Administratorhandbuch für die Konsole

AWS re:Post Private

AWS re:Post Private: Administratorhandbuch für die Konsole

Table of Contents

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-Plänen. Es bietet Zugriff auf Wissen und Experten, um die Cloud-Einführung zu beschleunigen und die Produktivität der Entwickler zu steigern. Mit Ihrem organisationsspezifischen privaten re:Post können Sie eine organisationsspezifische Entwickler-Community aufbauen, die die Effizienz in großem Umfang steigert und Zugriff auf wertvolle Wissensressourcen bietet. Darüber hinaus zentralisiert re:Post Private vertrauenswürdige AWS technische Inhalte und bietet private Diskussionsforen, um die Zusammenarbeit Ihrer Teams intern und mit AWS zu verbessern, um technische Hindernisse zu beseitigen, Innovationen zu beschleunigen und in der Cloud effizienter zu skalieren.

Weitere Informationen finden Sie unter AWS re:Post Private.

Zugriff auf re:Post Private

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 ihren privaten re:Post benennen und eine Subdomäne unter definieren`*.private.repost.aws`. Administratoren für den privaten re:Post einer Organisation können den Benutzerzugriff mit konfigurieren AWS IAM Identity Center und eine der folgenden Identitätsquellen für die Authentifizierung angeben: 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 die Branding- und Wissensanforderungen der Organisation anpassen. Die Mitglieder des AWS Kontoteams, z. B. Technical Account Managers, die mit der Architektur und den Workloads der Organisation vertraut sind, werden automatisch zum privaten re:Post der Organisation für die Zusammenarbeit hinzugefügt.

Administratoren für die re:Post Private-Anwendung können das Branding anpassen, Tags zur Klassifizierung von Inhalten hinzufügen und Themen auswählen, die für ihre Entwickler von Interesse sind, um Trainings- und technische Inhalte automatisch zu füllen. Sie können Benutzer auch einladen, ihrem privaten re:Post beizutreten, um die Zusammenarbeit zu verbessern. Weitere Informationen finden Sie im AWS re:Post Private Administration Guide.

Benutzer, die keine Administratorrechte sind, verwenden die Anwendung re:Post Private, 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 individueller Trainings- und technischer Inhalte, die auf ihre jeweiligen Themen zugeschnitten sind. Benutzer können auch direkt in ihrem privaten re:Post AWS nach öffentlichen technischen Inhalten suchen und private Threads für interne Diskussionen zu AWS öffentlichen Inhalten erstellen. Benutzer können AWS technische Probleme gemeinsam lösen und technische Beratung von anderen Benutzern des privaten re:Posts erhalten, indem sie eine Frage stellen, eine Antwort geben oder einen Artikel veröffentlichen. Benutzer können einen Diskussionsthread auch in einen -AWS SupportFall umwandeln. Benutzer können die Antworten von AWS Support zum privaten re:Post hinzufügen. Weitere Informationen finden Sie im AWS re:Post Private-Benutzerhandbuch.

Preisgestaltung

Nur Kunden mit Enterprise Support (ES)- und Enterprise On-Ramp (EOP)-Support-Plänen können den re:Post Private-Service abonnieren. Sie können zwischen den beiden verfügbaren Preisstufen wählen: Kostenloses Kontingent und Standardkontingent. Das kostenlose Kontingent bietet Ihnen die Möglichkeit, die Funktionen des Standardkontingents sechs Monate lang vollständig zu erkunden und auszuprobieren, bevor Sie nahtlos zu einem kostenpflichtigen Kontingent übergehen können. Wenn Sie das Standardkontingent verwenden, können Sie ein monatliches Abonnement pro Benutzer zahlen, um re:Post Private zu nutzen. Weitere Informationen finden Sie unter -Preisgestaltung.

Erste Schritte

Informationen zu den ersten Schritten mit re:Post Private finden Sie unter Voraussetzungen.

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 einen Enterprise- oder Enterprise On-Ramp-Supportplan anmelden.
- Du musst ihn AWS IAM Identity Center in derselben Region aktivieren, in der du deinen privaten re:Post einrichten möchtest.
- Sie müssen eine AWS Identity and Access Management Rolle erstellen, die über die erforderlichen Berechtigungen verfügt, um AWS Support Fälle für Sie zu erstellen, zu verwalten und zu lösen. Der Dienst re:POST Private verwendet diese Rolle, um API-Aufrufe an zu tätigen. AWS Support Weitere Informationen finden Sie unter Verwalten des Zugriffs auf die AWS Support Fallerstellung und -verwaltung in re:Post Private.

