati anziché utenti IAM quando possibile.

Per impostazione predefinita, AWS Identity and Access Management gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse AWS re:POST Private. Inoltre, non possono eseguire attività utilizzando l'API AWS Management Console AWS CLI, o AWS . Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi collegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente di IAM.

Argomenti

- Best practice per le policy
- 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 le risorse Re:post Private 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. Puoi 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 puoi 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 AWS servizio, 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 IAM Access Analyzer 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 Configurazione dell'accesso alle API protetto 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.

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'API o. AWS CLI 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": "*"
        }
    ]
}
```

Policy inline

Le politiche in linea sono politiche create e gestite dall'utente. È possibile incorporare le politiche in linea direttamente in un utente, gruppo o ruolo. I seguenti esempi di policy mostrano come assegnare le autorizzazioni per eseguire azioni AWS re:Post Private. Per informazioni generali sulle policy in linea, consulta Managing IAM policies nella AWS IAM User Guide. Puoi utilizzare AWS Management Console, AWS Command Line Interface (AWS CLI) o l' AWS Identity and Access Management API per creare e incorporare policy in linea.

Argomenti

- Accesso in sola lettura a Re:post Private
- Accesso completo a Re:Post Private

Accesso in sola lettura a Re:post Private

La seguente policy concede l'accesso in lettura a un utente per IAM Identity Center e la console privata re:POST. Questa policy consente all'utente di eseguire azioni Re:Post Private in sola lettura.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",

                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetSSOStatus",
                "sso:GetManagedApplicationInstance",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:ListProfileAssociations",

                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",

                "repostspace:GetSpace",
                "repostspace:ListSpaces",
                "repostspace:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Accesso completo a Re:Post Private

La seguente policy concede l'accesso completo a un utente per IAM Identity Center e la console re:POST Private. Questa policy consente all'utente di eseguire tutte le azioni di re:Post Private.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",

                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetSSOStatus",
                "sso:GetManagedApplicationInstance",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:ListProfileAssociations",

                "sso:CreateManagedApplicationInstance",
                "sso:DeleteManagedApplicationInstance",
                "sso:AssociateProfile",
                "sso:DisassociateProfile",

                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
                "sso-directory:SearchGroups",

                "kms:ListAliases",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:RetireGrant",

                "repostspace:*"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

AWS policy gestite per AWS Re:Post Private

L'utilizzo di policy AWS gestite semplifica l'aggiunta di autorizzazioni a utenti, gruppi e ruoli rispetto alla stesura delle policy da soli. Creare policy gestite dal cliente IAM per fornire al tuo team solo le autorizzazioni di cui ha bisogno richiede tempo e competenza. Utilizza le politiche AWS gestite per iniziare rapidamente. Queste politiche coprono casi d'uso comuni e sono disponibili nel tuo AWS account. Per ulteriori informazioni sulle policy AWS gestite, consulta le policy AWS gestite nella IAM User Guide.

AWS i servizi mantengono e aggiornano le politiche AWS gestite. Non è possibile modificare le autorizzazioni nelle politiche AWS gestite. I servizi potrebbero occasionalmente aggiungere autorizzazioni aggiuntive a una policy AWS gestita 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 politica AWS gestita quando viene lanciata 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 compromettono 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 tutti i AWS servizi e le risorse. Quando un servizio lancia una nuova funzionalità, AWS aggiunge autorizzazioni di sola lettura per nuove operazioni e risorse. Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

Argomenti

- AWS politica gestita: AWSRepostSpaceSupportOperationsPolicy
- AWS politica gestita: AWSrePostPrivateCloudWatchAccess
- AWS re:Post Aggiornamenti privati alle AWS policy gestite

AWS politica gestita: AWSRepostSpaceSupportOperationsPolicy

Questa policy consente al servizio AWS re:Post Private di creare, gestire e risolvere AWS Support casi creati tramite l'applicazione web re:POST Private.

```
{
```

```
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
   "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS politica gestita: AWSrePostPrivateCloudWatchAccess

Questa politica consente al servizio Re:Post Private di pubblicare dati su. CloudWatch

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CloudWatchPublishMetrics",
   "Effect": "Allow",
   "Action": [
    "cloudwatch:PutMetricData"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "cloudwatch:namespace": [
      "AWS/rePostPrivate",
      "AWS/Usage"
     ]
    }
   }
  }
 ]
```

