コンソール管理ガイド

AWS re:Post Private

AWS re:Post Private: コンソール管理ガイド

Table of Contents

AWS re:Post Private とは ... 1
re:Post Private にアクセスする ... 1
料金 ... 2
開始方法 ... 2
前提条件 ... 3
re:Post Private にオンボードする ... 4
セキュリティ ... 5
データ保護 ... 5
暗号化によるデータの保護 ... 6
転送中の暗号化 ... 7
キー管理 ... 7
re:Post Private が IAM と連携する方法 ... 7
re: プライベートアイデンティティベースのポリシーの投稿 ... 7
re: プライベートリソースベースのポリシーの投稿 ... 9
タグに基づく認可 ... 9
re: プライベート IAM ロールの投稿 ... 9
サービスリンクロール ... 10
サービスロール ... 10
サービスリンクロールの使用 ... 10
アイデンティティベースポリシーの例 ... 14
インラインポリシー ... 17
AWS マネージドポリシー ... 19
トラブルシューティング ... 22
コンプライアンス検証 ... 24
耐障害性 ... 25
インフラストラクチャセキュリティ ... 25
クォータ ... 27
Service Quotas ... 27
API スロットリング制限 ... 27
プライベート re:Post を作成、設定、カスタマイズする ... 29
新しいプライベート re:Post を作成する ... 29
re:Post Private での AWS Support ケースの作成と管理へのアクセスの管理 ... 31
AWS 管理ポリシーを使用するか、カスタマー管理ポリシーを作成する ... 32
IAM ポリシーの例 ... 33

IAM ロールを作成する 34
トラブルシューティング 35
ユーザーアクセスの設定と管理 36
プライベート re:Post をカスタマイズする 36
プライベート re:Post にユーザーを招待する 37
プライベートな re: POST を管理 38
ユーザーおよびグループの追加 38
グループにユーザーを追加する 39
ユーザーやグループを招待 39
ユーザーを管理者に昇格させる 40
ユーザーとグループを削除する 40
従業員を追加または削除する。AWS 41
非公開の re: POST を削除する 41
Re: Post プライベートモニタリング 43
によるモニタリング CloudWatch 43
re: POST プライベート API 呼び出しを使用して口ギングする AWS CloudTrail 44
re: プライベート情報をに投稿 CloudTrail 44
re: Post Private のログファイルエントリについて 46
トラブルシューティング 52
特定の AWS リージョンでプライベート re:Post を設定できない 52
アカウントにプライベート re:Post を設定できない 52
プライベート re:Post のユーザーまたはグループを管理できない 52
ドキュメント履歴 53
..... liv

AWS re:Post Private とは

AWS re:Post Private は、エンタープライズサポートまたはエンタープライズ On-Ramp サポートプランを持つ企業向けの AWS re:Post のプライベートバージョンです。知識とエキスパートにアクセスして、クラウドの導入を加速し、開発者の生産性を向上させます。組織固有のプライベート re:Post を使用すると、大規模な効率を高め、貴重なナレッジリソースにアクセスできる組織固有のデベロッパーコミュニティを構築できます。さらに、re:Post Private は信頼できるAWS技術コンテンツを一元化し、チームが社内や AWS と連携する方法を改善して技術的な障害を排除し、イノベーションを加速させ、クラウド内でより効率的にスケールするためのプライベートディスカッションフォーラムを提供します。

詳細については、「AWS re:Post Private」を参照してください。

re:Post Private にアクセスする

管理者は AWS re:Post Private コンソールを使用して、組織固有のプライベート re:Post を作成します。管理者がプライベート re:Post を作成すると、プライベート re:Post という名前を付け、 の下にサブドメインを定義できます`*.private.repost.aws`。組織のプライベート re:Post の管理者は、 を使用してユーザーアクセスを設定しAWS IAM Identity Center、認証のために Identity Center ディレクトリ、Active Directory、または外部の ID プロバイダーのいずれかの ID ソースを指定できます。ユーザーを設定すると、コンソール管理者は re:Post プライベート管理者ロールを 1 人以上のユーザーに割り当てることができます。re:Post プライベート管理者は、組織のブランドや知識のニーズに応じて、プライベート re:Post アプリケーションをカスタマイズできます。組織のアーキテクチャとワークロードに精通しているテクニカルアカウントマネージャーなどのAWSアカウントチームメンバーは、コラボレーションのために組織のプライベート re:Post に自動的に追加されます。

re:Post Private アプリケーションの管理者は、ブランドをカスタマイズしたり、コンテンツを分類するためのタグを追加したり、デベロッパーがトレーニングコンテンツと技術コンテンツを自動的に入力できるように関心のあるトピックを選択したりできます。また、コラボレーションを強化するために、プライベート re:Post に参加するようにユーザーを招待することもできます。詳細については、「AWS re:Post プライベート管理ガイド」を参照してください。

管理者以外のユーザーは、 re:Post プライベートアプリケーションを使用して、管理者が設定した認証情報を使用してサインインします。プライベート re:Post にサインインすると、ユーザーは目的のトピックを対象としたカスタマイズされたトレーニングや技術コンテンツなど、既存のコンテンツを閲覧または検索できます。ユーザーは、プライベート re:Post から直接AWSパブリックテクニカルコ

ンテンツを検索し、AWSパブリックコンテンツに関する内部ディスカッション用のプライベートスレッドを作成することもできます。ユーザーは、質問したり、回答を提供したり、記事を公開したりすることで、AWS技術的な問題を解決し、プライベート re:Post の他のユーザーから技術ガイダンスを受けることができます。ユーザーは、ディスカッションスレッドを AWS Supportケースに変換することもできます。ユーザーは、 からのレスポンスをAWS Supportプライベート re:Post に追加できます。詳細については、「AWS re:Post プライベートユーザーガイド」を参照してください。

料金

re:Post プライベートサービスをサブスクライブできるのは、Enterprise Support (ES) および Enterprise On-Ramp (EOP) サポートプランをご利用のお客様のみです。無料利用枠と標準利用枠の 2 つの利用可能な料金範囲から選択できます。無料利用枠を利用すると、有料利用枠にシームレスに移行する前に、標準利用枠の機能を 6 か月間完全に探索して試すことができます。Standard 階層を使用する場合、re:Post Private を使用するためのユーザーあたりの月額サブスクリプション料金を支払います。詳細については、「料金」を参照してください。