Onboarding zu re:Post Private über IAM Identity Center

re:Post Private lässt sich in integrierenAWS IAM Identity Center, um einen Identitätsverbund für Ihre Belegschaft bereitzustellen. Über IAM Identity Center werden Benutzer zu ihrem vorhandenen Unternehmensverzeichnis weitergeleitet, 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 die Zwei-Faktor-Authentifizierung durchgesetzt werden. Die Verwendung von IAM Identity Center wirkt sich nicht auf Ihre vorhandene IAM-Konfiguration aus.

Wenn Sie nicht über ein vorhandenes Benutzerverzeichnis verfügen 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 zum Zuweisen von Berechtigungen innerhalb eines privaten re:Post. Benutzerberechtigungen innerhalb eines privaten re:Post werden von einem Administrator für seine private 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 auch für das Konto AWS Organizations aktiviert haben.

> **Important**
>
> re:Post Private unterstützt nur Organisations-Instances von IAM Identity Center .

Sicherheit in re:POST Private

Cloud-Sicherheit hat höchste AWS Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für AWS re:POST Private gelten, finden Sie unter AWS Services im Umfang nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem 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 bei der Verwendung von re:POST Private anwenden können. In den folgenden Themen erfahren Sie, wie Sie re:POST Private konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre re:POST Private-Ressourcen zu überwachen und zu schützen.

Themen

Datenschutz in re:POST Private AWS

Das Modell der AWS gemeinsamen Verantwortung und 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 Systeme laufen. 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 im Abschnitt Datenschutz FAQ. Informationen zum Datenschutz in Europa finden Sie im AWS Shared Responsibility Model und im GDPR Blogbeitrag auf dem AWS Security Blog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. 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 eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden SieSSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen 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 FIPS 140-3 validierte kryptografische Module für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine benötigenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter Federal Information Processing Standard () 140-3. FIPS

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 einem anderen über die AWS -Services Konsole arbeiten,, oder. API AWS CLI 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 einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen angeben, um Ihre Anfrage an diesen Server URL zu validieren.

Datenschutz durch Verschlüsselung

Verschlüsselung im Ruhezustand

re:POST Private verwendet Amazon Simple Storage Service-Buckets, Amazon DynamoDB DynamoDB-Datenbanken, Amazon Neptune Neptune-Datenbanken und Amazon OpenSearch Service-Domains, 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 Protokoll, um mit Ihrer Client-Anwendung zu kommunizieren. HTTPS Es verwendet HTTPS und AWS signiert, um im Namen Ihrer Anwendung mit anderen Diensten zu kommunizieren.

Schlüsselverwaltung

Re:Post Private ist in Schlüssel integriert AWS Key Management Service und unterstützt AWS KMS diese. Du kannst die Datenverschlüsselungseinstellungen für deinen privaten re:POST anpassen, wenn du ihn erstellst. Dazu kannst du entweder einen vorhandenen AWS KMS Schlüssel auswählen oder einen neuen AWS KMS Schlüssel erstellen.

Wie funktioniert re:POST Private mit IAM

Bevor du re:POST Private verwendestIAM, um den Zugriff auf AWS re:POST Private zu verwalten, musst du wissen, welche IAM Funktionen du mit re:POST Private nutzen kannst. Einen allgemeinen Überblick darüber, wie re:POST Private und andere AWS Dienste funktionieren, finden Sie im Benutzerhandbuch unter AWS DienstelAM, mit denen funktioniert. IAM IAM

Auf privaten Identitäten basierende Richtlinien von re:POST

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

Aktionen

Administratoren können mithilfe von AWS JSON Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Action` Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen in re:POST Private verwenden vor der Aktion das folgende Präfix:. `repostspace:` Um beispielsweise jemandem die Erlaubnis zu erteilen, den `CreateSpace` API Vorgang re:POST Private auszuführen, nehmen Sie die `repostspace:CreateSpace` Aktion in seine Richtlinie auf. Richtlinienerklärungen müssen `Action` entweder ein `NotAction` Oder-Element enthalten. re:Post Private definiert eigene 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 privaten Aktionen von re:POST finden Sie im Benutzerhandbuch unter Von re:POST Private definierte Aktionen. IAM

Ressourcen

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Bedingungsschlüssel

re:POST Private stellt keine dienstspezifischen Bedingungsschlüssel bereit, unterstützt aber die Verwendung globaler Bedingungsschlüssel. Um alle AWS globalen Bedingungsschlüssel zu sehen, siehe AWS globale Bedingungskontextschlüssel im IAM Benutzerhandbuch.