```
}
```

AWS re:Post Aggiornamenti privati alle AWS policy gestite

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per Re:Post Private da quando questo servizio ha iniziato a tracciare queste modifiche. Per gli avvisi automatici sulle modifiche apportate alla pagina, iscriviti al feed RSS alla pagina Cronologia dei documenti.

La tabella seguente descrive importanti aggiornamenti alle politiche gestite di re:POST Private dal 26 novembre 2023.

Modifica	Descrizione	Data
Nuova politica - AWSrePost PrivateCloudWatchAccess	Nuova politica gestita per la pubblicazione dei dati su CloudWatch	26 novembre 2023
Nuova politica - AWSRepost SpaceSupportOperationsPolicy	Nuova policy gestita per la funzionalità AWS Support in AWS re:Post Private	26 novembre 2023
Re:Post Private ha iniziato a tracciare le modifiche	re:Post Private ha iniziato a tenere traccia delle modifiche per le sue politiche gestite AWS	26 novembre 2023

Risoluzione dei problemi relativi all'identità e all'accesso privati di AWS re:POST

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con re:Post Private e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Re:Post Private
- Non sono autorizzato a eseguire iam: PassRole

- Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse re:POST Private

Non sono autorizzato a eseguire un'azione in Re:Post Private

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 `repostPrivate:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 repostPrivate: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 `repostPrivate:`*`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 messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di assegnare un ruolo a Re:post Private.

Alcuni AWS servizi consentono di trasferire un ruolo esistente a quel servizio invece di 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.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in re:Post Private. Tuttavia, l'azione 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 risorse re:POST Private

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 servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se re:Post Private supporta queste funzionalità, consulta. Come funziona Re:post Private 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 re:Post Private

Per sapere se un AWS servizio programma rientra nell'ambito di specifici programmi di conformità, consulta AWS servizi la sezione Scope by Compliance Program AWS servizi 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 AWS servizi 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:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non AWS servizi tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti 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 AWS servizi 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)).
- Evaluating Resources with Rules nella AWS Config Developer Guide: 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 AWS servizio 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: AWS servizio 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 AWS servizio consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in AWS Re:Post Private

L'infrastruttura AWS globale è costruita attorno a zone di disponibilità. Regioni AWS 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 Re:Post Private

In quanto servizio gestito, AWS re:Post Private è protetto dalle procedure di sicurezza di rete AWS globali descritte nel white paper Amazon Web Services: Overview of Security Processes.

Utilizzi chiamate API AWS pubblicate per accedere a Re:Post Private attraverso la rete. I client devono supportare Transport Layer Security (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 AWS Identity and Access Management principale. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Quote private Re:post

AWS re:Post Private fornisce Re:Post privati che puoi utilizzare nel tuo account in una determinata regione. AWS Quando ti registri a Re:post Private, AWS imposta quote predefinite (precedentemente denominate limiti) sul numero di Re:post privati che puoi creare e sulle dimensioni dei re:posts privati.

Service Quotas

Di seguito sono riportate le quote predefinite per Re:post Private per il tuo account. AWS È possibile utilizzare la console Service Quotas per visualizzare la quota predefinita. Nessuna di queste quote è regolabile. Non puoi richiedere un aumento della quota.

Risorsa	Predefinito	Descrizione	Adattabile
Numero di Re:post privati	3	Il numero massimo di Re:posts privati in questo account nella regione corrente.	No
Dimensione privata gratuita di Re:post	10	La dimensione massima (in GB) di un Re:post privato gratuito.	No
Dimensione Re:post privata standard	100	La dimensione massima (in GB) di un Re:post privato standard.	No

Limiti di limitazione delle API

I seguenti limiti di limitazione si applicano per account e per regione in Re:post Private. Queste quote non possono essere aumentate.

Azioni	Frequenza di ricarica del token	Frequenza delle richieste	
CreateSpace	1	1	
ListSpaces	10	10	
GetSpace	10	10	
UpdateSpace	10	10	
DeleteSpace	1	1	
RegisterAdmin	10	100	
DeRegisterAdmin	10	100	
SendInvites	1	1	
TagResource	10	10	
UnTagResource	10	10	
ListTagsForResource	10	10	

Crea, configura e personalizza il tuo re:post privato

Argomenti

- Crea un nuovo re:post privato
- Gestione dell'accesso alla creazione e alla gestione dei AWS Support casi in Re:Post Private
- Configura e gestisci l'accesso degli utenti utilizzando AWS IAM Identity Center
- Personalizza il tuo re:post privato
- Invita gli utenti al tuo re:POST privato

Crea un nuovo re:post privato

Per creare un nuovo re:post privato, segui questi passaggi:

1. Apri la console Re:post Private all'indirizzo https://console.aws.amazon.com/repost-private/.
2. Nella home page della console, scegli Crea re:post privato.
3. Se non hai ancora configurato IAM Identity Center per il tuo account, scegli Open Identity Center. Segui le istruzioni in Guida introduttiva nella Guida per l'utente di AWS IAM Identity Center.
