Administratorhandbuch für die Konsole

AWS re:Post Private

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS re:Post Private: Administratorhandbuch für die Konsole

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und die Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

..... v
Was ist AWS re:Post Private? 1
Greifen Sie auf re:Post Private zu 1
Preisgestaltung 2
Melde dich für eine an AWS-Konto 2
Voraussetzungen 2
An Bord von re:POST Private 4
Sicherheit 5
Datenschutz 6
Datenschutz durch Verschlüsselung 7
Verschlüsselung während der Übertragung 7
Schlüsselverwaltung 7
So funktioniert re:Post Private mit IAM 7
Re: Post-Richtlinien, die auf privaten Identitäten basieren 7
Re:Post-Richtlinien, die auf privaten Ressourcen basieren 9
Autorisierung auf der Basis von Markierungen 9
Betreff: Private IAM-Rollen veröffentlichen 10
Service-linked Rollen 10
Servicerollen 10
Verwenden von servicegebundenen Rollen 10
Identity-based Beispiele für Richtlinien 14
Eingebundene Richtlinien 17
AWS verwaltete Richtlinien 19
Fehlerbehebung 22
Compliance-Validierung 24
Ausfallsicherheit 25
Infrastruktursicherheit 25
Kontingente 26
Servicekontingente 26
Grenzwerte für die API-Drosselung 26
Erstellen, Konfigurieren und Anpassen Ihres privaten re:Post 28
Erstellen eines neuen privaten re:Post 28
Verwalten Sie die Support Fallerstellung und -verwaltung 30
Verwenden oder erstellen Sie eine verwaltete Richtlinie 31

Beispiel für eine IAM-Richtlinie ... 32
Erstellen einer IAM-Rolle ... 33
Fehlerbehebung ... 35
Benutzerzugriff einrichten und verwalten ... 36
Personalisiere deinen privaten re:POST ... 36
Lade Nutzer zu deinem privaten re:POST ein ... 37
Verwalte deinen privaten re:POST ... 38
Hinzufügen von Benutzern ... 38
Füge Gruppen hinzu ... 39
Hinzufügen von Benutzern zu einer Gruppe ... 39
Lade Nutzer und Gruppen ein ... 40
Weisen Sie einem Benutzer eine Rolle zu ... 41
Benutzer entfernen ... 41
Gruppen entfernen ... 42
Einen Mitarbeiter hinzufügen oder entfernen AWS ... 42
Erstelle einen neuen Kanal in deinem privaten re:POST ... 42
Verwalte Benutzer und Gruppen in deinem Kanal ... 43
Lösche einen privaten re:Post ... 45
Überwachung von re:Post Private ... 47
Überwachung mit CloudWatch ... 47
Protokollierung von Re:POST Private API-Aufrufen mit AWS CloudTrail ... 48
Re:Veröffentlichen Sie private Informationen in CloudTrail ... 49
Grundlegendes zu den privaten Re:POST-Logdateieinträgen ... 50
Fehlerbehebung ... 56
Ich kann meinen privaten re:POST nicht in einer bestimmten Region einrichten AWS ... 56
Ich kann privaten re:POST nicht in meinem Konto einrichten ... 56
Benutzer oder Gruppen können in einem privaten re:POST nicht verwaltet werden ... 56
Dokumentverlauf ... 57

Hinweis zum Ende des Supports: Am 30. Juni 2027, AWS wird den Support für AWS re:Post Private beenden. Nach dem 30. Juni 2027 werden Sie nicht mehr auf die Re:Post Private-Konsole oder die Re:Post Private-Ressourcen zugreifen können. Weitere Informationen finden Sie unter Ende des Supports für AWS re:Post Private.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.

Was ist AWS re:Post Private?

AWS re:Post Private ist eine private Version von AWS re:Post für Unternehmen mit Enterprise Support oder Enterprise On-Ramp Support-Pläne. Es bietet Zugang zu Wissen und Experten, um die Cloud-Einführung zu beschleunigen und die Produktivität der Entwickler zu steigern. Mit Ihrem unternehmensspezifischen privaten Re:Post können Sie eine organisationsspezifische Entwickler-Community aufbauen, die die Effizienz in großem Maßstab steigert und Zugriff auf wertvolle Wissensressourcen bietet. Darüber hinaus zentralisiert Re:Post Private vertrauenswürdige AWS technische Inhalte und private Diskussionsforen, um die Zusammenarbeit Ihrer Teams intern und mit AWS zu verbessern, um technische Hindernisse zu beseitigen, Innovationen zu beschleunigen und effizienter in der Cloud zu skalieren.

Weitere Informationen finden Sie unter AWS re:Post Private.

Greifen Sie auf re:Post Private zu

Administratoren verwenden die AWS Re:POST Private-Konsole, um ihren organisationsspezifischen privaten Re:POST zu erstellen. Wenn Administratoren einen privaten Re:POST erstellen, können sie ihrem privaten Re:POST einen Namen geben und eine Subdomain definieren unter `*.private.repost.aws`. Administratoren für das private Re:POST einer Organisation können den Benutzerzugriff wie folgt konfigurieren AWS IAM Identity Center und geben Sie eine der folgenden Identitätsquellen für die Authentifizierung an: Identity Center-Verzeichnis, Active Directory oder einen externen Identitätsanbieter. Nach der Konfiguration der Benutzer können Konsolenadministratoren einem oder mehreren Benutzern eine re:POST Private-Administratorrolle zuweisen. re:POST Private-Administratoren können ihre private Re:Post-Anwendung an das Branding und die Wissensanforderungen des Unternehmens anpassen. Die AWS Mitglieder des Account-Teams, wie z. B. Technical Account Manager, die mit der Architektur und den Arbeitslasten des Unternehmens vertraut sind, werden automatisch zur Zusammenarbeit in den privaten Re:POST-Bereich der Organisation aufgenommen.

Administratoren der Re:Post Private-Anwendung können das Branding anpassen, Schlagworte hinzufügen, um Inhalte zu klassifizieren, und Themen auswählen, die für ihre Entwickler von Interesse sind, um sie automatisch mit Schulungen und technischen Inhalten zu versehen. Sie können Benutzer auch einladen, ihrem privaten Re:POST beizutreten, um die Zusammenarbeit zu verbessern. Weitere Informationen finden Sie unter AWS Re:Post — Handbuch für die private Verwaltung.

Non-administrative Benutzer verwenden die Re:Post Private-Anwendung, um sich mit Anmeldeinformationen anzumelden, die von ihrem Administrator konfiguriert wurden. Nach der Anmeldung bei einem privaten re:POST können Benutzer vorhandene Inhalte durchsuchen oder durchsuchen, einschließlich maßgeschneiderter Schulungen und technischer Inhalte, die auf ihre Interessengebiete zugeschnitten sind. Nutzer können auch suchen AWS öffentliche technische Inhalte direkt von ihrem privaten Re:Poste aus und erstelle private Threads für interne Diskussionen auf AWS öffentliche Inhalte. Benutzer können gemeinsam Lösungen finden AWS technische Probleme und holen sich technische Anleitungen von anderen Nutzern des privaten Re:Post, indem sie eine Frage stellen, eine Antwort geben oder einen Artikel veröffentlichen. Nutzer können einen Diskussionsthread auch in einen umwandeln Support Fall. Benutzer können wählen, ob sie die Antworten von hinzufügen möchten Support zum privaten re:POST. Weitere Informationen finden Sie unter AWS Re:Post Private-Benutzerhandbuch.

Preisgestaltung

Nur Kunden mit Enterprise Support (ES) und Enterprise On-Ramp (EOP) Support-Pläne können den Re:Post Private-Service abonnieren. Sie können aus den beiden verfügbaren Preisstufen wählen — dem kostenlosen Tarif und dem Standardtarif. Das kostenlose Kontingent bietet Ihnen die Möglichkeit, die Funktionen des Standard-Tarifs sechs Monate lang in vollem Umfang auszuprobieren, bevor Sie nahtlos zu einem kostenpflichtigen Tarif wechseln können. Wenn Sie die Standard-Stufe nutzen, können Sie für die Nutzung von re:Post Private ein monatliches Abonnement pro Nutzergebühr bezahlen. Weitere Informationen finden Sie unter – Preise.

Melde dich für eine an AWS-Konto

Um loszulegen mit AWS, du brauchst eine AWS-Konto. Es gibt zwei Möglichkeiten, sich anzumelden AWS. Wenn Sie die vollständige Kontrolle über die Kontokonfiguration und den Speicherort Ihrer Inhalte haben möchten oder wenn Sie regulierte Workloads wie HIPAA oder FedRAMP haben, verwenden Sie Melden Sie sich an für AWS (fortgeschritten). Wenn Sie ein neuer Benutzer sind und ein Konto verwenden möchten, das Sie bereits besitzen, um sich anzumelden AWS und erstellen Sie eine AWS Umgebung mit vorkonfigurierten Standardwerten in select AWS-Regionen, verwenden Melde dich an für AWS.

Voraussetzungen

Sie müssen die folgenden Voraussetzungen erfüllen, bevor Sie einen neuen privaten Re:Post erstellen oder einen vorhandenen privaten Re:Post in AWS re:Post Private verwalten können:

- Sie müssen sich für eine registrieren Unternehmen oder Unternehmen On-Ramp Unterstützungsplan.
- Du musst ermöglichen AWS IAM Identity Center in derselben Region, in der du deinen privaten Re:POST einrichten möchtest.
- Du musst einen erstellen AWS Identity and Access Management Rolle, die über die erforderlichen Berechtigungen zum Erstellen, Verwalten und Lösen verfügt Support Fälle für Sie. Der Re:Post Private Service verwendet diese Rolle, um API-Aufrufe zu tätigen Support. Weitere Informationen finden Sie unter Verwalten Sie den Zugriff auf Support Erstellung und Verwaltung von Fällen in Re:Post Private.