開始方法

re:Post Private の使用を開始するには、「」を参照してください前提条件。

前提条件

新しいプライベート re: POST を作成したり、AWS re: Post Private で既存のプライベート re: Post を管理したりするには、以下の前提条件を満たす必要があります。

- エンタープライズまたはエンタープライズオンランプSupport プランにサインアップする必要があります。
- プライベート re: POST AWS IAM Identity Centerを設定したい地域と同じ地域で有効にする必要があります。
- AWS Supportケースの作成、管理、AWS Identity and Access Management解決に必要な権限を持つロールを作成する必要があります。re: Post Private サービスはこのロールを使用してへの API 呼び出しを行います。AWS Support詳細については、「re:Post Private での AWS Support ケースの作成と管理へのアクセスの管理」を参照してください。

IAM Identity Center を通じてプライベートを re:Post にオンボードする

re:Post Private は と統合AWS IAM Identity Centerして、ワークフォースに ID フェデレーションを提供します。IAM Identity Center を通じて、ユーザーは既存の会社のディレクトリにリダイレクトされ、既存の認証情報でサインインします。その後、プライベート re:Post にシームレスにサインインします。これにより、パスワードポリシーや 2 要素認証などのセキュリティ設定が適用されます。IAM Identity Center を使用しても、既存の IAM 設定には影響しません。

既存のユーザーディレクトリがない場合、またはフェデレーションしない場合、IAM Identity Center は re:Post Private のユーザーとグループを作成するために使用できる統合ユーザーディレクトリを提供します。 re:Post Private は、プライベート re:Post 内のアクセス許可を割り当てるための IAM ユーザーとロールの使用をサポートしていません。プライベート re:Post 内のユーザーアクセス許可は、管理者がプライベート re:Post アプリケーションで設定します。

IAM Identity Center の詳細については、「AWS IAM Identity Center とは (AWS Single Sign-On の後継サービス)」を参照してください。IAM Identity Center の開始方法の詳細については、「 の開始方法」を参照してください。IAM Identity Center を使用するには、アカウントで もAWS Organizations有効化されている必要があります。

> **Important**
>
> re:Post Private は、IAM Identity Center の組織インスタンスのみをサポートします。

re:Post Private のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ — AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。また、 は、安全に使用できるサービス AWS も提供します。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。AWS re:Post Private に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、 お客様のデータの機密性、企業の要件、および適用可能な法律や規制といった他の要因 についても責任を担います。

このドキュメントは、 re:Post Private を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために re:Post Private を設定する方法を示します。また、 re:Post Private リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

- AWS re:Post Private でのデータ保護
- re:Post Private が IAM と連携する方法
- AWS re:Post Private のコンプライアンス検証
- AWS re:Post Private の耐障害性
- AWS re:Post Private のインフラストラクチャセキュリティ

AWS re:Post Private でのデータ保護

責任 AWS 共有モデル、AWS re:Post Private でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任が

あります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS サービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーのよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿されたAWS 責任共有モデルおよび GDPRのブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS サービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、または SDK を使用して re:Post Private AWS CLIまたは他の AWS サービス を使用する場合も同様です。AWS SDKs 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

暗号化によるデータの保護

保管中の暗号化

re:Post Private は、Amazon Simple Storage Service バケット、Amazon DynamoDB データベース、Amazon Neptune データベース、および Amazon マネージドキーまたはカスタマーマネージドキーを使用して保管時に暗号化された Amazon OpenSearch Service ドメインを使用します。

転送中の暗号化

re:Post Private は HTTPS プロトコルを使用してクライアントアプリケーションと通信します。HTTPS と AWS 署名を使用して、アプリケーションに代わって他の サービスと通信します。

キー管理

re:Post Private は と統合 AWS Key Management Service されており、 AWS KMS キーをサポートしています。プライベート re:Post のデータ暗号化設定は、作成時にカスタマイズできます。そのためには、既存の AWS KMS キーを選択するか、新しい AWS KMS キー を作成します。

re:Post Private が IAM と連携する方法

IAM を使用して AWS re:Post Private へのアクセスを管理する前に、re:Post Private で使用できる IAM 機能を理解しておく必要があります。re:Post Private およびその他の AWS のサービスが IAM と連携する方法の概要を把握するには、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

re: プライベートアイデンティティベースのポリシーの投稿

IAM アイデンティティベースのポリシーでは、許可または拒否されたアクションを指定できます。re:Post Private は特定のアクションをサポートします。JSON ポリシーで使用する要素については、「IAM ユーザーガイド」 の「IAM JSON ポリシー要素のリファレンス」(IAM JSON) をご参照ください。

アクション

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーの`Action`要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは、依存アクションと呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

re:Post Private のポリシーアクションは、アクションの前にプレフィックス を使用しますrepostspace:。例えば、re:Post Private CreateSpace API オペレーションを実行するアクセス許可を付与するには、ポリシーに repostspace:CreateSpaceアクションを含めます。ポリシーステートメントには、 Actionまたは NotAction要素を含める必要があります。 re:Post Private は、このサービスで実行できるタスクを記述する独自のアクションのセットを定義します。

単一ステートメントに複数アクションを指定するには、次のようにカンマで区切ります:

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

ワイルドカード (*) を使用して複数アクションを指定できます。例えば、Describe という単語で始まるすべてのアクションを指定するには、次のアクションを含めます。

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

re:Post Private アクションのリストを確認するには、IAM ユーザーガイドの「re:Post Private で定義されるアクション」を参照してください。

リソース

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource 要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

条件キー

re:Post Private はサービス固有の条件キーを提供しませんが、グローバル条件キーの使用をサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS「 グローバル条件コンテキストキー」を参照してください。

例

re:Post Private アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS re:Post Private アイデンティティベースのポリシーの例。

re: プライベートリソースベースのポリシーの投稿

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシー や Amazon S3 バケットポリシー があげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または AWS サービスを含めることができます。リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

re:Post Private はリソースベースのポリシーをサポートしていません。

タグに基づく認可

re:Post Private は、リソースのタグ付けまたはタグに基づいたアクセスの制御をサポートしています。詳細については、「タグ を使用した AWS リソースへのアクセスの制御」を参照してください。

re: プライベート IAM ロールの投稿

IAM ロールは、特定のアクセス許可を持つ AWS アカウント内のエンティティです。

re:Post Private での一時的な認証情報の使用

フェデレーションでサインインしたり、IAM ロールを引き受けたり、クロスアカウント ロールを引き受けたりするには、一時的な認証情報を使用することを強くお勧めします。一時的なセキュリ