4. Nella pagina Create private Re:post, per i prezzi, seleziona il livello gratuito o il livello Standard in base al tuo caso d'uso. Se hai già utilizzato il piano gratuito per il tuo account, l'opzione del livello gratuito non è disponibile.
5. In Dettagli, procedi come segue:

   In Nome, inserisci un nome univoco per il tuo Re:post privato.

   (Facoltativo) In Descrizione, inserisci una breve descrizione per il tuo re:post privato.

   Per Sottodominio personalizzato, inserisci un nome personalizzato per il sottodominio.
6. (Facoltativo) Per personalizzare le impostazioni di crittografia dei dati, in Crittografia dei dati, seleziona Personalizza le impostazioni di crittografia. Quindi, esegui una delle seguenti azioni:

   Per Scegli una chiave AWS KMS, seleziona una AWS Key Management Service chiave o un Amazon Resource Name (ARN).

   oppure

Scegli Crea una chiave AWS KMS. Quindi, crea la AWS KMS chiave.

7. (Facoltativo) In Accesso al servizio per l'integrazione del caso Support, seleziona Abilita l'accesso al servizio per questo Re:POST.

> **Note**
>
> Puoi attivare questa opzione anche dopo aver creato il Re:post privato.

Per Seleziona un ruolo IAM esistente di seguito o crea un nuovo ruolo nella console IAM, utilizza la barra di ricerca per trovare il tuo ruolo IAM esistente.

oppure

Scegli di creare un nuovo ruolo nella console IAM.

Se scegli di creare un nuovo ruolo, segui le istruzioni riportate inCreazione di un ruolo IAM.

Se scegli di utilizzare un ruolo di servizio esistente, nella barra di ricerca inserisci l'ARN del ruolo che desideri utilizzare. Scegli il ruolo dall'elenco a discesa.

Per ulteriori informazioni, consulta Gestione dell'accesso alla creazione e alla gestione dei AWS Support casi in Re:Post Private.

8. (Facoltativo) In Tag, scegli Aggiungi nuovo tag. Quindi inserisci le seguenti informazioni:

   Per Chiave, inserisci la tua chiave tag personalizzata.

   In Valore, inserisci il valore del tag personalizzato.

   Per aggiungere altri tag, scegli Aggiungi nuovo tag.

9. Scegli Crea questo re:POST.

Una pagina di conferma ti informerà che il tuo Re:post privato è in fase di creazione. Puoi visualizzare lo stato del re:post privato nel campo Stato. Quando viene creato il tuo re:post privato, nel campo Stato viene visualizzato Creazione in corso.

La creazione del Re:post privato richiede circa 30 minuti. Quando il tuo Re:post privato è pronto, il campo Stato viene visualizzato Online. Puoi utilizzare il sottodominio generato da AWS per il tuo

re:POST privato elencato nella scheda Impostazioni per accedere al tuo re:POST privato. Puoi visualizzare il sottodominio personalizzato per il tuo re:post privato nella scheda Impostazioni dopo aver completato la revisione.

Gestione dell'accesso alla creazione e alla gestione dei AWS Support casi in Re:Post Private

È necessario creare un ruolo AWS Identity and Access Management (IAM) per gestire l'accesso alla creazione e alla gestione dei AWS Support casi da AWS re:POST Private. Questo ruolo esegue per te le seguenti AWS Support azioni:

- CreateCase
- AddCommunicationToCase
- ResolveCase

Dopo aver creato il ruolo IAM, allega una policy IAM a questo ruolo in modo che il ruolo disponga delle autorizzazioni necessarie per completare queste azioni. Scegli questo ruolo quando crei il tuo re:POST privato nella console re:POST Private.

Gli utenti del tuo re:post privato hanno le stesse autorizzazioni che concedi al ruolo IAM.

> **Important**
>
> Se modifichi il ruolo IAM o la policy IAM, le modifiche si applicano al Re:post privato che hai configurato.

Segui queste procedure per creare il ruolo e la policy IAM.

Argomenti

- Utilizza una policy AWS gestita o crea una policy gestita dal cliente
- Policy IAM di esempio
- Creazione di un ruolo IAM
- Risoluzione dei problemi

Utilizza una policy AWS gestita o crea una policy gestita dal cliente

Per concedere le autorizzazioni di ruolo, puoi utilizzare una politica AWS gestita o una politica gestita dal cliente.

> **Tip**
>
> Se non desideri creare una policy manualmente, ti consigliamo di utilizzare invece una policy AWS gestita e di saltare questa procedura. Le politiche gestite dispongono automaticamente delle autorizzazioni necessarie per. AWS Support Non è necessario aggiornare le policy manualmente. Per ulteriori informazioni, consulta AWS politica gestita: AWSRepostSpaceSupportOperationsPolicy.

Segui questa procedura per creare una policy gestita dal cliente per il tuo ruolo. Questa procedura utilizza l'editor di policy JSON nella console IAM.

Per creare una politica gestita dai clienti per Re:post Private

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, selezionare Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Scegliere la scheda JSON.
5. Inserisci il tuo JSON, quindi sostituisci il JSON predefinito nell'editor. Puoi utilizzare la policy di esempio.
6. Scegliere Successivo: Tag.
7. (Facoltativo) Puoi aggiungere metadati alla policy collegando i tag come coppie chiave-valore.
8. Seleziona Successivo: Revisione.
9. Nella pagina Review policy (Rivedi policy), immetti un Name (Nome), ad esempio *`rePostPrivateSupportPolicy`*, e una Description (Descrizione) facoltativa.
10. Consulta la pagina di riepilogo per vedere le autorizzazioni consentite dalla policy, quindi scegli Crea policy.

Questa policy definisce le operazioni che questo ruolo può eseguire. Per ulteriori informazioni, consulta la pagina Creazione di policy IAM (console) nella Guida per l'utente di IAM.

Policy IAM di esempio

Puoi collegare al tuo ruolo IAM la seguente policy di esempio. Questa politica consente al ruolo di disporre delle autorizzazioni complete per tutte le azioni richieste. AWS Support Dopo aver configurato un re:post privato con il ruolo, qualsiasi utente del tuo re:post privato dispone delle stesse autorizzazioni.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
   "Action": [
    "support:AddAttachmentsToSet",
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
   ],
   "Resource": "*"
  }
 ]
}
```