Über das IAM Identity Center auf re:POST Private einsteigen

re:POST Private lässt sich integrieren und bietet so einen Identitätsverbund für Ihre Belegschaft. AWS IAM Identity Center Über IAM Identity Center werden Benutzer in ihr bestehendes Unternehmensverzeichnis umgeleitet, um sich mit ihren vorhandenen Anmeldeinformationen anzumelden. Anschließend sind sie nahtlos bei ihrem privaten re:POST angemeldet. Dadurch wird sichergestellt, dass Sicherheitseinstellungen wie Passwortrichtlinien und Zwei-Faktor-Authentifizierung durchgesetzt werden. Die Verwendung von IAM Identity Center hat keine Auswirkungen auf Ihre bestehende IAM-Konfiguration.

Wenn Sie kein vorhandenes Benutzerverzeichnis haben oder keinen Verbund bevorzugen, bietet IAM Identity Center ein integriertes Benutzerverzeichnis, mit dem Sie Benutzer und Gruppen für re:POST Private erstellen können. re:Post Private unterstützt nicht die Verwendung von IAM-Benutzern und -Rollen zur Zuweisung von Berechtigungen innerhalb einer privaten re:POST. Benutzerberechtigungen innerhalb einer privaten re:POST-Anwendung werden von einem Administrator in seiner privaten re:POST-Anwendung konfiguriert.

Weitere Informationen zu IAM Identity Center finden Sie unter Was ist AWS IAM Identity Center (Nachfolger von AWS Single Sign-On). Weitere Informationen zu den ersten Schritten mit IAM Identity Center finden Sie unter Erste Schritte. Um IAM Identity Center verwenden zu können, müssen Sie es auch für das AWS Organizations Konto aktiviert haben.

> **Important**
>
> re:POST Private unterstützt nur Organisationsinstanzen von IAM Identity Center.

Sicherheit in Re:Post Private

Cloud-Sicherheit unter AWS hat höchste Priorität. Als AWS Als Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die so konzipiert sind, dass sie die Anforderungen der sicherheitsrelevantesten Organisationen erfüllen.

Sicherheit ist eine gemeinsame Verantwortung zwischen AWS und du. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der laufenden Infrastruktur AWS Dienste in der AWS Cloud. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-party Auditoren testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheit im Rahmen der AWS Compliance-Programme. Weitere Informationen zu den Compliance-Programmen, die für AWS re:Post Private gelten, finden Sie unter AWS Dienstleistungen im Rahmen des Compliance-Programms.
- Sicherheit in der Cloud — Ihre Verantwortung wird bestimmt durch AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, die Anforderungen Ihres Unternehmens und die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung anwenden können, wenn Sie re:Post Private verwenden. Die folgenden Themen zeigen Ihnen, wie Sie re:Post Private so konfigurieren, dass Ihre Sicherheits- und Compliance-Ziele erreicht werden. Sie lernen auch, wie Sie andere verwenden AWS Dienste, die Ihnen helfen, Ihre Re:Post Private-Ressourcen zu überwachen und zu sichern.

Topics

- Datenschutz in AWS re:Post Private
- So funktioniert re:Post Private mit IAM
- Überprüfung der Konformität für AWS re:Post Private
- Resilienz in AWS re:Post Private
- Infrastruktursicherheit in AWS re:Post Private

Datenschutz in AWS re:Post Private

Das AWS Modell der gemeinsamen Verantwortung gilt für den Datenschutz in AWS re:Post Private. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum DatenschutzRechtliche. Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir Ihnen, Folgendes zu schützen AWS-Konto Anmeldeinformationen und richten Sie einzelne Benutzer ein mit AWS IAM Identity Center oder AWS Identity and Access Management (ICH BIN). So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Benutzen SSL/TLS um zu kommunizieren mit AWS Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten ein mit AWS CloudTrail. Für Informationen zur Verwendung CloudTrail Spuren zum Erfassen AWS Aktivitäten, siehe Arbeiten mit CloudTrail Wanderwege in der AWS CloudTrail Benutzerleitfaden.
- Benutzen AWS Verschlüsselungslösungen sowie alle darin enthaltenen Standard-Sicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie beim Zugriff auf FIPS 140-3-validierte kryptografische Module benötigen AWS Verwenden Sie über eine Befehlszeilenschnittstelle oder eine API einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Re:Post Private oder anderen arbeiten AWS-Services mithilfe der Konsole, der API, AWS CLI, oder AWS SDKs. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet

werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenschutz durch Verschlüsselung

Verschlüsselung im Ruhezustand

Re:POST Private verwendet Amazon Simple Storage Service-Buckets, Amazon DynamoDB-Datenbanken, Amazon Neptune-Datenbanken und Amazon OpenSearch Servicedomänen, die im Ruhezustand entweder mit von Amazon verwalteten Schlüsseln oder mit vom Kunden verwalteten Schlüsseln verschlüsselt werden.

Verschlüsselung während der Übertragung

Re:Post Private verwendet das HTTPS-Protokoll, um mit Ihrer Client-Anwendung zu kommunizieren. Es verwendet HTTPS und AWS Signaturen, um im Namen Ihrer Anwendung mit anderen Diensten zu kommunizieren.

Schlüsselverwaltung

Re:Post Private ist integriert in AWS Key Management Service und unterstützt AWS KMS Schlüssel. Du kannst die Datenverschlüsselungseinstellungen für deinen privaten re:POST anpassen, wenn du ihn erstellst. Dazu kannst du entweder ein vorhandenes wählen AWS KMS Schlüssel oder erstelle ein neues AWS KMS Schlüssel.

So funktioniert re:Post Private mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf AWS re:Post Private zu verwalten, müssen Sie wissen, welche IAM-Funktionen für re:Post Private verfügbar sind. Um einen allgemeinen Überblick darüber zu erhalten, wie RE:Post Private und andere AWS Dienste funktionieren mit IAM, siehe AWS Dienste, die mit IAM funktionieren in der IAM-Benutzerhandbuch.

Re: Post-Richtlinien, die auf privaten Identitäten basieren

Mit identitätsbasierten IAM-Richtlinien können Sie zulässige oder verweigerte Aktionen angeben. re:Post Private unterstützt bestimmte Aktionen. Informationen zu den Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Administratoren können Folgendes verwenden AWS JSON-Richtlinien, um festzulegen, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu gewähren.

Richtlinienaktionen in Re:Post Private verwenden das folgende Präfix vor der Aktion: `repostspace:`. Zum Beispiel, um jemandem die Erlaubnis zu erteilen, Re:Post Private auszuführen `CreateSpace` API-Betrieb, Sie schließen die ein `repostspace:CreateSpace` Maßnahmen in ihrer Richtlinie. Grundsatzerklärungen müssen entweder eine enthalten `Action` oder `NotAction` element. re:Post Private definiert einen eigenen Satz von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können.

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommata:

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

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

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

Eine Liste der Aktionen von re:Post Private finden Sie unter Von re:Post Private definierte Aktionen in der IAM-Benutzerhandbuch.

Ressourcen

Administratoren können verwenden AWS JSON-Richtlinien, um festzulegen, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Bedingungsschlüssel

Re:Post Private bietet keine dienstspezifischen Bedingungsschlüssel, unterstützt jedoch die Verwendung globaler Bedingungsschlüssel. Um alles zu sehen AWS globale Bedingungsschlüssel finden Sie unter AWS globale Bedingungskontextschlüssel in der IAM-Benutzerhandbuch.

Beispiele

Beispiele für identitätsbasierte Re:Post Private Richtlinien finden Sie unter Beispiele für auf der privaten Identität basierende Richtlinien von AWS Re:Post.

Re:Post-Richtlinien, die auf privaten Ressourcen basieren

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Principals können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS Dienste. Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können nicht verwenden AWS verwaltete Richtlinien von IAM in einer ressourcenbasierten Richtlinie.

Re:Post Private unterstützt keine ressourcenbasierten Richtlinien.

Autorisierung auf der Basis von Markierungen

Re:Post Private unterstützt das Taggen von Ressourcen oder die Steuerung des Zugriffs auf der Grundlage von Stichwörtern. Weitere Informationen finden Sie unter Steuerung des Zugriffs auf AWS-Ressourcen mithilfe von Tags.

Betreff: Private IAM-Rollen veröffentlichen

Ein IAM-Rolle ist eine Entität in Ihrem AWS Konto, das über bestimmte Berechtigungen verfügt.

Verwendung temporärer Anmeldeinformationen mit re:POST Private

Wir empfehlen dringend, temporäre Anmeldeinformationen zu verwenden, um sich mit einem Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontoübergreifende Rolle zu übernehmen. Temporäre Anmeldeinformationen erhalten Sie, indem Sie anrufen AWS STS API-Operationen wie AssumeRole oder GetFederationToken.

Re:Post Private unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-linked Rollen

Service-linked Rollen ermöglichen AWS Diensten den Zugriff auf Ressourcen in anderen Diensten, um eine Aktion für Sie abzuschließen. Service-linked Rollen werden in Ihrem IAM-Konto angezeigt und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Servicerollen

Diese Funktion ermöglicht es einem Dienst, eine Service-Rolle für dich. Diese Rolle ermöglicht es dem Dienst, auf Ressourcen in anderen Diensten zuzugreifen, um eine Aktion für Sie abzuschließen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Dienstes beeinträchtigen.

Verwendung von serviceverknüpften Rollen für Re:Post Private

AWS Re:Post Private verwendet AWS Identity and Access Management (ICH BIN) dienstgebundene Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit re:Post Private verknüpft ist. Service-linked Rollen werden von re:Post Private vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere Rollen aufzurufen AWS Dienste in Ihrem Namen.