ティ認証情報を取得するには、 AssumeRoleや などの AWS STS API オペレーションを呼び出しますGetFederationToken。

re:Post Private は、一時的な認証情報の使用をサポートしています。

サービスリンクロール

サービスにリンクされたロールを使用すると、 AWS サービスは他の サービスのリソースにアクセスして、ユーザーに代わってアクションを実行できます。サービスリンクロールは IAM アカウント内に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。

サービスロール

この機能を使用すると、サービスがサービスロールを引き受けることができます。このロールにより、サービスは他の サービスのリソースにアクセスして、ユーザーに代わってアクションを実行できます。詳細については、「AWS サービス にアクセス許可を委任するロールの作成」を参照してください。サービスロールは、IAM アカウントに表示され、アカウントによって所有されます。つまり、IAM 管理者は、このロールの権限を変更できます。ただし、それにより、サービスの機能が損なわれる場合があります。

re:Post Private のサービスにリンクされたロールの使用

AWS re:Post Private は AWS Identity and Access Management (IAM) サービスにリンクされたロール を使用します。サービスにリンクされたロールは、re:Post Private に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは re:Post Private によって事前定義されており、サービスがユーザーに代わって他の AWS サービスを呼び出すために必要なすべてのアクセス許可が含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がないため、re:Post Private の設定が簡単になります。re:Post Private は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、re:Post Private のみがそのロールを引き受けることができます。定義されるアクセス権限には、信頼ポリシーやアクセス許可ポリシーなどがあり、そのアクセス許可ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連動するAWS サービス」を開き、サービスにリンクされたロールの列内で「はい」と表記されたサービスをご確認ください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

re:Post Private のサービスにリンクされたロールのアクセス許可

re:Post Private は、 という名前のサービスにリンクされたロールを使用しますAWSServiceRoleForrePostPrivate。re:Post Private はこのサービスにリンクされたロールを使用してデータを に発行します CloudWatch。

AWSServiceRoleForrePostPrivate サービスにリンクされたロールは、次のサービスを信頼してロールを引き受けます。

- `repostspace.amazonaws.com`

という名前のロールアクセス許可ポリシーAWSrePostPrivateCloudWatchAccessにより、re:Post Private は指定されたリソースに対して次のアクションを実行できます。

- でのアクションcloudwatch: PutMetricData

ユーザー、グループ、ロールなどがサービスにリンクされたロールを作成、編集、削除できるようにするには、アクセス権限を設定する必要があります。詳細については、 IAM ユーザーガイド の「サービスリンクロールのアクセス許可」を参照してください。

詳細については、「AWSrePostPrivateCloudWatchAccess」を参照してください。

re:Post Private のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。 AWS Management Console、、 AWS CLIまたは AWS API で最初のプライベート re:Post を作成すると、re:Post Private がサービスにリンクされたロールを作成します。

> **Important**
>
> このサービスリンクロールは、このロールでサポートされている機能を使用する別のサービスでアクションが完了した場合にアカウントに表示されます。また、2023 年 12 月 1 日より前に re:Post Private サービスを使用していた場合、サービスにリンクされたロールのサポートが開始されると、re:Post Private はアカウントにAWSServiceRoleForrePostPrivateロールを作成しました。詳細については、「 に新しいロールが表示されました AWS アカウント」を参照してください。

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。最初のプライベート re:Post を作成すると、re:Post Private によってサービスにリンクされたロールが再度作成されます。

AWS CLI または AWS API で、サービス名を使用して`repostspace.amazonaws.com`サービスにリンクされたロールを作成します。詳細については、IAM ユーザーガイドの「サービスリンクロールの作成」を参照してください。このサービスリンクロールを削除しても、同じ方法でロールを再作成できます。

re:Post Private のサービスにリンクされたロールの編集

re:Post Private では、`AWSServiceRoleForrePostPrivate`サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、IAM ユーザーガイドの「サービスリンクロールの編集」を参照してください。

re:Post Private のサービスにリンクされたロールの削除

`AWSServiceRoleForrePostPrivate` ロールを手動で削除する必要はありません。 AWS Management Console、、 AWS CLIまたは AWS API でプライベート re:Post を削除すると、re:Post Private によってサービスにリンクされたロールが削除されます。

IAM コンソール、、または AWS API を使用して AWS CLI、サービスにリンクされたロールを手動で削除することもできます。

サービスにリンクされたロールを IAM で手動削除するには

IAM コンソール、、または AWS API を使用して AWS CLI、 AWSServiceRoleForrePostPrivate サービスにリンクされたロールを削除します。詳細については、IAM ユーザーガイドのサービスにリンクされたロールの削除を参照してください。

re:Post Private サービスにリンクされたロールでサポートされているリージョン

re:Post Private は、サービスが利用可能な AWS リージョンでサービスにリンクされたロールの使用をサポートしています。

リージョン名	リージョン識別子	re:Post Private でのサポート
米国東部 (バージニア北部)	us-east-1	はい
米国東部 (オハイオ)	us-east-2	なし
米国西部 (北カリフォルニア)	us-west-1	なし
米国西部 (オレゴン)	us-west-2	はい
アフリカ (ケープタウン)	af-south-1	いいえ
アジアパシフィック (香港)	ap-east-1	いいえ
アジアパシフィック (ジャカルタ)	ap-southeast-3	いいえ
アジアパシフィック (ムンバイ)	ap-south-1	なし
アジアパシフィック (大阪)	ap-northeast-3	いいえ
アジアパシフィック (ソウル)	ap-northeast-2	なし
アジアパシフィック (シンガポール)	ap-southeast-1	はい
アジアパシフィック (シドニー)	ap-southeast-2	はい
アジアパシフィック (東京)	ap-northeast-1	なし
カナダ (中部)	ca-central-1	はい
欧州 (フランクフルト)	eu-central-1	はい
欧州 (アイルランド)	eu-west-1	はい
欧州 (ロンドン)	eu-west-2	なし
欧州 (ミラノ)	eu-south-1	いいえ
欧州 (パリ)	eu-west-3	なし
欧州 (ストックホルム)	eu-north-1	なし

リージョン名	リージョン識別子	re:Post Private でのサポート
中東 (バーレーン)	me-south-1	なし
中東 (アラブ首長国連邦)	me-central-1	なし
南米 (サンパウロ)	sa-east-1	なし