> **Note**
>
> Per un elenco delle politiche AWS gestite per re:POST Private, consulta. AWS policy gestite per AWS Re:Post Private

Puoi aggiornare la politica per rimuovere un'autorizzazione da. AWS Support

Per le descrizioni di ciascuna operazione, consulta i seguenti argomenti nella documentazione di riferimento sulle autorizzazioni dei servizi:

- Operazioni, risorse e chiavi di condizione per AWS Support
- Operazioni, risorse e chiavi di condizione per Service Quotas

- Azioni, risorse e chiavi di condizione per AWS Identity and Access Management

Creazione di un ruolo IAM

Dopo avere creato questa policy, devi creare un ruolo IAM e quindi collegare la policy a tale ruolo. Scegli questo ruolo quando crei un Re:post privato nella console re:POST Private.

Per creare un ruolo per la creazione e la gestione dei casi AWS Support

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, scegli Ruoli e quindi Crea ruolo.
3. Per Trusted entity type (Tipo di entità attendibile), scegli Custom trust policy (Policy di attendibilità personalizzata).
4. Per la politica di fiducia personalizzata, inserisci quanto segue:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Principal": {
    "Service": "repostspace.amazonaws.com"
   },
   "Action": [
    "sts:AssumeRole",
    "sts:SetSourceIdentity"
   ]
  }
 ]
}
```

5. Seleziona Avanti.
6. In Politiche di autorizzazione, nella barra di ricerca, inserisci la politica AWS gestita o una politica gestita dai clienti che hai creato, ad *rePostPrivateSupportPolicy*esempio. Seleziona la casella di controllo accanto alle politiche di autorizzazione che desideri che il servizio abbia.
7. Seleziona Avanti.
8. Nella pagina Nome, rivedi e crea, per Nome del ruolo, inserisci un nome, ad esempio *rePostPrivateSupportRole*.

9. (Facoltativo) In Descrizione, inserisci una descrizione per il ruolo.
10. Rivedi la politica di fiducia e le autorizzazioni.
11. (Facoltativo) Puoi aggiungere metadati al ruolo collegando i tag come coppie chiave-valore. Per ulteriori informazioni sull'utilizzo dei tag con IAM, consulta Tagging delle risorse IAM.
12. Scegli Crea ruolo. Ora puoi scegliere questo ruolo quando configuri un re:post privato nella console re:POST Private. Per informazioni, consulta Crea un nuovo re:post privato.

Per ulteriori informazioni, consulta Creating a role for an AWS service (console) nella IAM User Guide.

Risoluzione dei problemi

Consulta i seguenti argomenti per gestire l'accesso a Re:Post Private.

Indice

- Voglio impedire a utenti specifici del mio re:POST privato di eseguire azioni specifiche
- Quando configuro un re:POST privato, non vedo il ruolo IAM che ho creato
- Al mio ruolo IAM manca un'autorizzazione
- Un errore indica che il mio ruolo IAM non è valido

Voglio impedire a utenti specifici del mio re:POST privato di eseguire azioni specifiche

Per impostazione predefinita, gli utenti del tuo re:post privato dispongono delle stesse autorizzazioni specificate nella policy IAM che colleghi al ruolo IAM che crei. Ciò significa che chiunque faccia parte del re:POST privato ha accesso in lettura o scrittura per creare e gestire i AWS Support casi, indipendentemente dal fatto che disponga o meno di un Account AWS utente IAM.

È preferibile seguire le best practice seguenti:

- Utilizza una policy IAM con le autorizzazioni minime richieste per. AWS Support Per informazioni, consulta AWS politica gestita: AWSRepostSpaceSupportOperationsPolicy.

Quando configuro un re:POST privato, non vedo il ruolo IAM che ho creato

Se il tuo ruolo IAM non compare nell'elenco dei ruoli IAM per re:Post Private;, significa che il ruolo non ha Re:Post Private come entità affidabile o che il ruolo è stato eliminato. Puoi aggiornare il ruolo esistente oppure crearne un altro. Per informazioni, consulta Creazione di un ruolo IAM.

Al mio ruolo IAM manca un'autorizzazione

Il ruolo IAM che crei per il tuo re:post privato necessita delle autorizzazioni per eseguire le azioni che desideri. Ad esempio, se desideri che gli utenti del re:post privato creino casi di supporto, il ruolo deve disporre dell'`support:CreateCase`autorizzazione. re:post Private si assume questo ruolo per eseguire queste azioni per te.

Se ricevi un errore relativo a un'autorizzazione mancante per AWS Support, verifica che la politica allegata al tuo ruolo disponga dell'autorizzazione richiesta.

Consulta la Policy IAM di esempio precedente.

Un errore indica che il mio ruolo IAM non è valido

Verifica di aver scelto il ruolo corretto per la configurazione privata di Re:post.

Configura e gestisci l'accesso degli utenti utilizzando AWS IAM Identity Center

re:Post Private si integra con AWS IAM Identity Center per fornire la federazione delle identità alla forza lavoro della tua organizzazione. Utilizza IAM Identity Center per creare o connettere gli utenti della tua organizzazione e gestirne centralmente l'accesso su tutti gli account e le AWS applicazioni. Per ulteriori informazioni su IAM Identity Center, consulta What is AWS IAM Identity Center (successore di AWS Single Sign-On). Per ulteriori informazioni su come iniziare a usare IAM Identity Center, consulta Getting started. Per utilizzare IAM Identity Center, devi aver AWS Organizations attivato anche l'account.

Personalizza il tuo re:post privato

Puoi aggiungere uno o più amministratori al tuo re:post privato dopo averlo creato. Gli amministratori utilizzano l'applicazione Re:post Private per avviare l'applicazione privata Re:post e gestire gli utenti al suo interno. Possono personalizzare il branding per il re:post privato, aggiungere tag per