Beispiele

Beispiele für identitätsbasierte Richtlinien von re:POST Private finden Sie unter. AWSre:POST Beispiele für Richtlinien, die auf privaten Identitäten basieren

Auf Ressourcen basierende Richtlinien von re:POST Private

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder Dienste gehören. AWS Ressourcenbasierte

Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien nicht IAM in einer ressourcenbasierten Richtlinie verwenden.

Re:Post Private unterstützt keine ressourcenbasierten Richtlinien.

Autorisierung auf der Basis von Markierungen

re:POST Private unterstützt das Markieren von Ressourcen oder die Steuerung des Zugriffs anhand von Tags. Weitere Informationen finden Sie unter Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags.

re:POST Private Rollen IAM

Eine IAMRolle ist eine Entität innerhalb Ihres AWS Kontos, die über bestimmte Berechtigungen verfügt.

Verwendung temporärer Anmeldeinformationen mit re:POST Private

Wir empfehlen dringend, temporäre Anmeldeinformationen zu verwenden, um sich bei Federation anzumelden, eine IAM Rolle zu übernehmen oder eine kontoübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API Operationen wie AssumeRoleoder GetFederationTokenaufrufen.

re:POST Private unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit dienstbezogenen Rollen können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, um eine Aktion für Sie abzuschließen. Mit Diensten verknüpfte Rollen werden in Ihrem IAM Konto angezeigt und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Servicerollen

Diese Funktion ermöglicht es einem Dienst, eine Servicerolle für Sie zu übernehmen. Diese Rolle ermöglicht es dem Dienst, auf Ressourcen in anderen Diensten zuzugreifen, um eine Aktion für Sie abzuschließen. Weitere Informationen finden Sie unter Eine Rolle zum Delegieren von Berechtigungen für einen AWS Dienst erstellen. Servicerollen werden in Ihrem IAM Konto angezeigt und gehören dem Konto. Das 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

AWSre:POST Private verwendet AWS Identity and Access Management () serviceverknüpfte Rollen. IAM Eine serviceverknüpfte Rolle ist ein einzigartiger Rollentyp, der direkt mit IAM re:POST Private verknüpft ist. Dienstbezogene Rollen sind von re:POST Private vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere Dienste in Ihrem Namen aufzurufen. AWS

Eine dienstbezogene 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. Zu den definierten Berechtigungen gehören die Vertrauensrichtlinie und die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen Entität zugeordnet werden. IAM

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

Berechtigungen für dienstverknüpfte Rollen für re:POST Private

re:POST Private verwendet die dienstverknüpfte Rolle namens AWSServiceRoleForrePostPrivate. re:Post Private verwendet diese dienstverknüpfte Rolle, um Daten zu veröffentlichen. CloudWatch

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

- `repostspace.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie `AWSrePostPrivateCloudWatchAccess` ermöglicht es re:POST Private, die folgenden Aktionen an den angegebenen Ressourcen durchzuführen:

- Aktion für: `cloudwatch` `PutMetricData`

Sie müssen Berechtigungen konfigurieren, damit eine Benutzer, Gruppen oder Rollen eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Dienstbezogene Rollenberechtigungen.

Weitere Informationen finden Sie unter AWSrePostPrivateCloudWatchAccess.

Eine dienstverknüpfte Rolle für re:POST Private erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn du deinen ersten privaten re:POST in der AWS Management Console, der oder der erstellst, erstellt re:POST Private die AWS API serviceverknüpfte Rolle für dich. AWS CLI

> **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 du den Dienst re:POST Private vor dem 1. Dezember 2023 genutzt hast, als er begann, serviceverknüpfte Rollen zu unterstützen, dann hat re:POST Private die Rolle in deinem Konto erstellt. `AWSServiceRoleForrePostPrivate` Weitere Informationen findest du unter Eine neue Rolle ist in meinem erschienen. 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.