AWS re:Post Private アイデンティティベースのポリシーの例

> **Note**
>
> セキュリティを強化するために、可能な限り IAM ユーザーではなくフェデレーティッドユーザーを作成してください。

デフォルトでは、 AWS Identity and Access Management ユーザーとロールには AWS re:Post Private リソースを作成または変更するアクセス許可はありません。また、、 AWS Management Console AWS CLI、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、ユーザーとロールに必要な、指定されたリソースで特定の API オペレーションを実行する権限をユーザーとロールに付与する IAM ポリシーを作成する必要があります。続いて、管理者はそれらの権限が必要な IAM ユーザーまたはグループにそのポリシーをアタッチする必要があります。

これらサンプルの、JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成 (コンソール)」を参照してください。

トピック

- ポリシーのベストプラクティス
- ユーザーが自分の権限を表示できるようにする

ポリシーのベストプラクティス

ID ベースのポリシーは、アカウント内で re:Post プライベートリソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生

する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、IAM ユーザーガイドのIAM でのポリシーとアクセス許可を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を通じてサービスアクションが使用される場合に AWS サービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素:条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、IAM ユーザーガイドのIAM Access Analyzer ポリシーの検証を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイドのMFA 保護 API アクセスの設定を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティベストプラクティス」を参照してください。

ユーザーが自分の権限を表示できるようにする

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

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

インラインポリシー

インラインポリシーは、ユーザーが作成して管理するポリシーです。インラインポリシーをユーザー、グループ、またはロールに直接埋め込むことができます。次のポリシー例は、AWS re:Post Private アクションを実行するアクセス許可を割り当てる方法を示しています。インラインポリシーの一般的な情報については、AWS IAM ユーザーガイドの「IAM ポリシーの管理」を参照してください。 AWS Management Console、 AWS Command Line Interface (AWS CLI)、または AWS Identity and Access Management API を使用して、インラインポリシーを作成して埋め込むことができます。

トピック

- re:Post Private への読み取り専用アクセス
- re:Post Private へのフルアクセス

re:Post Private への読み取り専用アクセス

次のポリシーは、IAM Identity Center および re:Post Private コンソールのユーザーに読み取りアクセスを許可します。このポリシーにより、ユーザーは読み取り専用の re:Post Private アクションを実行できます。

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

re:Post Private へのフルアクセス

次のポリシーは、IAM Identity Center および re:Post Private コンソールのユーザーにフルアクセスを付与します。このポリシーにより、ユーザーはすべての re:Post Private アクションを実行できます。

```
{
    "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 AWS re:Post Private の マネージドポリシー

AWS 管理ポリシーを使用すると、ユーザー、グループ、ロールにアクセス許可を追加する方が、自分でポリシーを作成するよりも簡単になります。チームに必要な許可のみを提供する IAM カスタマー管理ポリシーを作成するには、時間と専門知識が必要です。 AWS 管理ポリシーを使用して、すぐに開始できます。これらのポリシーは一般的なユースケースを対象としており、 AWS アカウントで利用できます。 AWS 管理ポリシーの詳細については、「IAM ユーザーガイド」の「 AWS 管理ポリシー」を参照してください。

AWS サービスは、 AWS マネージドポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可は変更できません。サービスは、 AWS マネージドポリシーに新しい機能をサポートするために追加のアクセス許可を追加することがあります。この種の更新は、ポリシーがアタッチされているすべてのアイデンティティ (ユーザー、グループ、ロール) に影響を与えます。サービスは、新機能の起動時または新しいオペレーションが利用可能になったときに、 AWS マネージドポリシーを更新する可能性が最も高くなります。サービスは AWS マネージドポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が損なわれることはありません。

さらに、 は、複数の サービスにまたがる職務機能の マネージドポリシー AWS をサポートします。例えば、 `ReadOnlyAccess` AWS 管理ポリシーは、すべての AWS サービスとリソースへの読み取り専用アクセスを提供します。サービスが新機能を起動すると、 は新しいオペレーションとリソースの読み取り専用アクセス許可 AWS を追加します。詳細については、「IAM ユーザーガイド」の「AWS 管理ポリシー」を参照してください。

トピック

- AWS マネージドポリシー： AWSRepostSpaceSupportOperationsPolicy
- AWS マネージドポリシー： AWSrePostPrivateCloudWatchAccess
- AWS re:Post Private updates to AWS マネージドポリシー

AWS マネージドポリシー： AWSRepostSpaceSupportOperationsPolicy

このポリシーにより、AWS re:Post Private サービスは re:Post Private ウェブアプリケーションを通じて作成された AWS Support ケースを作成、管理、解決できます。

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

AWS マネージドポリシー： AWSrePostPrivateCloudWatchAccess

このポリシーにより、re:Post Private サービスは にデータを公開できます CloudWatch。

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