classificare i contenuti e selezionare argomenti di interesse per il popolamento automatico dei contenuti. Per ulteriori informazioni, consulta AWS re:Post Private Administration Guide.

Invita gli utenti al tuo re:POST privato

Puoi aggiungere uno o più utenti al tuo re:post privato dopo averlo creato. Puoi invitare gli utenti a collaborare all'interno del tuo re:post privato. Gli utenti utilizzano l'applicazione Re:POST Private per accedere utilizzando le credenziali che avete configurato. Dopo aver effettuato l'accesso a un re:POST privato, gli utenti possono sfogliare o cercare contenuti esistenti, inclusi contenuti formativi e tecnici personalizzati relativi agli argomenti di loro interesse. Per ulteriori informazioni, consulta AWS re:Post Private User Guide.

Gestisci il tuo re:Post privato nella console re:Post Private

Questa sezione spiega come gestire il tuo re:Post privato nella console AWS re:Post Private.

Argomenti

- Aggiungi utenti e gruppi al tuo re:POST privato
- Aggiungi utenti a un gruppo nel tuo re:POST privato
- Invita utenti e gruppi al tuo re:POST privato
- Promuovi un utente nel tuo Re:post privato ad amministratore
- Rimuovi utenti o gruppi dal tuo re:POST privato
- Aggiungi o rimuovi un AWS dipendente dal tuo re:post privato
- Eliminare un Re:post privato da Re:post Private

Aggiungi utenti e gruppi al tuo re:POST privato

Se sei un amministratore, puoi aggiungere utenti e gruppi al tuo re:POST privato.

Aggiungi utenti al tuo re:post privato

1. Apri la console re:POST Private all'indirizzo https://console.aws.amazon.com/repost-private/.
2. Nel riquadro di navigazione, scegli Tutti i miei re:posts privati.
3. Scegli il Re:post privato che desideri gestire.
4. Scegli la scheda Users (Utenti);
5. In Utenti, scegli Aggiungi utenti e gruppi.
6. Dall'elenco, seleziona gli utenti che desideri aggiungere al tuo Re:post privato. Quindi, scegli Assegna.

Gli utenti selezionati vengono aggiunti al tuo Re:post privato ed elencati nella scheda Utenti.

Aggiungi gruppi al tuo re:POST privato

1. Apri la console re:POST Private all'indirizzo https://console.aws.amazon.com/repost-private/.
2. Nel riquadro di navigazione, scegli Tutti i miei re:posts privati.
3. Scegli il Re:post privato che desideri gestire.

4. Scegliere la scheda Groups (Gruppi).
5. Scegli Aggiungi utenti e gruppi.
6. Dall'elenco, seleziona i gruppi che desideri aggiungere al tuo Re:post privato. Quindi, scegli Assegna.

I gruppi selezionati vengono aggiunti al tuo Re:post privato ed elencati nella scheda Gruppi.

Aggiungi utenti a un gruppo nel tuo re:POST privato

Usa IAM Identity Center per aggiungere nuovi utenti a un gruppo esistente nel tuo re:POST privato. Per ulteriori informazioni, consulta Aggiungere utenti ai gruppi nella Guida per l'utente di AWS IAM Identity Center.

Invita utenti e gruppi al tuo re:POST privato

Segui questi passaggi per invitare utenti e gruppi al tuo re:post privato in AWS re:Post Private:

1. Apri la console re:POST Private all'indirizzo https://console.aws.amazon.com/repost-private/.
2. Nel riquadro di navigazione, scegli Tutti i miei re:posts privati.
3. Scegli il Re:post privato che desideri gestire.
4. Per invitare utenti al tuo re:post privato, scegli la scheda Utenti.

   Dall'elenco, seleziona gli utenti che desideri invitare al tuo Re:post privato. Quindi, scegli Utenti onboard per re:POST.
5. Nella finestra di dialogo Aggiungi utenti a questa finestra di dialogo privata di Re:post, inserisci le seguenti informazioni:

   In Oggetto, inserisci l'oggetto del messaggio email che stai inviando.

   In Body, inserisci un messaggio di benvenuto per il tuo Re:post privato.

   Scegli Invia email di onboarding.
6. Per invitare gruppi al tuo re:post privato, scegli la scheda Gruppi.

   Dall'elenco, seleziona i gruppi che desideri invitare nel tuo Re:post privato. Quindi, scegli Gruppi onboard per re:POST.

7. Nei gruppi incorporati in questa finestra di dialogo privata di Re:post, inserisci le seguenti informazioni:

   In Oggetto, inserisci l'oggetto del messaggio email che stai inviando.

   In Body, inserisci un messaggio di benvenuto per il tuo Re:post privato.

   Scegli Invia email di onboarding.

Il messaggio di benvenuto viene inviato a tutti gli utenti e i gruppi selezionati con informazioni su come accedere al tuo re:POST privato.

Promuovi un utente nel tuo Re:post privato ad amministratore

Per promuovere un utente privato di Re:POST a amministratore, segui questi passaggi:

1. Apri la console Re:POST Private all'indirizzo https://console.aws.amazon.com/repost-private/.
2. Nel riquadro di navigazione, scegli Tutti i miei re:posts privati.
3. Scegli il Re:post privato che desideri gestire.
4. Scegli la scheda Users (Utenti);
5. Seleziona uno o più utenti che desideri promuovere ad amministratore.
6. Scegli Modifica ruolo, quindi scegli Rendi amministratore.

Gli utenti selezionati vengono promossi ad amministratori. Nella scheda Utenti, il ruolo di questi utenti viene aggiornato in Amministratore.

Rimuovi utenti o gruppi dal tuo re:POST privato

Se sei un amministratore, puoi rimuovere utenti o gruppi dal tuo re:POST privato.

Rimuovi utenti dal tuo re:POST privato

1. Apri la console re:POST Private all'indirizzo https://console.aws.amazon.com/repost-private/.
2. Nel riquadro di navigazione, scegli Tutti i miei re:posts privati.
3. Scegli il Re:post privato che desideri gestire.
4. In Utenti, dall'elenco, seleziona gli utenti che desideri rimuovere dal tuo re:post privato. Quindi, scegli Rimuovi.

Gli utenti selezionati vengono rimossi dal tuo Re:post privato. Le informazioni sugli utenti rimossi non vengono più visualizzate nella scheda Utenti.