Eine dienstgebundene Rolle erleichtert die Einrichtung von re:Post Private, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. re:Post Private definiert die Berechtigungen seiner dienstverknüpften Rollen, und sofern nicht anders definiert, kann nur re:Post Private seine Rollen

übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Diensten, die dienstbezogene Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren und suchen Sie nach den Diensten, die Ja in der Service-linked Rollen Spalte. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Service-linked Rollenberechtigungen für Re:Post Private

re:Post Private verwendet die mit dem Dienst verknüpfte Rolle namens AWSServiceRoleForrePostPrivate. re:Post Private verwendet diese dienstbezogene Rolle, um Daten zu veröffentlichen CloudWatch.

Das AWSServiceRoleForrePostPrivate Die dienstgebundene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `repostspace.amazonaws.com`

Die Richtlinie für Rollenberechtigungen heißt `AWSrePostPrivateCloudWatchAccess` ermöglicht es re:Post Private, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion am `cloudwatch`: `PutMetricData`

Sie müssen Berechtigungen konfigurieren, damit eine Benutzer, Gruppen oder Rollen eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie unter Service-linked Rollenberechtigungen in der IAM-Benutzerhandbuch.

Weitere Informationen finden Sie unter AWSrePostPrivateCloudWatchAccess.

Erstellung einer serviceverknüpften Rolle für Re:Post Private

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn du deinen ersten privaten Re:Post erstellst in der AWS-Managementkonsole, der AWS CLI, oder der AWS API, re:Post Private erstellt die serviceverknüpfte Rolle für Sie.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten

Features verwendet. Wenn Sie den Re:Post Private-Dienst vor dem 1. Dezember 2023 verwendet haben, als er begann, serviceverknüpfte Rollen zu unterstützen, hat Re:Post Private außerdem den `AWSServiceRoleForrePostPrivate` Rolle in deinem Konto. Weitere Informationen finden Sie unter Eine neue Rolle erschien in meinem AWS-Konto.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn du deinen ersten privaten Re:POST erstellst, erstellt re:POST Private die serviceverknüpfte Rolle erneut für dich.

In der AWS CLI oder der AWS API, erstellen Sie eine serviceverknüpfte Rolle mit der `repostspace.amazonaws.com` Dienstname. Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeitung einer dienstverknüpften Rolle für Re:Post Private

Mit Re:Post Private können Sie das nicht bearbeiten `AWSServiceRoleForrePostPrivate` Rolle, die mit einem Dienst verknüpft ist. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Re:Post Private

Sie müssen die Rolle `AWSServiceRoleForrePostPrivate` nicht manuell löschen. Wenn du deinen privaten Re:POST löschst in der AWS-Managementkonsole, der AWS CLI, oder der AWS API, re:Post Private löscht die mit dem Dienst verknüpfte Rolle für Sie.

Sie können auch die IAM-Konsole verwenden, die AWS CLI, oder die AWS API zum manuellen Löschen der dienstverknüpften Rolle.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die AWS CLI, oder die AWS API zum Löschen der AWSServiceRoleForrePostPrivate Mit einem Dienst verknüpfte Rolle. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte Rollen von Re:Post Private

Re:Post Private unterstützt die Verwendung dienstbezogener Rollen in der AWS Regionen, in denen der Service verfügbar ist.

Name der Region	Regions-ID	Unterstützung in Re:Post Private
USA Ost (Nord-Virginia)	us-east-1	Ja
USA Ost (Ohio)	us-east-2	Nein
USA West (Nordkalifornien)	us-west-1	Nein
USA West (Oregon)	us-west-2	Ja
Afrika (Kapstadt)	af-south-1	Nein
Asien-Pazifik (Hongkong)	ap-east-1	Nein
Asien-Pazifik (Jakarta)	ap-southeast-3	Nein
Asien-Pazifik (Mumbai)	ap-south-1	Nein
Asia Pacific (Osaka)	ap-northeast-3	Nein
Asien-Pazifik (Seoul)	ap-northeast-2	Nein
Asien-Pazifik (Singapur)	ap-southeast-1	Ja
Asien-Pazifik (Sydney)	ap-southeast-2	Ja
Asien-Pazifik (Tokyo)	ap-northeast-1	Nein
Kanada (Zentral)	ca-central-1	Ja
Europa (Frankfurt)	eu-central-1	Ja
Europa (Ireland)	eu-west-1	Ja
Europa (London)	eu-west-2	Nein

Name der Region	Regions-ID	Unterstützung in Re:Post Private
Europa (Milan)	eu-south-1	Nein
Europa (Paris)	eu-west-3	Nein
Europa (Stockholm)	eu-north-1	Nein
Naher Osten (Bahrain)	me-south-1	Nein
Naher Osten (VAE)	me-central-1	Nein
Südamerika (São Paulo)	sa-east-1	Nein

Beispiele für auf der privaten Identität basierende Richtlinien von AWS Re:Post

> **Note**
>
> Für mehr Sicherheit sollten Sie nach Möglichkeit Verbundbenutzer anstelle von IAM-Benutzern erstellen.

In der Standardeinstellung AWS Identity and Access Management Benutzer und Rollen sind nicht berechtigt, private AWS Re:POST-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit dem ausführen AWS-Managementkonsole, AWS CLI, oder AWS API. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern und Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Benutzern oder -Gruppen anfügen, die diese Berechtigungen benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Themen

- Best Practices für Richtlinien

- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand Re:Post Private-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn du identitätsbasierte Richtlinien erstellst oder bearbeitest, befolge diese Richtlinien und Empfehlungen:

- Beginnen Sie mit AWS verwaltete Richtlinien und Umstellung auf Berechtigungen mit geringsten Rechten — Um mit der Vergabe von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, verwenden Sie AWS verwaltete Richtlinien die Berechtigungen für viele gängige Anwendungsfälle gewähren. Sie sind in Ihrem verfügbar AWS-Konto. Wir empfehlen, die Berechtigungen weiter zu reduzieren, indem Sie Folgendes definieren AWS vom Kunden verwaltete Richtlinien, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese im Rahmen einer bestimmten Aktion genutzt werden AWS-Service, wie CloudFormation. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere

und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Mehrstufige Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem AWS-Konto, schalten Sie MFA für zusätzliche Sicherheit ein. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI oder AWS API.

```
{
    "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": "*"
        }
    ]
}
```

Eingebundene Richtlinien

Inline-Richtlinien sind Richtlinien, die Sie erstellen und verwalten. Sie können Inline-Richtlinien direkt in einen Benutzer, eine Gruppe oder eine Rolle einbetten. Die folgenden Richtlinienbeispiele zeigen, wie Berechtigungen für die Durchführung von AWS Re:Post Private-Aktionen zugewiesen werden. Allgemeine Informationen zu integrierten Richtlinien finden Sie unter Verwaltung von IAM-Richtlinien in der AWS IAM-Benutzerhandbuch. Sie können das verwenden AWS-Managementkonsole, AWS Command Line Interface (AWS CLI) oder AWS Identity and Access Management API zum Erstellen und Einbetten von Inline-Richtlinien.

Themen

- Read-only Zugriff auf Re:Post Private
- Voller Zugriff auf Re:Post Private

Read-only Zugriff auf Re:Post Private

Die folgende Richtlinie gewährt einem Benutzer Lesezugriff für das IAM Identity Center und die Re:POST Private-Konsole. Diese Richtlinie ermöglicht es dem Benutzer, re:POST Private-Aktionen auszuführen, die nur lesbar sind.

JSON

```
{
    "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": "*"
        }
    ]
}
```

Voller Zugriff auf Re:Post Private

Die folgende Richtlinie gewährt einem Benutzer vollen Zugriff auf das IAM Identity Center und die re:POST Private-Konsole. Diese Richtlinie ermöglicht es dem Benutzer, alle Re:POST Private-Aktionen durchzuführen.