```
    "cloudwatch:PutMetricData"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "cloudwatch:namespace": [
      "AWS/rePostPrivate",
      "AWS/Usage"
     ]
    }
   }
  }
 ]
}
```

AWS re:Post Private updates to AWS マネージドポリシー

re:Post Private の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。このページへの変更に関する自動アラートについては、ドキュメント履歴 ページの RSS フィードを購読してください。

次の表は、2023 年 11 月 26 日以後の re:Post プライベート管理ポリシーの重要な更新を示しています。

変更	説明	日付
新しいポリシー - AWSrePostPrivateCloudWatchAccess	にデータを発行するための新しい マネージドポリシー CloudWatch	2023 年 11 月 26 日
新しいポリシー - AWSRepostSpaceSupportOperationsPolicy	AWS re:Post Private の AWS サポート機能の新しい マネージドポリシー	2023 年 11 月 26 日
re:Post Private が変更の追跡を開始	re:Post Private が AWS マネージドポリシーの変更の追跡を開始	2023 年 11 月 26 日

AWS re:Post Private アイデンティティとアクセスのトラブルシューティング

re:Post Private と IAM を使用する際に発生する可能性がある一般的な問題の診断と修正には、以下の情報を参考にしてください。

トピック

- re:Post Private でアクションを実行する権限がない
- iam を実行する権限がありません。PassRole
- 自分の 以外のユーザーに re:Post プライベートリソース AWS アカウント へのアクセスを許可したい

re:Post Private でアクションを実行する権限がない

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なrepostPrivate:*GetWidget* アクセス許可を持っていない場合に発生するものです。

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

この場合、repostPrivate:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

iam を実行する権限がありません。PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して re:Post Private にロールを渡すことができるようにする必要があります。

一部の AWS サービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、そのサービスに既存のロールを渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

次の例のエラーは、 という IAM marymajor ユーザーがコンソールを使用して re:Post Private でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに iam:PassRole アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

自分の 以外のユーザーに re:Post プライベートリソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- re:Post Private がこれらの機能をサポートしているかどうかを確認するには、「」を参照してくださいre:Post Private が IAM と連携する方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイドの外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

AWS re:Post Private のコンプライアンス検証

AWS サービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS サービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS サービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

  > **Note**
  >
  > すべての AWS サービス が HIPAA の対象となるわけではありません。詳細については、HIPAA 対応サービスのリファレンスを参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド – コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS サービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config

- AWS Security Hub – これにより AWS サービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、Security Hub のコントロールリファレンスを参照してください。
- Amazon GuardDuty — これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、、、ワークロード、コンテナ、データに対する潜在的な脅威 AWS サービス を検出します。 GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件への対応に役立ちます。
- AWS Audit Manager – これにより AWS サービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

AWS re:Post Private の耐障害性

AWS グローバルインフラストラクチャは AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供し、低レイテンシー、高スループット、高冗長ネットワークで接続されます。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

AWS re:Post Private のインフラストラクチャセキュリティ

マネージドサービスである AWS re:Post Private は、ホワイトペーパー「Amazon Web Services: セキュリティプロセスの概要」に記載されている AWS グローバルネットワークセキュリティの手順で保護されています。

AWS が公開した API コールを使用して、ネットワーク経由で re:Post Private にアクセスします。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライ

アントでサポートされている必要があります。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

さらに、リクエストは、アクセスキー ID とプリン AWS Identity and Access Management シパルに関連付けられたシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時セキュリティ認証情報を生成し、リクエストに署名することもできます。

リポストのプライベートクォータ

AWS re: Post Private では、特定のリージョンのアカウントで使用できるプライベート re: Posts を提供しています。AWSre: Post Private にサインアップすると、作成できるプライベート re: POST の数とプライベート re: Posts のサイズにデフォルトクォータ (以前は制限と呼ばれていました) AWS が設定されます。

Service Quotas

以下は、アカウントの re: Post Private のデフォルトクォータです。AWSService Quotas コンソールを使用してデフォルトクォータを表示できます。これらのクォータはいずれも調整できません。クォータの増額をリクエストすることはできません。

リソース	デフォルト	説明	引き上げ可能
非公開の re: 投稿数	3	現在のリージョンにおけるこのアカウント内の非公開の re: Posts の最大数。	No
無料のプライベート re: POST サイズ	10	無料のプライベート re: Post の最大サイズ (GB 単位)。	No
プライベート re: POST の標準サイズ	100	スタンダードプライベート re: POST の最大サイズ (GB 単位)。	No

API スロットリング制限

re: Post Private では、アカウントごと、リージョンごとに以下のスロットリング制限が適用されます。これらのクォータを増やすことはできません。

アクション	トークンの補充率	リクエストのレート	
CreateSpace	1	1	

アクション	トークンの補充率	リクエストのレート
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

プライベート re:Post を作成、設定、カスタマイズする