Erstellen Sie im AWS CLI oder im AWS API eine dienstverknüpfte Rolle mit dem Dienstnamen. `repostspace.amazonaws.com` Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer dienstbezogenen Rolle. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeitung einer serviceverknüpften Rolle für re:POST Private

Mit re:POST Private können Sie die mit dem Dienst verknüpfte Rolle nicht bearbeiten. `AWSServiceRoleForrePostPrivate` Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten auf die Rolle verweisen könnten. Sie können die Beschreibung der Rolle jedoch mit bearbeiten. IAM Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Bearbeiten einer dienstbezogenen Rolle.

Löschen einer serviceverknüpften Rolle für re:POST Private

Sie müssen die Rolle `AWSServiceRoleForrePostPrivate` nicht manuell löschen. Wenn du deinen privaten re:POST in der AWS Management Console, der oder der re:POST Private löschst AWS CLI AWS API, wird die dienstverknüpfte Rolle für dich gelöscht.

Sie können auch die IAM Konsole, die oder die verwenden, um die mit dem Dienst AWS CLI verknüpfte Rolle manuell AWS API zu löschen.

Um die dienstverknüpfte Rolle manuell zu löschen, verwenden Sie IAM

Verwenden Sie die IAM Konsole, den oder AWS CLI, AWS API um die AWSServiceRoleForrePostPrivate dienstverknüpfte Rolle zu löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Löschen einer dienstbezogenen Rolle.

Unterstützte Regionen für dienstverknüpfte re:POST Private-Rollen

re:POST Private unterstützt die Verwendung von serviceverknüpften Rollen in den AWS Regionen, in denen der Dienst verfügbar ist.

Name der Region	Regions-ID	Support 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
Asien-Pazifik (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

Name der Region	Regions-ID	Support in re:POST Private
Kanada (Zentral)	ca-central-1	Ja
Europa (Frankfurt)	eu-central-1	Ja
Europa (Ireland)	eu-west-1	Ja
Europa (London)	eu-west-2	Nein
Europa (Mailand)	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 () UAE	me-central-1	Nein
Südamerika (São Paulo)	sa-east-1	Nein

AWSre:POST Beispiele für Richtlinien, die auf privaten Identitäten basieren

> **Note**
>
> Um die Sicherheit zu erhöhen, sollten Sie nach Möglichkeit Verbundbenutzer anstelle von IAM Benutzern erstellen.

Standardmäßig sind AWS Identity and Access Management Benutzer und Rollen nicht berechtigt, private AWS re:POST-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit dem AWS Management Console AWS CLI, oder ausführen. AWS API Ein IAM Administrator muss IAM Richtlinien erstellen, die Benutzern und Rollen die Berechtigung gewähren, bestimmte API Operationen mit den angegebenen Ressourcen auszuführen, die sie benötigen. Der Administrator muss diese Richtlinien dann den IAM Benutzern oder Gruppen zuordnen, für die diese Berechtigungen erforderlich sind.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter IAMRichtlinien erstellen im IAMBenutzerhandbuch.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand private re:POST-Ressourcen in deinem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie AWS im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen.
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung 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 IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS -Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.

- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.
- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Um festzulegen, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die Inline- und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. AWS CLI 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 Sie Berechtigungen für AWS re:POST-Private-Aktionen zuweisen. Allgemeine Informationen zu Inline-Richtlinien finden Sie im AWSIAMBenutzerhandbuch unter IAMRichtlinien verwalten. Sie können das AWS Management Console, AWS Command Line Interface (AWSCLI) oder das verwenden, AWS Identity and Access Management API um Inline-Richtlinien zu erstellen und einzubetten.

Themen

- Schreibgeschützter Zugriff auf re:Post Private
- Voller Zugriff auf re:POST Private

Schreibgeschützter Zugriff auf re:Post Private

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

```
{
    "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 IAM Identity Center und re:POST Private Console. Diese Richtlinie ermöglicht es dem Benutzer, alle re:POST Private-Aktionen durchzuführen.

```
{
    "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 re:POST Private AWS

Durch die Verwendung AWS verwalteter Richtlinien ist das Hinzufügen von Berechtigungen für Benutzer, Gruppen und Rollen einfacher, als wenn Sie selbst Richtlinien schreiben müssen. Es erfordert Zeit und Fachwissen, um vom IAMKunden verwaltete Richtlinien zu erstellen, die Ihrem Team nur die Berechtigungen gewähren, die es benötigt. Verwenden Sie AWS verwaltete Richtlinien, um schnell loszulegen. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Dienste können gelegentlich zusätzliche Berechtigungen zu einer AWS verwalteten Richtlinie hinzufügen, um neue Funktionen zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Es ist sehr wahrscheinlich, dass Dienste eine AWS verwaltete Richtlinie aktualisieren, wenn eine neue Funktion eingeführt wird oder wenn neue Operationen verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die `ReadOnlyAccess` AWS verwaltete Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst eine neue Funktion startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien.