JSON

```
{
    "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 verwaltete Richtlinien für AWS re:Post Private

Verwenden AWS Verwaltete Richtlinien machen das Hinzufügen von Berechtigungen zu Benutzern, Gruppen und Rollen einfacher, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Verwenden AWS verwaltete Richtlinien, um schnell loszulegen. Diese Richtlinien decken gängige Anwendungsfälle ab und sind in Ihrem AWS Konto. Für weitere

Informationen über AWS verwaltete Richtlinien finden Sie unter AWS verwaltete Richtlinien in der IAM-Benutzerhandbuch.

AWS Dienste pflegen und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in nicht ändern AWS verwaltete Richtlinien. Dienste können gelegentlich zusätzliche Berechtigungen zu einem hinzufügen AWS verwaltete Richtlinie zur Unterstützung neuer Funktionen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Dienste aktualisieren am ehesten eine AWS verwaltete Richtlinie, wenn eine neue Funktion gestartet wird oder wenn neue Funktionen verfügbar werden. Dienste entfernen keine Berechtigungen von AWS verwaltete Richtlinie, sodass Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigen.

Darüber hinaus AWS unterstützt verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Zum Beispiel die `ReadOnlyAccess` AWS Die verwaltete Richtlinie bietet nur Lesezugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion einführt, AWS fügt schreibgeschützte Berechtigungen für neue Operationen und Ressourcen hinzu. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Themen

- AWS verwaltete Richtlinie: AWSRepostSpaceSupportOperationsPolicy
- AWS verwaltete Richtlinie: AWSrePostPrivateCloudWatchAccess
- AWS Re:Post Private Aktualisierungen für AWS Verwaltete Richtlinien

AWS verwaltete Richtlinie: AWSRepostSpaceSupportOperationsPolicy

Diese Richtlinie ermöglicht es dem AWS Re:Post Private Service, diese zu erstellen, zu verwalten und zu lösen Support Fälle, die über die Re:Post Private-Webanwendung erstellt werden.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
   "Action": [
    "support:AddAttachmentsToSet",
```

```
    "support:AddCommunicationToCase",
    "support:CreateCase",
    "support:DescribeCases",
    "support:DescribeCommunications",
    "support:ResolveCase"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS verwaltete Richtlinie: AWSrePostPrivateCloudWatchAccess

Diese Richtlinie ermöglicht es dem Re:Post Private-Dienst, Daten zu veröffentlichen CloudWatch.

JSON

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

AWS Re:Post Private Aktualisierungen für AWS Verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen an AWS verwaltete Richtlinien für re:POST Private, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Dokumentverlauf-Seite.

In der folgenden Tabelle werden wichtige Aktualisierungen der von Re:Post Private verwalteten Richtlinien seit dem 26. November 2023 beschrieben.

Änderungen	Beschreibung	Date
Neue Richtlinie - AWSrePost PrivateCloudWatchAccess	Neue verwaltete Richtlinie für die Veröffentlichung von Daten in CloudWatch	26. November 2023
Neue Richtlinie - AWSRepost SpaceSupportOperationsPolicy	Neue verwaltete Richtlinie für die AWS-Support-Funktion in AWS re:Post Private	26. November 2023
Re:Post Private hat begonnen, Änderungen zu verfolgen	Re:Post Private hat damit begonnen, Änderungen für seine zu verfolgen AWS verwaltete Richtlinien	26. November 2023

Fehlerbehebung bei AWS Re:Post Private Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit re:Post Private und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion in Re:Post Private durchzuführen
- Ich bin nicht berechtigt, iam: auszuführenPassRole
- Ich möchte Leute außerhalb von mir zulassen AWS-Konto um auf meine Re:Post Private Ressourcen zuzugreifen

Ich bin nicht berechtigt, eine Aktion in Re:Post Private durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `repostPrivate:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 repostPrivate:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `repostPrivate:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam: auszuführenPassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, das auszuführen `iam:PassRole` In diesem Fall müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Re:Post Private übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine vorhandene Rolle an diesen Dienst zu übergeben, anstatt eine neue Dienstrolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer den Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in re:Post Private auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Leute außerhalb von mir zulassen AWS-Konto um auf meine Re:Post Private Ressourcen zuzugreifen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Ob re:Post Private diese Funktionen unterstützt, erfahren Sie unter So funktioniert re:Post Private mit IAM.
- Um zu erfahren, wie Sie überall Zugriff auf Ihre Ressourcen gewähren AWS-Konten die Sie besitzen, finden Sie Bereitstellung des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto das Sie besitzen in der IAM-Benutzerhandbuch.
- Um zu erfahren, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren AWS-Konten, siehe Bereitstellung des Zugangs zu AWS-Konten im Besitz von Dritten in der IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Überprüfung der Konformität für AWS re:Post Private

Unser neues AWS Das Anmeldeerlebnis ist nicht für regulierte Arbeitslasten konzipiert. Wenn Sie unser neues verwenden AWS Erfahrung mit der Registrierung, die Sie aber nutzen möchten AWS für regulierte Arbeitslasten können Sie melden Sie sich an für AWS (fortgeschritten) oder aktiviere erweiterte Funktionen für dein AWS Umwelt.

Um zu erfahren, ob ein AWS-Service fällt in den Geltungsbereich bestimmter Compliance-Programme, siehe AWS-Services im Geltungsbereich des Compliance-Programms und wählen Sie das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme.

Sie können Prüfberichte von Drittanbietern mithilfe von AWS Artifact. Weitere Informationen finden Sie unter Berichte werden heruntergeladen in AWS Artifact.

Ihre Compliance-Verantwortung bei der Verwendung AWS-Services hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens sowie den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Compliance-Verantwortung bei der Verwendung AWS-Services, siehe AWS Dokumentation zur Sicherheit.

Resilienz in AWS re:Post Private

Die AWS Die globale Infrastruktur basiert auf AWS-Regionen und Verfügbarkeitszonen. AWS-Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Für weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter AWS Weltweite Infrastruktur.

Infrastruktursicherheit in AWS re:Post Private

Als verwalteter Service ist AWS re:Post Private geschützt durch AWS globale Netzwerksicherheitsverfahren, die in der beschrieben werden Amazon Web Services: Überblick über Sicherheitsprozesse Whitepaper.

Du verwendest AWS veröffentlichte API-Aufrufe für den Zugriff auf Re:Post Private über das Netzwerk. Kunden müssen Transport Layer Security (TLS) 1.0 oder neuer unterstützen. Wir empfehlen TLS 1.2 oder neuer. Kunden müssen außerdem Verschlüsselungssammlungen mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral) unterstützen Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral) Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert werden, der einem AWS Identity and Access Management Schulleiter. Alternativ können Sie mit AWS -Security-Token-Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

re:POST Private Kontingente

AWS re:Post Private bietet private re:Posts, die Sie in Ihrem Konto in einer bestimmten Region verwenden können. AWS Wenn Sie sich für re:POST Private registrieren, werden Standardkontingente (früher als Limits bezeichnet) für die Anzahl der privaten re:Posts, die Sie erstellen können, und für die Größe der privaten re:Posts AWS festgelegt.

Servicekontingente

Im Folgenden sind die Standardkontingente für re:POST Private für dein Konto aufgeführt. AWS Sie können die Konsole Service Quotas verwenden, um das Standardkontingent anzuzeigen. Keines dieser Kontingente ist anpassbar. Sie können keine Erhöhung des Kontingents beantragen.

Ressource	Standard	Beschreibung	Einstellbar
Anzahl der privaten Re:Posts	3	Die maximale Anzahl privater re:Posts in diesem Konto in der aktuellen Region.	Nein
Größe der kostenlosen privaten Re:Post	10	Die maximale Größe (in GB) einer kostenlosen privaten Re:Post.	Nein
Standardgröße für private Re:Post	100	Die maximale Größe (in GB) einer standardmäßigen privaten Re:Post.	Nein

Grenzwerte für die API-Drosselung

Die folgenden Drosselungsgrenzen gelten pro Konto und Region in re:POST Private. Diese Kontingente können nicht erhöht werden.

Aktionen	Rate für das Nachfüllen von Tokens	Rate der Anforderungen	
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	

Erstellen, Konfigurieren und Anpassen Ihres privaten re:Post

In diesem Abschnitt wird erklärt, wie Sie Ihren privaten re:POST in der AWS re:POST Private-Konsole erstellen, konfigurieren und anpassen können.

Themen

- Erstellen eines neuen privaten re:Post
- Verwalten Sie den Zugriff auf Support Erstellung und Verwaltung von Fällen in Re:Post Private
- Richten Sie den Benutzerzugriff ein und verwalten Sie ihn mit AWS IAM Identity Center
- Passen Sie Ihren privaten Re:POST an
- Laden Sie Benutzer zu Ihrem privaten re:POST ein

Erstellen eines neuen privaten re:Post

Gehen Sie wie folgt vor, um einen neuen privaten Re:POST zu erstellen:

1. Öffne die private Re:POST-Konsole unter. https://console.aws.amazon.com/repost-private/
2. Wähle auf der Startseite der Konsole Create private Re:POST aus.
3. Wenn Sie IAM Identity Center noch nicht für Ihr Konto konfiguriert haben, wählen Sie Open Identity Center. Folgen Sie den Anweisungen unter Erste Schritte im AWS IAM Identity Center-Benutzerhandbuch.
4. Wählen Sie auf der Seite Create private Re:POST für die Preisgestaltung je nach Ihrem Anwendungsfall das kostenlose Kontingent oder das Standard-Kontingent aus. Wenn Sie das kostenlose Kontingent bereits für Ihr Konto genutzt haben, steht Ihnen die Option „Kostenloses Kontingent“ nicht zur Verfügung.
5. Gehen Sie unter Details wie folgt vor:

   Geben Sie unter Name einen eindeutigen Namen für Ihren privaten Re:POST ein.

   (Optional) Geben Sie unter Beschreibung eine kurze Beschreibung für Ihren privaten Re:POST ein.

   Geben Sie unter Benutzerdefinierte Subdomain einen benutzerdefinierten Namen für Ihre Subdomain ein.

6. (Optional) Um Ihre Datenverschlüsselungseinstellungen anzupassen, wählen Sie unter Datenverschlüsselung die Option Verschlüsselungseinstellungen anpassen aus. Führen Sie dann eine der folgenden Aktionen aus:

   Wählen Sie unter Wählen Sie einen AWS-KMS-Schlüssel einen AWS Key Management Service Schlüssel oder einen Amazon-Ressourcennamen (ARN) aus.

   –oder–

   Wählen Sie Einen AWS KMS-Schlüssel erstellen aus. Erstellen Sie dann den AWS KMS Schlüssel.

7. (Optional) Wählen Sie unter Servicezugriff für die Integration von Support-Anfragen die Option Servicezugriff für diesen Re:POST aktivieren aus.

   > **Note**
   >
   > Sie können diese Option auch aktivieren, nachdem Sie den privaten Re:POST erstellt haben.

   Wählen Sie unten eine vorhandene IAM-Rolle aus oder erstellen Sie eine neue Rolle in der IAM-Konsole. Verwenden Sie die Suchleiste, um Ihre vorhandene IAM-Rolle zu finden.

   –oder–

   Wählen Sie in der IAM-Konsole die Option „Neue Rolle erstellen“.

   Wenn Sie eine neue Rolle erstellen möchten, folgen Sie den Anweisungen unterErstellen einer IAM-Rolle.

   Wenn Sie eine vorhandene Servicerolle verwenden möchten, geben Sie in der Suchleiste den ARN der Rolle ein, die Sie verwenden möchten. Wählen Sie die Rolle aus der Dropdownliste aus.

   Weitere Informationen finden Sie unter Verwalten Sie den Zugriff auf Support Erstellung und Verwaltung von Fällen in Re:Post Private.

8. (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus. Geben Sie dann die folgenden Informationen ein:

   Geben Sie für Key Ihren benutzerdefinierten Tag-Schlüssel ein.

Geben Sie für Value Ihren benutzerdefinierten Tag-Wert ein.

Um weitere Tags hinzuzufügen, wählen Sie Neues Tag hinzufügen aus.

9. Wähle Create this re:POST.

Auf einer Bestätigungsseite wirst du darüber informiert, dass dein privater Re:POST erstellt wird. Du kannst den Status des privaten Re:Post im Feld Status einsehen. Wenn dein privater Re:POST erstellt wurde, wird im Feld Status der Eintrag Creating angezeigt.

Es dauert ungefähr 30 Minuten, bis der private Re:POST erstellt wird. Wenn dein privater Re:POST bereit ist, wird im Statusfeld Online angezeigt. Sie können die von AWS generierte Subdomain für Ihren privaten re:POST verwenden, die auf der Registerkarte „Einstellungen“ aufgeführt ist, um auf Ihren privaten re:POST zuzugreifen. Nach Abschluss der Überprüfung können Sie die benutzerdefinierte Subdomain für Ihren privaten re:POST auf der Registerkarte „Einstellungen“ einsehen.

> **Note**
>
> Ab dem 18. April 2025 unterstützen alle neuen Re:Post Private-Instances Dual-Stack-Netzwerke mit IPv4- und IPv6-Konnektivität.

Verwalten Sie den Zugriff auf Support Erstellung und Verwaltung von Fällen in Re:Post Private

Sie müssen eine AWS Identity and Access Management (IAM-) Rolle erstellen, um den Zugriff auf die Erstellung und Verwaltung von Kundenvorgängen von AWS re:Post Private aus zu Support verwalten. Diese Rolle führt die folgenden Support Aktionen für Sie aus:

- CreateCase
- AddCommunicationToCase
- ResolveCase

Nachdem Sie die IAM-Rolle erstellt haben, fügen Sie dieser Rolle eine IAM-Richtlinie hinzu, sodass die Rolle über die erforderlichen Berechtigungen zum Ausführen dieser Aktionen verfügt. Sie wählen diese Rolle, wenn Sie Ihren privaten re:POST in der Re:POST Private-Konsole erstellen.

Nutzer in deinem privaten re:POST haben dieselben Berechtigungen, die du der IAM-Rolle gewährst.

> **Important**
>
> Wenn Sie die IAM-Rolle oder die IAM-Richtlinie ändern, gelten Ihre Änderungen für den privaten Re:POST, den Sie konfiguriert haben.

Befolgen Sie diese Verfahren, um Ihre IAM-Rolle und -Richtlinie zu erstellen.

Themen

- Verwenden Sie eine AWS verwaltete Richtlinie oder erstellen Sie eine vom Kunden verwaltete Richtlinie
- Beispiel für eine IAM-Richtlinie
- Erstellen einer IAM-Rolle
- Fehlerbehebung

Verwenden Sie eine AWS verwaltete Richtlinie oder erstellen Sie eine vom Kunden verwaltete Richtlinie

Um Ihre Rollenberechtigungen zu gewähren, können Sie entweder eine AWS verwaltete Richtlinie oder eine vom Kunden verwaltete Richtlinie verwenden.

> **Tip**
>
> Wenn Sie eine Richtlinie nicht manuell erstellen möchten, empfehlen wir, stattdessen eine AWS verwaltete Richtlinie zu verwenden und dieses Verfahren zu überspringen. Verwaltete Richtlinien verfügen automatisch über die erforderlichen Berechtigungen für Support. Sie müssen die Richtlinien nicht manuell aktualisieren. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AWSRepostSpaceSupportOperationsPolicy.

Gehen Sie wie folgt vor, um eine vom Kunden verwaltete Richtlinie für Ihre Rolle zu erstellen. Dieses Verfahren verwendet den JSON-Richtlinieneditor in der IAM-Konsole.

Um eine vom Kunden verwaltete Richtlinie für Re:Post Private zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter. https://console.aws.amazon.com/iam/
2. Wählen Sie im Navigationsbereich Richtlinien.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie den Tab JSON.
5. Geben Sie Ihren JSON ein und ersetzen Sie dann den Standard-JSON im Editor. Sie können die Beispielrichtlinie verwenden.
6. Wählen Sie Next: Markierungen (Weiter: Markierungen).
7. (Optional) Sie können Tags als Schlüssel-Wert-Paare verwenden, um der Richtlinie Metadaten hinzuzufügen.
8. Wählen Sie Weiter: Prüfen aus.
9. Geben Sie auf der Seite Review policy (Richtlinie überprüfen) einen Name (Namen), z. B. *rePostPrivateSupportPolicy*, und eine Description (Beschreibung) (optional) ein.
10. Sehen Sie auf der Übersichtsseite nach, welche Berechtigungen die Richtlinie zulässt, und wählen Sie dann Richtlinie erstellen aus.

Diese Richtlinie definiert die Aktionen, die die Rolle ausführen kann. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Beispiel für eine IAM-Richtlinie

Sie können die folgende Beispielrichtlinie Ihrer IAM-Rolle anfügen. Diese Richtlinie gewährt der Rolle volle Berechtigungen für alle erforderlichen Aktionen für Support. Nachdem Sie einen privaten re:POST mit der Rolle konfiguriert haben, hat jeder Benutzer in Ihrem privaten re:POST dieselben Berechtigungen.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Sid": "RepostSpaceSupportOperations",
   "Effect": "Allow",
```

```
    "Action": [
     "support:AddAttachmentsToSet",
     "support:AddCommunicationToCase",
     "support:CreateCase",
     "support:DescribeCases",
     "support:DescribeCommunications",
     "support:ResolveCase"
    ],
    "Resource": "*"
   }
  ]
}
```