トピック

- 新しいプライベート re:Post を作成する
- re:Post Private での AWS Support ケースの作成と管理へのアクセスの管理
- を使用してユーザーアクセスを設定および管理する AWS IAM Identity Center
- プライベート re:Post をカスタマイズする
- プライベート re:Post にユーザーを招待する

新しいプライベート re:Post を作成する

新しいプライベート re:Post を作成するには、次の手順に従います。

1. re:Post プライベートコンソールを https://console.aws.amazon.com/repost-private/ で開きます。
2. コンソールのホームページで、プライベート re:Post の作成を選択します。
3. アカウントに IAM Identity Center がまだ設定されていない場合は、Open Identity Center を選択します。AWS IAM Identity Center ユーザーガイドの「開始方法」の手順に従います。
4. 「プライベート re:Post の作成」ページの「料金表」で、ユースケースに基づいて無料利用枠または標準利用枠を選択します。アカウントにすでに 無料利用枠を使用している場合、無料利用枠オプションは使用できません。
5. 詳細 で、次の操作を行います。

   名前に、プライベート re:Post の一意の名前を入力します。

   (オプション) 説明 に、プライベート re:Post の簡単な説明を入力します。

   カスタムサブドメイン には、サブドメインのカスタム名を入力します。
6. (オプション) データ暗号化設定をカスタマイズするには、「データ暗号化」で「暗号化設定のカスタマイズ」を選択します。次に、次のいずれかのアクションを実行します。

   AWS KMS キーの選択 で、 AWS Key Management Service キーまたは Amazon リソースネーム (ARN) を選択します。

   -または-

AWS KMS キーの作成を選択します。次に、AWS KMS キー を作成します。

7. (オプション) サポートケース統合のサービスアクセス で、この re:Post のサービスアクセスを有効にする を選択します。

> **Note**
>
> プライベート re:Post を作成した後で、このオプションをオンにすることもできます。

以下の既存の IAM ロールを選択するか、IAM コンソール で新しいロールを作成してください で、検索バーを使用して既存の IAM ロールを検索します。

-または-

IAM コンソール で新しいロールの作成を選択します。

新しいロールを作成する場合は、「」の手順に従いますIAM ロールを作成する。

既存のサービスロールを使用する場合は、検索バーで、使用するロールの ARN を入力します。ドロップダウンリストからロールを選択します。

詳細については、「re:Post Private での AWS Support ケースの作成と管理へのアクセスの管理」を参照してください。

8. (オプション) タグ で、新しいタグを追加 を選択します。次に、次の情報を入力します。

キー に、カスタムタグキーを入力します。

値 に、カスタムタグ値を入力します。

タグをさらに追加するには、[Add new tag] (新しいタグを追加) を選択します。

9. この re:Post の作成を選択します。

プライベート re:Post が作成されていることが確認ページに表示されます。プライベート re:Post のステータスは、ステータス フィールドで確認できます。プライベート re:Post が作成されると、ステータスフィールドには の作成と表示されます。

プライベート re:Post が作成されるまでに約 30 分かかります。プライベート re:Post の準備ができたら、ステータスフィールドにオンライン が表示されます。設定 タブの下にリストされているプ

ライベート re:Post の AWS 生成サブドメインを使用して、プライベート re:Post にアクセスできます。レビューが完了したら、設定タブでプライベート re:Post のカスタムサブドメインを表示できます。

re:Post Private での AWS Support ケースの作成と管理へのアクセスの管理

AWS re:Post Private からの AWS Support ケースの作成と管理へのアクセスを管理するには、 (IAM) ロールを作成 AWS Identity and Access Management する必要があります。このロールは、次の AWS Support アクションを実行します。

- CreateCase
- AddCommunicationToCase
- ResolveCase

IAM ロールを作成したら、IAM ポリシーをこのロールにアタッチして、ロールがこれらのアクションを完了するために必要なアクセス許可を持つようにします。re:Post プライベートコンソールでプライベート re:Post を作成するときに、このロールを選択します。

プライベート re:Post のユーザーは、IAM ロールに付与するのと同じアクセス許可を持ちます。

> **Important**
>
> IAM ロールまたは IAM ポリシーを変更すると、変更は設定したプライベート re:Post に適用されます。

IAM ロールとポリシーを作成するときは、以下の手順に従います。

トピック

- AWS 管理ポリシーを使用するか、カスタマー管理ポリシーを作成する
- IAM ポリシーの例
- IAM ロールを作成する
- トラブルシューティング

AWS 管理ポリシーを使用するか、カスタマー管理ポリシーを作成する

ロールのアクセス許可を付与するには、 AWS 管理ポリシーまたはカスタマー管理ポリシーのいずれかを使用できます。

> **Tip**
>
> ポリシーを手動で作成しない場合は、代わりに AWS 管理ポリシーを使用して、この手順をスキップすることをお勧めします。管理ポリシーには、 に必要なアクセス許可が自動的に付与されます AWS Support。ユーザーがポリシーを手動で更新する必要はありません。詳細については、「AWS マネージドポリシー： AWSRepostSpaceSupportOperationsPolicy」を参照してください。

ロール用のカスタマー管理ポリシーを作成するには、次の手順に従います。この手順では、IAM コンソールの JSON ポリシーエディタを使用します。

re:Post Private のカスタマー管理ポリシーを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. ナビゲーションペインで、ポリシー を選択します。
3. ポリシーの作成を選択します。
4. [JSON] タブを選択します。
5. JSON を入力し、エディタでデフォルトの JSON を置き換えます。ポリシーの例を利用できます。
6. [次へ: タグ] を選択します。
7. (オプション) キーバリューペアとしてのタグを使用して、メタデータをポリシーに追加することができます。
8. [次へ: 確認] を選択します。
9. [Review policy] (ポリシーの確認) ページで、名前 (*rePostPrivateSupportPolicy* など) と説明 (任意) を入力します。
10. [Summary] (概要) ページを調べて、ポリシーで許可されるアクセス許可を確認し、[Create policy] (ポリシーの作成) を選択します。

このポリシーによって、このロールが実行できるアクションが定義されます。詳細については、IAM ユーザーガイドのIAM ポリシーの作成 (コンソール) を参照してください。

IAM ポリシーの例

IAM ロールには、以下のポリシーの例をアタッチできます。このポリシーは、ロールが に必要なすべてのアクションに対する完全なアクセス許可を持つことを許可します AWS Support。ロールを使用してプライベート re:Post を設定すると、プライベート re:Post のすべてのユーザーが同じアクセス許可を持ちます。

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

> **Note**
>
> re:Post Private の AWS マネージドポリシーのリストについては、「」を参照してくださいAWS AWS re:Post Private の マネージドポリシー。

ポリシーを更新して、 からアクセス許可を削除できます AWS Support。

各アクションの説明については、「サービス認証リファレンス」の以下のトピックを参照してください。

- AWS Support のアクション、リソース、条件キー
- 「Service Quotas のアクション、リソース、および条件キー」
- のアクション、リソース、および条件キー AWS Identity and Access Management

IAM ロールを作成する

このポリシーを作成したら、IAM ロールを作成し、そのロールにポリシーをアタッチする必要があります。re:Post Private コンソールでプライベート re:Post を作成するときに、このロールを選択します。

AWS Support ケースの作成と管理用のロールを作成するには

1. にサインイン AWS Management Console し、https://console.aws.amazon.com/iam/ で IAM コンソールを開きます。
2. ナビゲーションペインで ロール を選択してから、ロールを作成する を選択します。