Themen

- AWS verwaltete Richtlinie: AWSRepostSpaceSupportOperationsPolicy
- AWS verwaltete Richtlinie: AWSrePostPrivateCloudWatchAccess
- AWSRe:POST Private aktualisiert verwaltete Richtlinien AWS

AWS verwaltete Richtlinie: AWSRepostSpaceSupportOperationsPolicy

Diese Richtlinie ermöglicht es dem AWS re:POST Private-Dienst, AWS Support Fälle zu erstellen, zu verwalten und zu lösen, die über die re:POST Private-Webanwendung erstellt wurden.

```
{
 "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

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

AWSRe:POST Private aktualisiert verwaltete Richtlinien AWS

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für re:POST Private an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS Feed auf der Seite, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.
Dokumentverlauf

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

Änderung	Beschreibung	Datum
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 verwalteten Richtlinien zu verfolgen AWS	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 auftreten können. IAM

Themen

- Ich bin nicht berechtigt, eine Aktion in re:POST Private durchzuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine privaten re:POST-Ressourcen ermöglichen

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 `mateojackson` IAM Benutzer versucht, die Konsole zu verwenden, um Details zu einer fiktiven *`my-example-widget`* Ressource anzuzeigen, aber nicht über die fiktiven Berechtigungen verfügt. `repostPrivate:`*`GetWidget`*

```
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 auszuführen: PassRole

Wenn du die Fehlermeldung erhältst, dass du nicht autorisiert bist, die `iam:PassRole` Aktion durchzuführen, müssen deine Richtlinien aktualisiert werden, damit du eine Rolle an re:POST Private übergeben kannst.

Einige AWS -Services ermöglichen es dir, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM Benutzer mit dem 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 Personen außerhalb von mir den Zugriff AWS-Konto auf meine privaten re:POST-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem

die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, kannst du diese Richtlinien verwenden, um Personen Zugriff auf deine Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Um zu erfahren, ob re:POST Private diese Funktionen unterstützt, siehe. Wie funktioniert re:POST Private mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM Benutzerhandbuch unter Einem Benutzer Zugriff auf einen anderen IAMBenutzer gewähren AWS-Konto , der Ihnen gehört.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund). IAM
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

Konformitätsprüfung für re:POST Private AWS

Informationen darüber, ob AWS -Service ein AWS -Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS -Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS -Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.

- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

  > **Note**
  >
  > Nicht alle sind berechtigt AWS -Services . HIPAA Weitere Informationen finden Sie in der Referenz für HIPAA qualifizierte Dienste.

- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS -Services und die Leitlinien für Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zusammengefasst.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS -Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS -Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- AWS Audit Manager— Auf diese AWS -Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in AWS re:POST Private

Die AWS globale Infrastruktur basiert AWS-Regionen auf Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, 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.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Infrastruktursicherheit in AWS re:POST Private

Als verwalteter Service ist AWS Re:POST Private durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Sie verwenden AWS veröffentlichte API Aufrufe, um über das Netzwerk auf re:POST Private zuzugreifen. Clients müssen Transport Layer Security (TLS) 1.0 oder höher unterstützen. Wir empfehlen TLS 1.2 oder höher. Kunden müssen außerdem Cipher Suites mit Perfect Forward Secrecy (PFS) wie (Ephemeral Diffie-Hellman) oder (DHEElliptic Curve Ephemeral Diffie-Hellman) unterstützen. ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. AWS Identity and Access Management 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	Anpassbar
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

Themen

Erstellen eines neuen privaten re:Post

Gehen Sie folgendermaßen vor, um einen neuen privaten re:Post zu erstellen:

1. Öffnen Sie die re:Post Private-Konsole unter https://console.aws.amazon.com/repost-private/.
2. Wählen Sie auf der Homepage der Konsole Privates re:Post erstellen aus.
3. Wenn Sie IAM Identity Center noch nicht für Ihr Konto konfiguriert haben, wählen Sie Identity Center öffnen aus. Folgen Sie den Anweisungen unter Erste Schritte im AWS IAM Identity Center-Benutzerhandbuch.
4. Wählen Sie auf der Seite Privaten re:Post erstellen für Preise die Option Kostenloses Kontingent oder Standardkontingent basierend auf Ihrem Anwendungsfall aus. Wenn Sie bereits das kostenlose Kontingent für für Ihr Konto verwendet 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 für Benutzerdefinierte Subdomäne einen benutzerdefinierten Namen für Ihre Subdomäne 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 für Wählen Sie einen AWS KMS-Schlüssel einen - AWS Key Management Service Schlüssel oder einen Amazon-Ressourcennamen (ARN) aus.

–oder–

Wählen Sie Erstellen eines AWS KMS-Schlüssels aus. Erstellen Sie dann den AWS KMS Schlüssel .

7. (Optional) Wählen Sie unter Servicezugriff für die Integration von Support-Fällen 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 für Bitte 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 Neue Rolle in der IAM-Konsole erstellen aus.

Wenn Sie eine neue Rolle erstellen möchten, folgen Sie den Anweisungen unter Erstellen 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 Dropdown-Liste aus.

Weitere Informationen finden Sie unter Verwalten des Zugriffs auf die AWS Support Fallerstellung und -verwaltung 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 Schlüssel Ihren benutzerdefinierten Tag-Schlüssel ein.

Geben Sie für Wert Ihren benutzerdefinierten Tag-Wert ein.

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

9. Wählen Sie Create this re:Post aus.

Auf einer Bestätigungsseite werden Sie darüber informiert, dass Ihr privater re:Post erstellt wird. Sie können den Status des privaten re:Post im Feld Status anzeigen. Wenn Ihr privater re:Post erstellt wird, wird im Feld Status die Meldung Erstellen angezeigt.

Es dauert etwa 30 Minuten, bis der private re:Post erstellt ist. Wenn Ihr privater re:Post bereit ist, zeigt das Feld Status Online an. Sie können die von AWS generierte Subdomäne für Ihren privaten re:Post verwenden, die auf der Registerkarte Einstellungen aufgeführt ist, um auf Ihren privaten re:Post zuzugreifen. Sie können die benutzerdefinierte Subdomäne für Ihren privaten re:Post nach Abschluss der Überprüfung auf der Registerkarte Einstellungen anzeigen.

Verwalten des Zugriffs auf die AWS Support Fallerstellung und -verwaltung in re:Post Private

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

- CreateCase
- AddCommunicationToCase
- ResolveCase

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

Benutzer in Ihrem privaten re:Post haben die gleichen Berechtigungen, die Sie der IAM-Rolle gewähren.

> **Important**
>
> Wenn Sie die IAM-Rolle oder die IAM-Richtlinie ändern, gelten Ihre Änderungen für den von Ihnen konfigurierten privaten re:Post.

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

Themen

Verwenden einer - AWS verwalteten Richtlinie oder Erstellen einer kundenverwalteten Richtlinie

Um Ihrer Rolle Berechtigungen zu erteilen, können Sie entweder eine von AWS verwaltete Richtlinie oder eine vom Kunden verwaltete Richtlinie verwenden.

> **Tip**
>
> Wenn Sie eine Richtlinie nicht manuell erstellen möchten, empfehlen wir Ihnen, stattdessen eine AWS von verwaltete Richtlinie zu verwenden und dieses Verfahren zu überspringen. Verwaltete Richtlinien verfügen automatisch über die erforderlichen Berechtigungen für AWS 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.

So erstellen Sie eine vom Kunden verwaltete Richtlinie für re:Post Private

1. Melden Sie sich bei der an AWS Management Console 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. Auf der Seite Zusammenfassung finden Sie die Berechtigungen, die 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 erlaubt der Rolle, über vollständige Berechtigungen für alle erforderlichen Aktionen für zu verfügen AWS Support. Nachdem Sie einen privaten re:Post mit der Rolle konfiguriert haben, hat jeder Benutzer in Ihrem privaten re:Post die gleichen Berechtigungen.

```
{
 "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 von AWS verwalteten Richtlinien für re:Post Private finden Sie unter AWS verwaltete Richtlinien für re:POST Private AWS.

Sie können die Richtlinie aktualisieren, um eine Berechtigung aus zu entfernen AWS 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 aus, wenn Sie einen privaten re:Post in der re:Post Private-Konsole erstellen.

So erstellen Sie eine Rolle für die AWS Support Fallerstellung und -verwaltung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Roles (Rollen) und dann Create role (Rolle erstellen).
3. Für Trusted entity type (Vertrauenstyp der Entität), wählen Sie Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie).
4. Geben Sie für Benutzerdefinierte Vertrauensrichtlinie Folgendes ein:

```
{
 "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 unter Berechtigungsrichtlinien in der Suchleiste die AWS von verwaltete Richtlinie oder eine vom Kunden verwaltete Richtlinie ein, die Sie erstellt haben, z. B. *rePostPrivateSupportPolicy*. Aktivieren Sie das Kontrollkästchen neben den Berechtigungsrichtlinien, die der Service haben soll.
7. Wählen Sie Weiter aus.
8. Geben Sie auf der Seite Name, Überprüfung und Erstellung für Rollenname einen Namen ein, z. B. *rePostPrivateSupportRole*.
9. (Optional) Geben Sie unter Beschreibung eine Beschreibung für die 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 Service (Konsole) im IAM-Benutzerhandbuch.

Fehlerbehebung

Weitere Informationen zum Verwalten des Zugriffs auf re:Post Private finden Sie in den folgenden Themen.

Inhalt

- Meiner IAM-Rolle fehlt eine Berechtigung
- Ein Fehler besagt, dass meine IAM-Rolle ungültig ist

Ich möchte bestimmte Benutzer in meinem privaten re:Post auf bestimmte Aktionen beschränken

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

Wir empfehlen Ihnen, die folgenden bewährten Methoden:

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

Wenn ich einen privaten re:Post konfiguriere, wird die von mir erstellte IAM-Rolle nicht angezeigt

Wenn Ihre IAM-Rolle nicht in der IAM-Rolle für re:Post Private erscheint;-Liste, bedeutet dies, 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 Sie für Ihren privaten re:Post erstellen, benötigt Berechtigungen zum Ausführen der gewünschten Aktionen. Wenn Sie beispielsweise möchten, dass Ihre Benutzer im privaten re:Post Supportfälle erstellen, muss die Rolle über die -`support:CreateCase`Berechtigung verfügen. re:Post Private übernimmt diese Rolle, um diese Aktionen für Sie auszuführen.

Wenn Sie eine Fehlermeldung über eine fehlende Berechtigung für erhalten AWS Support, stellen Sie sicher, dass 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 ungültig ist

Stellen Sie sicher, dass Sie die richtige Rolle für Ihre private re:Post-Konfiguration ausgewählt haben.

Einrichten und Verwalten des Benutzerzugriffs mit AWS IAM Identity Center

re:Post Private lässt sich in integrieren AWS IAM Identity Center , um einen Identitätsverbund für die Belegschaft Ihrer Organisation bereitzustellen. Verwenden Sie IAM Identity Center, um Benutzer aus Ihrer Organisation zu erstellen oder zu verbinden und ihren Zugriff über alle AWS Konten und Anwendungen hinweg 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 auch für das Konto AWS Organizations aktiviert haben.

Anpassen Ihres privaten re:Post

Sie können Ihrem privaten re:Post einen oder mehrere Administratoren hinzufügen, nachdem Sie ihn erstellt haben. Administratoren verwenden die Anwendung re:Post Private, um den privaten re:Post zu starten und Benutzer darin zu verwalten. Sie können das Branding für den privaten re:Post anpassen, Tags zur Klassifizierung von Inhalten hinzufügen und Themen auswählen, die für die automatische Nutzung 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

Sie können Ihrem privaten re:Post einen oder mehrere Benutzer hinzufügen, nachdem Sie ihn erstellt haben. Sie können Benutzer zur Zusammenarbeit in Ihrem privaten re:Post einladen. Benutzer verwenden die re:Post Private-Anwendung, um sich mit von Ihnen konfigurierten Anmeldeinformationen anzumelden. Nachdem sich bei einem privaten re:Post angemeldet haben, können Benutzer vorhandene Inhalte durchsuchen oder durchsuchen, einschließlich maßgeschneiderter Trainings- und technischer Inhalte, die auf ihre jeweiligen Themen zugeschnitten sind. Weitere Informationen finden Sie im AWS re:Post Private-Benutzerhandbuch.