> **Note**
>
> Eine Liste der AWS verwalteten Richtlinien für re:POST Private finden Sie unter. AWS verwaltete Richtlinien für AWS re:Post Private

Sie können die Richtlinie aktualisieren, um eine Genehmigung von zu entfernen. Support

Beschreibungen der einzelnen Aktionen finden Sie in den folgenden Themen in der Service-Autorisierungsreferenz:

- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Support
- Aktionen, Ressourcen und Bedingungsschlüssel für Service Quotas
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Identity and Access Management

Erstellen einer IAM-Rolle

Nachdem Sie die Richtlinie erstellt haben, müssen Sie eine IAM-Rolle erstellen und die Richtlinie dann dieser Rolle anfügen. Sie wählen diese Rolle, wenn Sie in der Re:POST Private-Konsole einen privaten re:POST erstellen.

Um eine Rolle zu erstellen für Support Erstellung und Verwaltung von Fällen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.

2. Wählen Sie im Navigationsbereich Rollen und dann Rolle erstellen.
3. Für Trusted entity type (Vertrauenstyp der Entität), wählen Sie Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie).
4. Geben Sie unter Benutzerdefinierte Vertrauensrichtlinie Folgendes ein:

   JSON

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

5. Wählen Sie Weiter aus.
6. Geben Sie in der Suchleiste unter Zugriffsrichtlinien die AWS verwaltete Richtlinie oder eine vom Kunden verwaltete Richtlinie ein, die Sie erstellt haben, z. *rePostPrivateSupportPolicy* B. Aktivieren Sie das Kontrollkästchen neben den Berechtigungsrichtlinien, die der Dienst haben soll.
7. Wählen Sie Weiter aus.
8. Geben Sie auf der Seite Name, überprüfen und erstellen unter Rollenname einen Namen ein, z. *rePostPrivateSupportRole* B.
9. (Optional) Geben Sie unter Beschreibung eine Beschreibung für die neue Rolle ein.
10. Überprüfen Sie die Vertrauensrichtlinie und die Berechtigungen.
11. (Optional) Sie können Tags als Schlüssel-Wert-Paare verwenden, um der Rolle Metadaten hinzuzufügen. Weitere Informationen dazu, wie Sie verwenden können von Tags mit IAM finden Sie unter Tagging von Amazon RDSIAM-Ressourcen.

12. Wählen Sie Rolle erstellen aus. Sie können diese Rolle jetzt auswählen, wenn Sie einen privaten re:POST in der Re:POST Private-Konsole konfigurieren. Siehe Erstellen eines neuen privaten re:Post.

Weitere Informationen finden Sie unter Erstellen einer Rolle für einen AWS Dienst (Konsole) im IAM-Benutzerhandbuch.

Fehlerbehebung

Informationen zur Verwaltung des Zugriffs auf re:Post Private finden Sie in den folgenden Themen.

Inhalt

- Ich möchte bestimmte Benutzer in meinem privaten Re:POST von bestimmten Aktionen ausschließen
- Wenn ich einen privaten Re:POST konfiguriere, sehe ich die von mir erstellte IAM-Rolle nicht
- Meiner IAM-Rolle fehlt eine Berechtigung
- Ein Fehler besagt, dass meine IAM-Rolle nicht gültig ist

Ich möchte bestimmte Benutzer in meinem privaten Re:POST von bestimmten Aktionen ausschließen

Standardmäßig verfügen Benutzer in Ihrem privaten Re:POST über dieselben Berechtigungen, die in der IAM-Richtlinie festgelegt sind, die Sie der von Ihnen erstellten IAM-Rolle zuordnen. Das bedeutet, dass jeder im privaten re:POST Lese- oder Schreibzugriff hat, um Support Fälle zu erstellen und zu verwalten, unabhängig davon, ob er einen oder einen IAM-Benutzer hat oder nicht. AWS-Konto

Wir empfehlen Ihnen, die folgenden bewährten Methoden:

- Verwenden Sie eine IAM-Richtlinie, die über die erforderlichen Mindestberechtigungen für die verfügt. Support Siehe AWS verwaltete Richtlinie: AWSRepostSpaceSupportOperationsPolicy.