Rimuovi i gruppi dal tuo re:post privato

1. Apri la console re:POST Private all'indirizzo https://console.aws.amazon.com/repost-private/.
2. Nel riquadro di navigazione, scegli Tutti i miei re:posts privati.
3. Scegli il Re:post privato che desideri gestire.
4. Scegliere la scheda Groups (Gruppi).
5. Dall'elenco, seleziona i gruppi che desideri rimuovere dal tuo re:post privato. Quindi, scegli Rimuovi.

I gruppi selezionati vengono rimossi dal tuo Re:post privato. Le informazioni sui gruppi rimossi non vengono più visualizzate nella scheda Gruppi.

Aggiungi o rimuovi un AWS dipendente dal tuo re:post privato

Se disponi di un piano di supporto Enterprise o Enterprise On-Ramp, puoi aggiungere o rimuovere un dipendente AWS dal tuo re:post privato. Contatta Concierge Support o il tuo Technical Account Manager (TAM) per ulteriori informazioni.

Eliminare un Re:post privato da Re:post Private

Per eliminare un re:Post privato in AWS re:Post Private, segui questi passaggi:

1. Apri la console re:POST Private all'indirizzo https://console.aws.amazon.com/repost-private/.
2. Nel riquadro di navigazione, scegli Tutti i miei re:posts privati.
3. Scegli il Re:post privato che desideri gestire, quindi scegli Elimina.
4. Seleziona tutte le opzioni per confermare e confermare che desideri eliminare definitivamente il Re:post privato e i dati ad esso associati.

> **Important**
>
> Quando elimini il Re:post privato, tutte le informazioni di configurazione relative al Re:post privato verranno eliminate. Dopo l'eliminazione del Re:post privato, non puoi ripristinarne alcun contenuto.

5. Inserisci il nome del tuo re:post privato quando ti viene richiesto un ulteriore consenso scritto. Quindi, scegli Elimina.

Occorrono circa 30 minuti per eliminare il tuo Re:post privato.

Monitoraggio di AWS Re:Post Private

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di AWS Re:Post Private e delle altre AWS soluzioni. AWSfornisce i seguenti strumenti di monitoraggio per guardare re:Post Private, 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 istanze Amazon EC2 e avviare automaticamente nuove istanze quando necessario. Per ulteriori informazioni, consulta la Amazon User Guide. CloudWatch
- AWS CloudTrailacquisisce le chiamate API e gli eventi correlati effettuati da o per te Account AWS e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consultare la Guida per l'utente AWS CloudTrail.

Monitoraggio di AWS re:Post Private con Amazon CloudWatch

Puoi monitorare AWS re:Post Private utilizzando Amazon CloudWatch, che raccoglie dati grezzi e li elabora in metriche leggibili quasi in tempo reale. Queste statistiche vengono conservate per 15 mesi in modo da poter accedere alle informazioni storiche e avere una prospettiva migliore sulle prestazioni della tua applicazione o del tuo servizio 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 servizio re:Post Private riporta le seguenti metriche nel namespace. `AWS/rePostPrivate`

Parametro	Descrizione
`NumberOfSpaces`	Il numero di Re:posts privati nell'account corrente. Unità: numero
`NumberOfUsers`	Il numero di utenti in un Re:post privato. Questa metrica utilizza SpaceID come dimensione.

Parametro	Descrizione
	Unità: numero
`ContentSize`	La quantità di contenuti in un Re:post privato. Questa metrica utilizza SpaceID come dimensione. Unità: byte

Le seguenti dimensioni sono supportate per le metriche Re:POST Private.

Dimensione	Descrizione
`spaceId`	L'identificatore univoco per il re:POST privato.

Registrazione delle chiamate API private AWS re:POST utilizzando AWS CloudTrail

AWS re:Post Private è integrato con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Re:Post Private. CloudTrail acquisisce tutte le chiamate API per Re:POST Private come eventi. Le chiamate acquisite includono chiamate dalla console re:POST Private e chiamate in codice alle operazioni dell'API re:POST Private. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per RE:post Private. 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 la richiesta che è stata fatta a Re:post Private, 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 CloudTrail, consulta la Guida per l'AWS CloudTrailutente.

Re:Pubblica informazioni private in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in Re:Post Private, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare

gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Lavorare con la cronologia CloudTrail degli eventi.

Per una registrazione continua degli eventi del tuo sitoAccount AWS, compresi gli eventi di Re:Post Private, 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 percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Creazione di un trail per l'account AWS
- 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 le azioni re:Post Private vengono registrate CloudTrail e documentate nel riferimento all'API privata AWS re:Post. re:Post Private supporta la registrazione delle seguenti azioni come eventi nei file di registro: CloudTrail

- CreateSpace
- DeleteSpace
- DeregisterAdmin
- GetSpace
- ListSpaces
- ListTagsForResource
- RegisterAdmin
- SendInvites
- TagResource
- UntagResource
- UpdateSpace

re:Post Private supporta la registrazione delle seguenti azioni come eventi nei file di registro: AWS Support CloudTrail

- CreateCase
- AddCommunicationToCase
- ResolveCase

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 Elemento CloudTrail userIdentity.

Informazioni sulle voci dei file di registro privati di re:POST

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'`CreateSpace`azione.