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 und Gruppen zu Ihrem privaten re:POST hinzu

Wenn Sie ein Administrator sind, können Sie Benutzer und Gruppen zu Ihrem privaten re:Post hinzufügen.

Füge Nutzer zu deinem privaten re:Post hinzu

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.
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.

Füge Gruppen zu deinem privaten re:Post hinzu

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.
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.

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

Gehen Sie wie folgt vor, um Benutzer und Gruppen 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.

Befördere einen Nutzer in deinem privaten re:POST zum Administrator

Gehen Sie wie folgt vor, um einen privaten re:POST-Benutzer zum Administrator zu ernennen:

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. Wähle einen oder mehrere Benutzer aus, die du zum Administrator ernennen möchtest.
6. Wählen Sie „Rolle bearbeiten“ und anschließend „Zum Administrator ernennen“.

Die ausgewählten Benutzer werden zu Administratoren befördert. Auf der Registerkarte Benutzer wird die Rolle für diese Benutzer auf Administrator aktualisiert.

Entferne Benutzer oder Gruppen aus deinem privaten re:Post

Wenn Sie ein Administrator sind, können Sie Benutzer oder Gruppen aus Ihrem privaten re:Post entfernen.

Entferne Nutzer aus deinem privaten re:Post

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.
4. Wähle unter Nutzer aus der Liste die Nutzer aus, die du aus deinem privaten re:Post entfernen möchtest. Wähle dann Entfernen.

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

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

Löschen Sie einen privaten re:Post aus re:Post Private

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.

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 AWS Lösungen. AWSbietet die folgenden Überwachungstools, um re:POST Private zu beobachten, 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 Metriken 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 Kennzahlen Ihrer Amazon EC2 EC2-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder für Sie getätigt wurden, AWS-Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 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. Amazon CloudWatch sammelt Rohdaten und verarbeitet sie zu lesbaren Metriken, die nahezu in Echtzeit verfügbar 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 Service re:POST Private meldet die folgenden Metriken im `AWS/rePostPrivate` Namespace.

Metrik	Beschreibung
`NumberOfSpaces`	Die Anzahl der privaten re:Posts im Girokonto.

Metrik	Beschreibung
	Einheiten: Anzahl
`NumberOfUsers`	Die Anzahl der Benutzer 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	Beschreibung
`spaceId`	Die eindeutige Kennung für den privaten re:Post.

Protokollieren von privaten API-Aufrufen von AWS re:POST mit AWS CloudTrail

AWS re:Post Private ist in einen Service integriertAWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in re:POST Private ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für re:POST Private als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der re:POST Private-Konsole und Code-Aufrufe der re:POST Private API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 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 von gesammelten Informationen können Sie die Anfrage CloudTrail, die 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 ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrailBenutzerhandbuch.

re:Private Informationen posten in CloudTrail

CloudTrail ist auf deinem aktiviert, AWS-Konto wenn du das Konto erstellst. Wenn in re:POST Private eine Aktivität stattfindet, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Event-Verlauf in einem Event aufgezeichnet. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Mit dem CloudTrail Ereignisverlauf arbeiten.

Für eine fortlaufende Aufzeichnung der Ereignisse in deinemAWS-Konto, einschließlich der Ereignisse für re:POST Private, erstelle einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 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 stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. 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 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 Reference protokolliert CloudTrail und sind in dieser 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 die Protokollierung der folgenden AWS 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. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu den Einträgen in der privaten re:POST-Protokolldatei

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 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 Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, 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 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": "2023-11-07T21:17:19Z",
               "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 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": "2023-11-09T22:28:23Z",
                "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 demonstriert. 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

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 AWSre:POST Beispiele für Richtlinien, die auf privaten Identitäten basieren.

Dokumentverlauf

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

Änderung	Beschreibung	Datum
Aktualisieren	USA Ost (Nord-Virginia), Asien-Pazifik (Sydney), Kanada (Zentral) und Europa (Irland) wurden zu den unterstützten Regionen hinzugefügt	10. Mai 2024
Aktualisieren	Asien-Pazifik (Singapur) wurde zu den unterstützten Regionen hinzugefügt	6. März 2024
Neue Ressourcen	Dokumentation für von AWS verwaltete Richtlinien für AWS re:Post Private hinzugefügt	26. November 2023
Erstversion	Erste Version des Administratorhandbuchs für re:POST Private Console	26. November 2023

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.