Wenn ich einen privaten Re:POST konfiguriere, sehe ich die von mir erstellte IAM-Rolle nicht

Wenn Ihre IAM-Rolle nicht in der Liste „IAM-Rolle für re:Post Private;“ erscheint, bedeutet das, dass die Rolle nicht über re:Post Private als vertrauenswürdige Entität verfügt oder dass die Rolle gelöscht

wurde. Sie können die vorhandene Rolle aktualisieren oder eine neue erstellen. Siehe Erstellen einer IAM-Rolle.

Meiner IAM-Rolle fehlt eine Berechtigung

Die IAM-Rolle, die du für deinen privaten Re:POST erstellst, benötigt Berechtigungen, um die gewünschten Aktionen ausführen zu können. Wenn Sie beispielsweise möchten, dass Ihre Benutzer im privaten re:POST Support-Anfragen erstellen, muss die Rolle über die `support:CreateCase` entsprechende Berechtigung verfügen. re:Post Private übernimmt diese Rolle, um diese Aktionen für Sie auszuführen.

Wenn Sie eine Fehlermeldung bezüglich einer fehlenden Berechtigung für erhalten Support, überprüfen Sie, ob die Ihrer Rolle zugeordnete Richtlinie über die erforderliche Berechtigung verfügt.

Lesen Sie das vorhergehende Beispiel für eine IAM-Richtlinie.

Ein Fehler besagt, dass meine IAM-Rolle nicht gültig ist

Vergewissern Sie sich, dass Sie die richtige Rolle für Ihre private Re:POST-Konfiguration ausgewählt haben.

Richten Sie den Benutzerzugriff ein und verwalten Sie ihn mit AWS IAM Identity Center

Re:Post Private lässt sich mit AWS IAM Identity Center integrieren und bietet so einen Identitätsverbund für die Belegschaft Ihres Unternehmens. Verwenden Sie IAM Identity Center, um Benutzer aus Ihrem Unternehmen zu erstellen oder zu verbinden und ihren Zugriff auf alle AWS Konten und Anwendungen zentral zu verwalten. Weitere Informationen zu IAM Identity Center finden Sie unter Was ist AWS IAM Identity Center (Nachfolger von AWS Single). Sign-On Weitere Informationen zu den ersten Schritten mit IAM Identity Center finden Sie unter Erste Schritte. Um IAM Identity Center verwenden zu können, müssen Sie es auch für das AWS Organizations Konto aktiviert haben.

Passen Sie Ihren privaten Re:POST an

Du kannst deinem privaten Re:POST einen oder mehrere Administratoren hinzufügen, nachdem du ihn erstellt hast. Administratoren verwenden die Re:Post Private-Anwendung, um den privaten Re:POST zu starten und die Benutzer darin zu verwalten. Sie können das Branding für den privaten

Re:post anpassen, Tags hinzufügen, um Inhalte zu klassifizieren, und Themen auswählen, die für das automatische Auffüllen von Inhalten von Interesse sind. Weitere Informationen finden Sie im AWS re:Post Private Administration Guide.

Laden Sie Benutzer zu Ihrem privaten re:POST ein

Du kannst deinem privaten Re:POST einen oder mehrere Nutzer hinzufügen, nachdem du ihn erstellt hast. Du kannst Nutzer zur Zusammenarbeit in deinem privaten re:POST einladen. Benutzer verwenden die Re:Post Private-Anwendung, um sich mit den von Ihnen konfigurierten Anmeldeinformationen anzumelden. Nach der Anmeldung bei einem privaten re:POST können Benutzer vorhandene Inhalte durchsuchen oder durchsuchen, einschließlich maßgeschneiderter Schulungen und technischer Inhalte, die auf ihre Interessengebiete zugeschnitten sind. Weitere Informationen finden Sie im AWS re:Post Private User Guide.

Verwalte deinen privaten re:POST in der Re:Post Private-Konsole

In diesem Abschnitt wird erklärt, wie Sie Ihren privaten re:POST in der AWS re:POST Private-Konsole verwalten können.

Themen

- Fügen Sie Benutzer zu Ihrem privaten re:POST hinzu
- Füge Gruppen zu deinem privaten re:POST hinzu
- Füge Nutzer zu einer Gruppe in deinem privaten re:Post hinzu
- Laden Sie Benutzer und Gruppen zu Ihrem privaten re:Post ein
- Weist einem Nutzer in deinem privaten re:Post eine Rolle zu
- Entferne Benutzer aus deinem privaten re:Post
- Entferne Gruppen aus deinem privaten re:Post
- Füge einen AWS Mitarbeiter zu deinem privaten re:Post hinzu oder entferne ihn
- Erstelle einen neuen Channel in deinem privaten re:Post
- Verwalte Benutzer und Gruppen in deinem Kanal
- Lösche deinen privaten re:Post

Fügen Sie Benutzer zu Ihrem privaten re:POST hinzu

Wenn Sie ein Administrator sind, können Sie Benutzer zu Ihrem privaten re:POST hinzufügen.

1. Öffnen Sie die private re:POST-Konsole unter. https://console.aws.amazon.com/repost-private/
2. Wählen Sie im Navigationsbereich All my private re:Posts aus.
3. Wähle den privaten re:Post aus, den du verwalten möchtest.
4. Wählen Sie die Registerkarte Users.
5. Wähle unter Benutzer die Option Benutzer und Gruppen hinzufügen aus.
6. Wählen Sie aus der Liste die Benutzer aus, die Sie zu Ihrem privaten re:Post hinzufügen möchten. Wähle dann Zuweisen.

Die ausgewählten Benutzer werden zu deinem privaten re:POST hinzugefügt und im Tab Benutzer aufgeführt.

Die Nutzer, die du hinzugefügt hast, erhalten eine Onboarding-E-Mail von deinem privaten re:Post. Ihr privater re:POST überprüft die Liste der Benutzer und Gruppen einmal täglich, um sicherzustellen, dass eine Onboarding-E-Mail an diejenigen gesendet wird, die noch keine erhalten haben. Die Onboarding-E-Mail enthält Informationen darüber, wie Sie sich bei Ihrem privaten re:POST anmelden können.

Füge Gruppen zu deinem privaten re:POST hinzu

Wenn Sie ein Administrator sind, können Sie Gruppen zu Ihrem privaten re:POST hinzufügen.

1. Öffnen Sie die re:POST-Private-Konsole unter. https://console.aws.amazon.com/repost-private/
2. Wählen Sie im Navigationsbereich All my private re:Posts aus.
3. Wähle den privaten re:Post aus, den du verwalten möchtest.
4. Wählen Sie die Registerkarte Groups (Gruppen).
5. Wähle Benutzer und Gruppen hinzufügen.
6. Wähle aus der Liste die Gruppen aus, die du zu deinem privaten re:Post hinzufügen möchtest. Wähle dann Zuweisen.

Die ausgewählten Gruppen werden zu deinem privaten re:POST hinzugefügt und im Tab Gruppen aufgeführt.

Die Gruppen, die du hinzugefügt hast, erhalten eine Onboarding-E-Mail von deinem privaten re:Post. Ihr privater re:POST überprüft die Liste der Benutzer und Gruppen einmal täglich, um sicherzustellen, dass eine Onboarding-E-Mail an diejenigen gesendet wird, die noch keine erhalten haben. Die Onboarding-E-Mail enthält Informationen darüber, wie Sie sich bei Ihrem privaten re:POST anmelden können.

Füge Nutzer zu einer Gruppe in deinem privaten re:Post hinzu

Verwenden Sie IAM Identity Center, um neue Benutzer zu einer bestehenden Gruppe in Ihrem privaten re:POST hinzuzufügen. Weitere Informationen finden Sie unter Hinzufügen von Benutzern zu Gruppen im AWS IAM Identity Center-Benutzerhandbuch.

Laden Sie Benutzer und Gruppen zu Ihrem privaten re:Post ein

> **Note**
>
> Das Einladen von Benutzern und Gruppen zu deinem privaten re:POST ist optional. Die Benutzer und Gruppen, die du hinzugefügt hast, erhalten eine Onboarding-E-Mail von deinem privaten re:Post. Ihr privater re:POST überprüft die Liste der Benutzer und Gruppen einmal täglich, um sicherzustellen, dass eine Onboarding-E-Mail an diejenigen gesendet wird, die noch keine erhalten haben.

Gehen Sie wie folgt vor, um Benutzer und Gruppen manuell zu Ihrem privaten re:POST in AWS re:Post Private einzuladen:

1. Öffnen Sie die re:POST Private Konsole unter. https://console.aws.amazon.com/repost-private/
2. Wählen Sie im Navigationsbereich All my private re:Posts aus.
3. Wähle den privaten re:Post aus, den du verwalten möchtest.
4. Um Nutzer zu deinem privaten re:POST einzuladen, wähle den Tab Benutzer.

   Wähle aus der Liste die Nutzer aus, die du zu deinem privaten re:Post einladen möchtest. Wähle dann Onboard users to re:POST aus.
5. Geben Sie im Dialogfeld „Benutzer in diesen privaten re:POST einbinden“ die folgenden Informationen ein:

   Geben Sie unter Betreff den Betreff der E-Mail-Nachricht ein, die Sie senden.