```
{
   "eventVersion": "1.08",
   "userIdentity": {
       "type": "AssumedRole",
       "principalId": "AROAQM47QIR7WLEXAMPLE:user",
       "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
       "accountId": "123456789012",
       "accessKeyId": "EXAMPLE_KEY_ID",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR7WLEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User",
                "accountId": "123456789012",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-06T19:24:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-06T21:37:44Z",
    "eventSource": "repostspace.amazonaws.com",
    "eventName": "CreateSpace",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",
    "requestParameters": {
        "spaceName": "Test space name",
        "spaceSubdomain": "customsubdomain",
        "tagSet": {},
        "tier": "2000",
        "roleArn": "",
        "spaceDescription": "Test space description"
    },
    "responseElements": {
        "spaceId": "SPLPWvQmv9SIWYF30EXAMPLE",
        "Access-Control-Expose-Headers": "x-amzn-errortype, x-amzn-requestid, x-amzn-
errormessage, x-amzn-trace-id, x-amz-apigw-id, date"
    },
    "requestID": "71d815e0-6632-4ec9-9fac-92af3e4a86dc",
    "eventID": "30a6c3da-ce2e-4931-ba5d-b3cc7cf16ec8",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`RegisterAdmin`azione.


```
{
   "eventVersion": "1.08",
   "userIdentity": {
       "type": "AssumedRole",
       "principalId": "AROAQM47QIR7WLEXAMPLE:user",
       "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
       "accountId": "123456789012",
       "accessKeyId": "EXAMPLE_KEY_ID",
       "sessionContext": {
           "sessionIssuer": {
               "type": "Role",
               "principalId": "AROAQM47QIR7WLEXAMPLE",
               "arn": "arn:aws:iam::123456789012:role/User",
               "accountId": "123456789012",
               "userName": "User"
           },
           "webIdFederationData": {},
           "attributes": {
               "creationDate": "2023-11-07T21:17:19Z",
               "mfaAuthenticated": "false"
           }
       }
   },
   "eventTime": "2023-11-07T21:24:23Z",
   "eventSource": "repostspace.amazonaws.com",
   "eventName": "RegisterAdmin",
   "awsRegion": "us-west-2",
   "sourceIPAddress": "205.251.233.183",
   "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",
   "requestParameters": {
       "adminId": "08612310-a0f1-7063-3e54-fb2960444dd1",
       "spaceId": "SPlYNZE-ylQEmAXpmEXAMPLE"
   },
   "responseElements": {
       "Access-Control-Expose-Headers": "x-amzn-errortype, x-amzn-requestid, x-amzn-
errormessage, x-amzn-trace-id, x-amz-apigw-id, date"
   },
```

```
    "requestID": "9939ebbe-8599-4f9a-827b-4995e3006001",
    "eventID": "e1873b18-f80c-4934-9ff2-bf5b35c78031",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`ListSpaces`azione.