3. [Trusted entity type] (信頼されたエンティティのタイプ) で、[Custom trust policy] (カスタム信頼ポリシー) を選択します。
4. カスタム信頼ポリシー には、次のように入力します。

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

5. [次へ] を選択します。
6. アクセス許可ポリシー の検索バーに、 などの作成した AWS 管理ポリシーまたはカスタマー管理ポリシーを入力します*rePostPrivateSupportPolicy*。サービスに付与するアクセス許可ポリシーの横にあるチェックボックスをオンにします。

7. [次へ] を選択します。
8. 名前、レビュー、作成 ページのロール名 に、 などの名前を入力しま す*rePostPrivateSupportRole*。
9. (オプション) [説明] にロールの説明を入力します。
10. 信頼ポリシーとアクセス許可を確認します。
11. (オプション) キーと値のペアとしてタグを使用し、メタデータをロールに追加できます。IAM でのタグの使用の詳細については、「IAM リソースのタグ付け」を参照してください。
12. [ロールの作成] を選択します。re:Post Private コンソールでプライベート re:Post を設定するときに、このロールを選択できるようになりました。新しいプライベート re:Post を作成する を参照してください。

詳細については、「IAM ユーザーガイド」の「 AWS サービスのロールの作成 (コンソール) 」を参照してください。

トラブルシューティング

re:Post Private へのアクセスを管理するには、以下のトピックを参照してください。

目次

- プライベート re:Post の特定のユーザーを特定のアクションに制限したい
- プライベート re:Post を設定すると、作成した IAM ロールが表示されない
- IAM ロールにアクセス許可が付与されていない
- IAM ロールが有効ではないというエラー

プライベート re:Post の特定のユーザーを特定のアクションに制限したい

デフォルトでは、プライベート re:Post のユーザーは、作成した IAM ロールにアタッチする IAM ポリシーで指定されたのと同じアクセス許可を持ちます。つまり、プライベート re:Post 内のすべてのユーザーは、 AWS アカウント または IAM ユーザーの有無にかかわらず、 AWS Support ケースを作成および管理するための読み取りまたは書き込みアクセス権を持ちます。

推奨されるベストプラクティスを以下に示します：

- に対して最低限必要なアクセス許可を持つ IAM ポリシーを使用します AWS Support。AWS マネージドポリシー： AWSRepostSpaceSupportOperationsPolicy を参照してください。

プライベート re:Post を設定すると、作成した IAM ロールが表示されない

re:Post Private; list の IAM ロールに IAM ロールが表示されない場合は、ロールに re:Post Private が信頼されたエンティティとして含まれていないか、ロールが削除されたことを意味します。既存のロールを更新するか、新しいロールを作成します。IAM ロールを作成する を参照してください。

IAM ロールにアクセス許可が付与されていない

プライベート re:Post 用に作成する IAM ロールには、必要なアクションを実行するためのアクセス許可が必要です。例えば、プライベート re:Post のユーザーにサポートケースを作成させる場合、ロールには アクセス`support:CreateCase`許可が必要です。 re:Post Private は、これらのアクションを実行するためにこのロールを引き受けます。

のアクセス許可が不足しているというエラーが表示された場合は AWS Support、ロールにアタッチされたポリシーに必要なアクセス許可があることを確認します。

前述の「IAM ポリシーの例」を参照してください。

IAM ロールが有効ではないというエラー

プライベート re:Post 設定に正しいロールが選択されていることを確認します。

を使用してユーザーアクセスを設定および管理する AWS IAM Identity Center

re:Post Private は と統合 AWS IAM Identity Center して、組織のワークフォースに ID フェデレーションを提供します。IAM Identity Center を使用して、組織からユーザーを作成または接続し、すべての AWS アカウントとアプリケーションへのアクセスを一元管理します。IAM Identity Center の詳細については、「AWS IAM Identity Center とは (AWS Single Sign-On の後継サービス)」を参照してください。IAM Identity Center の開始方法の詳細については、「 の開始方法」を参照してください。IAM Identity Center を使用するには、アカウントに対して も AWS Organizations 有効化されている必要があります。

プライベート re:Post をカスタマイズする

プライベート re:Post の作成後に、1 人以上の管理者を追加できます。管理者は re:Post プライベートアプリケーションを使用して、プライベート re:Post を起動し、その中のユーザーを管理します。プライベート re:Post のブランドをカスタマイズしたり、コンテンツを分類するためのタグを

追加したり、コンテンツの自動母集団の対象となるトピックを選択したりできます。詳細については、「AWS re:Post プライベート管理ガイド」を参照してください。

プライベート re:Post にユーザーを招待する

プライベート re:Post の作成後に、1 人以上のユーザーをプライベート re:Post に追加できます。プライベート re:Post 内でコラボレーションするようにユーザーを招待できます。ユーザーは re:Post プライベートアプリケーションを使用して、設定した認証情報を使用してサインインします。プライベート re:Post にサインインすると、ユーザーは目的のトピックを対象としたカスタマイズされたトレーニングや技術コンテンツなど、既存のコンテンツを閲覧または検索できます。詳細については、「AWS re:Post プライベートユーザーガイド」を参照してください。

re: POST プライベートコンソールでプライベート re: POST を管理

このセクションでは、AWS re: Post プライベートコンソールでプライベート re: POST を管理する方法について説明します。

トピック

- プライベート re: POST にユーザーとグループを追加します。
- プライベート re: POST のグループにユーザーを追加します。
- ユーザーとグループをプライベート re: POST に招待します。
- プライベート re: POST のユーザーを管理者に昇格させます。
- プライベート re: POST からユーザーまたはグループを削除します。
- 非公開の re: POST AWS に従業員を追加または削除する
- re: POST プライベートからプライベート re: POST を削除する

プライベート re: POST にユーザーとグループを追加します。

管理者の場合は、プライベート re: POST にユーザーとグループを追加できます。

プライベートの re: POST にユーザーを追加します。

1. https://console.aws.amazon.com/repost-private/ にある re: POST プライベートコンソールを開きます。
2. ナビゲーションペインで、「すべてのマイプライベート re: Posts」を選択します。
3. 管理したい非公開の re: POST を選択します。
4. [Users] (ユーザー) タブを選択します。
5. 「ユーザー」で「ユーザーとグループを追加」を選択します。
6. リストから、プライベート re: POST に追加したいユーザーを選択します。次に、「割り当て」を選択します。

選択したユーザーがプライベート re: POST に追加され、「ユーザー」タブに表示されます。

プライベートの re: POST にグループを追加します。

1. https://console.aws.amazon.com/repost-private/ にある re: POST プライベートコンソールを開きます。
2. ナビゲーションペインで、「すべてのマイプライベート re: Posts」を選択します。
3. 管理したい非公開の re: POST を選択します。
4. [Groups] (グループ) タブを選択します。
5. [ユーザーとグループを追加] を選択します。
6. リストから、プライベート re: POST に追加したいグループを選択します。次に、「割り当て」を選択します。

選択したグループがプライベート re: POST に追加され、「グループ」タブに一覧表示されます。

プライベート re: POST のグループにユーザーを追加します。

IAM Identity Center を使用して、プライベート re: POST の既存のグループに新しいユーザーを追加します。詳細については、『AWS IAM Identity Center ユーザーガイド』の「グループへのユーザーの追加」を参照してください。

ユーザーとグループをプライベート re: POST に招待します。

次の手順に従って、AWS re: Post Private のプライベート re: Post にユーザーとグループを招待します。