   Geben Sie im Feld Text eine Willkommensnachricht für Ihren privaten re:Post ein.

   Wähle Onboarding-E-Mail senden.
6. Um Gruppen zu deinem privaten re:POST einzuladen, wähle den Tab Gruppen.

   Wähle aus der Liste die Gruppen aus, die du zu deinem privaten re:Post einladen möchtest. Wähle dann Onboard groups to re:POST aus.
7. Gib im Dialogfeld Gruppen in diesen privaten re:POST einbinden die folgenden Informationen ein:

   Geben Sie unter Betreff den Betreff der E-Mail-Nachricht ein, die Sie senden.

   Geben Sie im Feld Text eine Willkommensnachricht für Ihren privaten re:Post ein.

Wähle Onboarding-E-Mail senden.

Die Willkommensnachricht wird an alle ausgewählten Benutzer und Gruppen mit Informationen darüber gesendet, wie Sie sich bei Ihrem privaten re:Post anmelden können.

Weist einem Nutzer in deinem privaten re:Post eine Rolle zu

Sie können Ihren privaten re:POST-Benutzern eine der folgenden Berechtigungen zuweisen:

- Administrator: Ein Benutzer, der berechtigt ist, die Konfiguration Ihres privaten re:POST zu ändern
- Experte: Ein Benutzer, der berechtigt ist, die von der Community bereitgestellten Antworten zu überprüfen und zu validieren
- Moderator: Ein Benutzer, der auf Anfragen in der Moderationswarteschlange antworten kann
- Support-Anforderer: Ein Benutzer, der Tickets für die Support von ihm gestellten Fragen erstellen kann

Gehen Sie wie folgt vor, um Ihrem privaten re:POST-Benutzer eine Rolle zuzuweisen:

1. Öffnen Sie die re:POST Private Konsole unter. https://console.aws.amazon.com/repost-private/
2. Wählen Sie im Navigationsbereich All my private re:Posts aus.
3. Wähle den privaten re:Post aus, den du verwalten möchtest.
4. Wählen Sie die Registerkarte Users.
5. Wählen Sie einen oder mehrere Benutzer aus, denen Sie die Rollen zuweisen möchten.
6. Wählen Sie Rolle bearbeiten und wählen Sie dann die Rolle aus, die Sie den ausgewählten Benutzern zuweisen möchten.

Den ausgewählten Benutzern wird die Rolle zugewiesen, die Sie ausgewählt haben. Auf der Registerkarte Benutzer wird die Rolle für diese Benutzer auf die Rolle aktualisiert, die Sie ausgewählt haben.

Entferne Benutzer aus deinem privaten re:Post

Wenn Sie ein Administrator sind, können Sie Benutzer aus Ihrem privaten re:POST entfernen.

1. Öffnen Sie die private re:POST-Konsole unter. https://console.aws.amazon.com/repost-private/
2. Wählen Sie im Navigationsbereich All my private re:Posts aus.
3. Wähle den privaten re:Post aus, den du verwalten möchtest.
4. Wähle unter Nutzer aus der Liste die Nutzer aus, die du aus deinem privaten re:Post entfernen möchtest. Wählen Sie dann Entfernen aus.

Die ausgewählten Benutzer werden aus deinem privaten re:Post entfernt. Informationen zu den entfernten Benutzern werden nicht mehr auf der Registerkarte Benutzer angezeigt.

Entferne Gruppen aus deinem privaten re:Post

Wenn Sie ein Administrator sind, können Sie Gruppen aus Ihrem privaten re:POST entfernen.

1. Öffnen Sie die re:POST-Private-Konsole unter. https://console.aws.amazon.com/repost-private/
2. Wählen Sie im Navigationsbereich All my private re:Posts aus.
3. Wähle den privaten re:Post aus, den du verwalten möchtest.
4. Wählen Sie die Registerkarte Groups (Gruppen).
5. Wähle aus der Liste die Gruppen aus, die du aus deinem privaten re:POST entfernen möchtest. Wähle dann Entfernen.

Die ausgewählten Gruppen werden aus deinem privaten re:Post entfernt. Informationen zu den entfernten Gruppen werden nicht mehr unter dem Tab Gruppen angezeigt.

Füge einen AWS Mitarbeiter zu deinem privaten re:Post hinzu oder entferne ihn

Wenn du einen Enterprise- oder Enterprise On-Ramp-Supportplan hast, kannst du einen AWS Mitarbeiter zu deinem privaten re:Post hinzufügen oder daraus entfernen. Weitere Informationen erhalten Sie vom Concierge-Support oder Ihrem Technical Account Manager (TAM).

Erstelle einen neuen Channel in deinem privaten re:Post

Du kannst Kanäle in deinem privaten re:POST erstellen, um Inhalte gezielt zu teilen, die Organisation zu verbessern, den Datenschutz zu verbessern und die Rechteverwaltung zu vereinfachen. Kanäle sind spezielle private Bereiche in deinem privaten re:POST und helfen dir dabei, den

Zugriff auf Inhalte detailliert zu kontrollieren. Mit dieser Funktion können Sie den Zugriff für bestimmte Benutzer oder Gruppen verwalten, indem Sie ihn an Ihre Organisationsstruktur und Ihre Geschäftsanforderungen anpassen.

Gehen Sie wie folgt vor, um in Ihrem privaten re:Post in AWS re:Post Private einen Channel zu erstellen:

1. Öffnen Sie die re:POST Private-Konsole unter. https://console.aws.amazon.com/repost-private/
2. Wählen Sie im Navigationsbereich All my private re:Posts aus.
3. Wähle den privaten re:Post aus, den du verwalten möchtest, und wähle dann den Tab Kanäle.
4. Wählen Sie Create channel (Channel erstellen).
5. Geben Sie unter Channel name (Channelname) einen Namen für Ihren Channel ein.
6. Gib unter Kanalbeschreibung eine kurze Beschreibung deines Kanals ein.
7. Wählen Sie Erstellen aus.

Ihr Kanal wird erstellt und unter der Kanalliste angezeigt.

> **Note**
>
> Um den Kanalnamen oder die Kanalbeschreibung zu aktualisieren, wähle Kanal bearbeiten.

Verwalte Benutzer und Gruppen in deinem Kanal

> **Note**
>
> Du kannst nur bestehende Nutzer und Gruppen aus deinem privaten re:POST zu deinen Kanälen hinzufügen.

Um deinem Kanal innerhalb deines privaten re:POSTs Nutzer oder Gruppen hinzuzufügen, gehe wie folgt vor:

1. Öffne die re:POST Private Konsole unter. https://console.aws.amazon.com/repost-private/
2. Wählen Sie im Navigationsbereich All my private re:Posts aus.
3. Wähle den privaten re:Post aus, den du verwalten möchtest, und wähle dann den Tab Kanäle.

4. Wähle den Kanal aus, zu dem du die Benutzer oder Gruppen hinzufügen möchtest.
5. Wähle Benutzer verwalten.

   Du siehst die Liste aller Benutzer und Gruppen in deinem privaten re:Post.
6. Wähle einen oder mehrere Benutzer und Gruppen aus, die du dem Kanal hinzufügen möchtest.
7. Wähle Zum Kanal hinzufügen.

   Die Benutzer und Gruppen, die Sie ausgewählt haben, werden dem Kanal hinzugefügt.

   Sie können den aktualisierten Status der Benutzer und Gruppen in der Spalte Status sehen.
8. Klicken Sie auf Schließen.

> **Note**
>
> Du kannst deinem Kanal keinen Benutzer oder keine Gruppe als Administrator zuweisen.

Um Nutzer oder Gruppen innerhalb deines privaten re:POSTs aus deinem Kanal zu entfernen, befolge diese Schritte:

1. Wählen Sie die Registerkarte Channels aus.
2. Wähle den Kanal aus, aus dem du die Benutzer oder Gruppen entfernen möchtest.
3. Wähle Benutzer verwalten.

   Du siehst die Liste aller Benutzer und Gruppen in deinem Kanal.
4. Wähle einen oder mehrere Benutzer und Gruppen aus, die du aus dem Kanal entfernen möchtest.
5. Wähle Aus Kanal entfernen.

   Die Benutzer und Gruppen, die Sie ausgewählt haben, werden aus dem Kanal entfernt.

   Sie können den aktualisierten Status der Benutzer und Gruppen in der Spalte Status sehen.
6. Klicken Sie auf Schließen.

Ein Benutzer oder eine Gruppe, die du aus deinem Kanal entfernst, wird nicht aus deinem privaten re:Post entfernt. Ein Benutzer oder eine Gruppe, die du aus deinem privaten re:Post entfernst, wird aus allen Kanälen innerhalb dieses privaten re:Posts entfernt.

Gehen Sie wie folgt vor, um die Rollen eines oder mehrerer Benutzer oder Gruppen in Ihrem Kanal zu bearbeiten:

1. Wählen Sie die Registerkarte Channels aus.
2. Wähle den Kanal aus, in dem du die Rollen der Benutzer oder Gruppen bearbeiten möchtest.
3. Wähle Benutzer verwalten.

   Du siehst die Liste aller Benutzer und Gruppen in deinem Kanal.
4. Wähle einen oder mehrere Benutzer und Gruppen aus, für die du die Rollen bearbeiten möchtest.
5. Wählen Sie Rolle bearbeiten.
6. Wählen Sie die gewünschte Option aus.

   Mit den verfügbaren Optionen kannst du deinen Kanalbenutzer oder deine Gruppe zu einem Experten, Moderator oder Support-Anforderer machen. Sie können diese Rollen auch aus Ihren Benutzern oder Gruppen entfernen. Weitere Informationen zu diesen Rollen finden Sie unterWeist einem Nutzer in deinem privaten re:Post eine Rolle zu.