```
 {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR7WLEXAMPLE:user",
        "arn": "arn:aws:sts::123456789012:assumed-role/User/user",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR7WLEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/User",
                "accountId": "123456789012",
                "userName": "User"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-09T22:28:23Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-09T22:38:34Z",
    "eventSource": "repostspace.amazonaws.com",
    "eventName": "ListSpaces",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/119.0.0.0 Safari/537.36",
```

```
    "requestParameters": null,
    "responseElements": null,
    "requestID": "95be587b-c04f-4eb0-9269-12fee33ae2e3",
    "eventID": "9777da32-545f-44c4-af0b-1d9109b8cbc3",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'`ResolveCase`azione. È possibile utilizzare l'`sourceIdentity`elemento di questa voce di registro per identificare l'utente che ha risolto il caso.

```
 {
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR76DQZ7N5WX:create-support-case-
Uk1iHNTWQEOLmR2BR1FDJQ",
        "arn": "arn:aws:sts::123456789012:assumed-role/AWSRepostSpaceRole/create-
support-case-Uk1iHNTWQEOLmR2BR1FDJQ",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR76DQZ7N5WX",
                "arn": "arn:aws:iam::123456789012:role/AWSRepostSpaceRole",
                "accountId": "123456789012",
                "userName": "AWSRepostSpaceRole"
            },
            "attributes": {
                "creationDate": "2023-11-17T21:46:42Z",
                "mfaAuthenticated": "false"
            },
            "sourceIdentity": "28e17330-10f1-705d-7cba-3a62a6b10e2e"
        }
    },
    "eventTime": "2023-11-17T21:46:44Z",
    "eventSource": "support.amazonaws.com",
```

```
    "eventName": "ResolveCase",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.68.27.29",
    "userAgent": "aws-sdk-nodejs/2.1363.0 linux/v16.20.2 exec-env/AWS_ECS_FARGATE
 promise",
    "requestParameters": {
        "caseId": "case-123456789012-muen-2023-75d2c35481b96357"
    },
    "responseElements": {
        "initialCaseStatus": "unassigned",
        "finalCaseStatus": "resolved"
    },
    "requestID": "594b91c6-df1c-47e4-a834-d67d67f34b9d",
    "eventID": "7fc9cbe4-c8d5-4d61-a016-e076de272fff",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "support.us-west-2.amazonaws.com"
    }
}
```

Risoluzione dei problemi di re:Post Private

Le seguenti informazioni possono aiutarti a risolvere i problemi con AWS re:Post Private.

Argomenti

- Non riesco a configurare il mio re:Post privato in una regione specifica AWS
- Non riesco a configurare il re:post privato nel mio account
- Non puoi gestire utenti o gruppi in un re:POST privato

Non riesco a configurare il mio re:Post privato in una regione specifica AWS

Re:POST Private è disponibile solo nelle regioni Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Europa (Francoforte), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Canada (Centrale) ed Europa (Irlanda). Assicurati di creare il tuo re:Post privato in una di queste regioni.

Non riesco a configurare il re:post privato nel mio account

Assicurati di aver abilitato AWS IAM Identity Center il tuo account e di aver configurato IAM Identity Center nella stessa regione in cui desideri creare il Re:post privato. Per ulteriori informazioni, consulta Prerequisiti.

Non puoi gestire utenti o gruppi in un re:POST privato

Assicurati di disporre delle autorizzazioni necessarie per modificare un Re:post privato e gestire utenti e gruppi all'interno del Re:post privato. Per ulteriori informazioni, consulta Esempi di policy basate sull'identità privata di AWS re:Post.

Cronologia dei documenti

La tabella seguente descrive le versioni della documentazione per AWS re:Post Private:

Modifica	Descrizione	Data
Aggiorna	Aggiunti Stati Uniti orientali (Virginia settentrionale), Asia Pacifico (Sydney), Canada (Centrale) ed Europa (Irlanda) alle regioni supportate	10 maggio 2024
Aggiorna	È stata aggiunta l'area Asia Pacifico (Singapore) alle regioni supportate	6 marzo 2024
Nuove risorse	Aggiunta documentazione per le policy gestite da AWS per AWS Re:Post Private	26 novembre 2023
Versione iniziale	Versione iniziale della Re:POST Private Console Administration Guide	26 novembre 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.