   Sie können die aktualisierten Rollen für die Benutzer und Gruppen in der Spalte Rollen sehen.
7. Klicken Sie auf Schließen.

Du kannst die Rollen für Benutzer oder Gruppen innerhalb eines Channels so einstellen, dass sie sich von denen in deinem privaten re:Post unterscheiden.

Lösche deinen privaten re:Post

Gehen Sie wie folgt vor, um einen privaten re:Post in AWS re:Post Private zu löschen:

1. Öffnen Sie die re:POST Private-Konsole unter. https://console.aws.amazon.com/repost-private/
2. Wählen Sie im Navigationsbereich All my private re:Posts aus.
3. Wählen Sie den privaten re:Post aus, den Sie verwalten möchten, und wählen Sie dann Löschen.
4. Wähle alle Optionen aus, um zu bestätigen, dass du den privaten re:POST und die damit verknüpften Daten dauerhaft löschen möchtest.

> **Important**
>
> Wenn du den privaten re:POST löschst, werden alle Konfigurationsinformationen, die sich auf den privaten re:Post beziehen, gelöscht. Nachdem der private re:Post gelöscht wurde, kannst du keine Inhalte mehr daraus wiederherstellen.

5. Gib den Namen deines privaten re:POSTs ein, wenn du um eine zusätzliche schriftliche Zustimmung gebeten wirst. Wählen Sie dann Löschen aus.

Es dauert ungefähr 30 Minuten, bis dein privater re:POST gelöscht ist.

Überwachung von AWS re:Post Private

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Re:Post Private und Ihren anderen Lösungen. AWS AWS bietet die folgenden Überwachungstools, um re:POST Private anzusehen, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die CPU-Auslastung oder andere Messwerte Ihrer Amazon EC2-Instances CloudWatch verfolgen lassen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder für Sie getätigt wurden, AWS-Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Überwachung von AWS Re:Post Private mit Amazon CloudWatch

Sie können AWS Re:Post Private mithilfe von Amazon überwachen CloudWatch, das Rohdaten sammelt und sie zu lesbaren Metriken verarbeitet, die nahezu in Echtzeit sind. Diese Statistiken werden 15 Monate lang aufbewahrt, sodass Sie auf historische Informationen zugreifen und sich einen besseren Überblick über die Leistung Ihrer Webanwendung oder Ihres Services verschaffen können. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Der Re:Post Private-Service meldet die folgenden Metriken im `AWS/rePostPrivate` Namespace.

Metrik	Description
`NumberOfSpaces`	Die Anzahl der privaten Re:Posts im aktuellen Konto.

Metrik	Description
	Einheiten: Anzahl
`NumberOfUsers`	Die Anzahl der Nutzer in einem privaten Re:POST. Diese Metrik verwendet SpaceID als Dimension. Einheiten: Anzahl
`ContentSize`	Die Menge an Inhalten in einem privaten Re:Post. Diese Metrik verwendet SpaceID als Dimension. Einheiten: Byte

Die folgenden Dimensionen werden für die Re:Post Private-Metriken unterstützt.

Dimension	Description
`spaceId`	Die eindeutige Kennung für den privaten Re:POST.

Protokollierung von AWS re:POST Private API-Aufrufen mit AWS CloudTrail

AWS re:Post Private ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Service in re:Post Private durchgeführten Aktionen bereitstellt. CloudTrail erfasst alle API-Aufrufe für re:Post Private als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Re:Post Private-Konsole und Codeaufrufe an die Re:Post Private API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übertragung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für re:Post Private. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Event-Verlauf einsehen. Anhand der gesammelten Informationen können Sie ermitteln CloudTrail, welche Anfrage an re:POST Private gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde und weitere Details.

Weitere Informationen dazu finden CloudTrail Sie im AWS CloudTrail Benutzerhandbuch.

Re:Veröffentlichen Sie private Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in Re:Post Private eine Aktivität stattfindet, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Eventverlauf in einem Ereignis aufgezeichnet. Sie können die letzten Ereignisse in Ihrem ansehen, suchen und herunterladen. AWS-Konto Weitere Informationen finden Sie unter Arbeiten mit dem CloudTrail Eventverlauf.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem Konto AWS-Konto, einschließlich der Ereignisse für Re:Post Private, erstellen Sie einen Trail. Ein Trail ermöglicht die Übermittlung CloudTrail von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Erstellen eines Trails für Ihr AWS-Konto
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle re:POST Private-Aktionen werden von der AWS re:Post Private API-Referenz protokolliert CloudTrail und sind darin dokumentiert. re:POST Private unterstützt die Protokollierung der folgenden Aktionen als Ereignisse in Protokolldateien: CloudTrail

- CreateSpace
- DeleteSpace
- DeregisterAdmin
- GetSpace
- ListSpaces
- ListTagsForResource
- RegisterAdmin
- SendInvites

- TagResource
- UntagResource
- UpdateSpace

re:Post Private unterstützt das Protokollieren der folgenden Support Aktionen als Ereignisse in den Protokolldateien: CloudTrail

- CreateCase
- AddCommunicationToCase
- ResolveCase

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldeinformationen gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu den privaten Re:POST-Logdateieinträgen

Ein Trail ist eine Konfiguration, die die Übermittlung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Logdateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, daher erscheinen sie in keiner bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail Logeintrag, der die `CreateSpace` Aktion demonstriert.

```
{
   "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"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `RegisterAdmin` Aktion veranschaulicht.

```
{
   "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"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ListSpaces` Aktion veranschaulicht.

```
 {
    "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"
}
```


Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ResolveCase` Aktion veranschaulicht. Sie können das `sourceIdentity` Element in diesem Protokolleintrag verwenden, um den Benutzer zu identifizieren, der den Fall gelöst hat.


```
 {
    "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"
    }
}
```

Problembehebung bei re:POST Private

Die folgenden Informationen können Ihnen bei der Behebung von Problemen mit AWS re:Post Private helfen.

Themen

- Ich kann meinen privaten re:POST nicht in einer bestimmten Region einrichten AWS
- Ich kann privaten re:POST nicht in meinem Konto einrichten
- Benutzer oder Gruppen können in einem privaten re:POST nicht verwaltet werden

Ich kann meinen privaten re:POST nicht in einer bestimmten Region einrichten AWS

re:POST Private ist nur in den Regionen USA Ost (Nord-Virginia), USA West (Oregon), Europa (Frankfurt), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Kanada (Zentral) und Europa (Irland) verfügbar. Vergewissere dich, dass du deinen privaten re:POST in einer dieser Regionen erstellst.

Ich kann privaten re:POST nicht in meinem Konto einrichten

Stellen Sie sicher, dass Sie das AWS IAM Identity Center für Ihr Konto aktiviert und das IAM Identity Center in derselben Region eingerichtet haben, in der Sie den privaten re:POST erstellen möchten. Weitere Informationen finden Sie unter Voraussetzungen.

Benutzer oder Gruppen können in einem privaten re:POST nicht verwaltet werden

Vergewissere dich, dass du über die erforderlichen Rechte verfügst, um einen privaten re:Post zu bearbeiten und Benutzer und Gruppen innerhalb des privaten re:Post zu verwalten. Weitere Informationen finden Sie unter Beispiele für auf der privaten Identität basierende Richtlinien von AWS Re:Post.

Dokumentverlauf

In der folgenden Tabelle werden die Dokumentationsversionen für AWS re:Post Private beschrieben:

Änderung	Beschreibung	Datum
Mitteilung zum Ende des Supports	Hinweis zum Ende des Supports: Am 30. Juni 2027 AWS wird der Support für AWS re:Post Private eingestellt. Nach dem 30. Juni 2027 werden Sie nicht mehr auf die Re:Post Private-Konsole oder die Ressourcen von Re:Post Private zugreifen können. Weitere Informationen finden Sie unter Ende des Supports für AWS re:Post Private.	30. Juni 2026
Aktualisieren	Es wurden Anweisungen zum Hinzufügen eines Kanals und zum Verwalten von Benutzern innerhalb eines Kanals hinzugefügt	3. Juli 2025
Aktualisieren	Informationen zur Unterstützung von IPv6-Konnektivität	18. April 2025
Aktualisieren	Es wurden Anweisungen für das automatische Onboarding von Benutzern und eine verbesserte Inhaltsmoderation hinzugefügt	22. Oktober 2024
Aktualisieren	Die Anweisungen zum Zuweisen von Rollen zu Benutzern wurden aus dem	9. Oktober 2024

	Administratorhandbuch in das Administratorhandbuch für die Konsole verschoben	
Überprüfung und Verbesserung der Struktur des Leitfadens	Die Struktur des Leitfadens wurde überprüft und Verbesserungen vorgenommen, um das Kundenerlebnis bei der Suche nach Informationen für bestimmte Szenarien zu verbessern.	24. September 2024
Aktualisieren	USA Ost (Nord-Virginia), Asien-Pazifik (Sydney), Kanada (Zentral) und Europa (Irland) zu den unterstützten Regionen hinzugefügt	10. Mai 2024
Aktualisieren	Asien-Pazifik (Singapur) zu den unterstützten Regionen hinzugefügt	6. März 2024
Aktualisieren	Es wurden Informationen hinzugefügt, die darauf hinweisen, dass re:Post Private nur Organisationsinstanzen von IAM Identity Center unterstützt	16. Januar 2024
Neue Ressourcen	Dokumentation für von AWS verwaltete Richtlinien für AWS re:Post Private hinzugefügt	26. November 2023
Erstversion	Erste Veröffentlichung des Verwaltungsleitfadens für die re:POST Private Console	26. November 2023