1. https://console.aws.amazon.com/repost-private/ の re: POST プライベートコンソールを開きます。
2. ナビゲーションペインで、「すべてのマイプライベート re: Posts」を選択します。
3. 管理したい非公開の re: POST を選択します。
4. プライベートの re: POST にユーザーを招待するには、「ユーザー」タブを選択します。

   リストから、プライベート re: POST に招待したいユーザーを選択します。次に、「re: POST するユーザーをオンボーディングする」を選択します。
5. 「この非公開の re: POST への登録ユーザー」ダイアログボックスに、以下の情報を入力します。

   [件名] には、送信するメールメッセージの件名を入力します。

   Body には、プライベート re: POST のウェルカムメッセージを入力します。

「オンボーディングメールを送信」を選択します。

6. プライベートな re: POST にグループを招待するには、「グループ」タブを選択します。

   リストから、プライベート re: POST に招待したいグループを選択します。次に、re: POST するオンボードグループを選択します。

7. 「この非公開の re: POST へのオンボードグループ」ダイアログボックスに、以下の情報を入力します。

   [件名] には、送信するメールメッセージの件名を入力します。

   Body には、プライベート re: POST のウェルカムメッセージを入力します。

   「オンボーディングメールを送信」を選択します。

選択したすべてのユーザーとグループに、非公開の re: POST へのサインイン方法に関する情報が記載されたウェルカムメッセージが送信されます。

プライベート re: POST のユーザーを管理者に昇格させます。

プライベート re: POST ユーザーを管理者に昇格させるには、以下の手順に従ってください。

1. https://console.aws.amazon.com/repost-private/ で re: Post プライベートコンソールを開きます。
2. ナビゲーションペインで、「すべてのマイプライベート re: Posts」を選択します。
3. 管理したい非公開の re: POST を選択します。
4. [Users] (ユーザー) タブを選択します。
5. 管理者に昇格させたいユーザーを 1 人以上選択します。
6. [ロールを編集] を選択し、[管理者に設定] を選択します。

選択したユーザーが管理者に昇格します。「ユーザ」タブでは、これらのユーザのロールが「管理者」に更新されます。

プライベート re: POST からユーザーまたはグループを削除します。

管理者の場合は、プライベート re: POST からユーザーまたはグループを削除できます。

プライベート re: POST からユーザーを削除する

1. https://console.aws.amazon.com/repost-private/ にある re: POST プライベートコンソールを開きます。
2. ナビゲーションペインで、「すべてのマイプライベート re: Posts」を選択します。
3. 管理したい非公開の re: POST を選択します。
4. 「ユーザー」で、プライベートの re: POST から削除したいユーザーをリストから選択します。次に [削除] を選択します。

選択したユーザーがプライベート re: POST から削除されます。削除したユーザーに関する情報は「ユーザー」タブに表示されなくなります。

プライベート re: POST からグループを削除する

1. https://console.aws.amazon.com/repost-private/ にある re: POST プライベートコンソールを開きます。
2. ナビゲーションペインで、「すべてのマイプライベート re: Posts」を選択します。
3. 管理したい非公開の re: POST を選択します。
4. [Groups] (グループ) タブを選択します。
5. リストから、プライベート re: POST から削除したいグループを選択します。次に [削除] を選択します。

選択したグループがプライベート re: POST から削除されます。削除したグループに関する情報は「グループ」タブに表示されなくなります。

非公開の re: POST AWS に従業員を追加または削除する

エンタープライズまたはエンタープライズオンランプSupport プランをお持ちの場合は、プライベート re: POST に AWS 従業員を追加または削除できます。詳細については、コンシェルジュSupport またはテクニカルアカウントマネージャー (TAM) にお問い合わせください。

re: POST プライベートからプライベート re: POST を削除する

AWS re: Post プライベートでプライベート re: POST を削除するには、以下の手順に従ってください。

1. https://console.aws.amazon.com/repost-private/ の re: POST プライベートコンソールを開きます。
2. ナビゲーションペインで、「すべてのマイプライベート re: Posts」を選択します。
3. 管理したい非公開の re: POST を選択し、「削除」を選択します。
4. すべてのオプションを選択して、非公開の re: POST とそれに関連するデータを完全に削除することを確認し、確定します。

> **Important**
>
> 非公開の re: POST を削除すると、非公開の re: POST に関連する設定情報はすべて削除されます。非公開の re: POST を削除すると、そこからコンテンツを復元することはできません。

5. 追加の書面による同意を求めるメッセージが表示されたら、非公開の re: POST の名前を入力します。その後、[Delete] (削除) をクリックします。

非公開の re: POST が削除されるまで約 30 分かかります。

AWS リポストプライベートモニタリング

モニタリングは、AWS re: Post Private AWS やその他のソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 AWSには、re: Post Private を監視したり、問題が発生した場合に報告したり、必要に応じて自動アクションを実行したりするための以下のモニタリングツールが用意されています。

- Amazon は、 CloudWatchAWSAWSユーザーのリソースと実行中のアプリケーションをリアルタイムで監視します。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、および指定したメトリクスが指定したしきい値に達したときに通知またはアクションを実行するアラームの設定を行うことができます。たとえば、Amazon EC2 インスタンスの CPU CloudWatch 使用率やその他のメトリックスを追跡し、必要に応じて新しいインスタンスを自動的に起動できます。詳細については、Amazon CloudWatch ユーザーガイドを参照してください。
- AWS CloudTrailによって、またはお客様のために行われた API AWS アカウント 呼び出しと関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。AWS を呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrailユーザーガイドを参照してください。

アマゾンでの AWS re: Post プライベートモニタリング CloudWatch

Amazon を使用して AWS re: Post Private をモニタリングできます。Amazon は未加工データを収集し CloudWatch、それを読み取り可能でほぼリアルタイムのメトリックスに処理します。これらの統計は 15 か月間保存されるため、履歴情報にアクセスして、ウェブアプリケーションやサービスのパフォーマンスをより的確に把握できます。また、特定のしきい値をモニタリングするアラームを設定し、しきい値に達したときに通知を送信したりアクションを実行したりできます。詳細については、Amazon CloudWatch ユーザーガイドを参照してください。

re: Post Private サービスはネームスペース内の以下のメトリックスを報告しますAWS/rePostPrivate。

メトリクス	説明
NumberOfSpaces	現在のアカウント内の非公開の re: POST の数。 単位はカウント

メトリクス	説明
NumberOfUsers	プライベート re: POST のユーザー数。このメトリクスは SpaceID をディメンションとして使用します。 単位はカウント
ContentSize	プライベート re: POST 内のコンテンツの量。このメトリクスは SpaceID をディメンションとして使用します。 単位: バイト

re: Post Private メトリクスでは以下のディメンションがサポートされています。

ディメンション	説明
spaceId	プライベート re: POST のユニークな識別子。

使用した AWS re: POST プライベート API 呼び出しのロギング AWS CloudTrail

AWS re: Post Private はAWS CloudTrail、re: Post Private 内のユーザー、ロール、AWSまたはサービスによって実行されたアクションの記録を提供するサービスと統合されています。 CloudTrail re: Post Private のすべての API 呼び出しをイベントとしてキャプチャします。キャプチャされた呼び出しには、re: Post プライベートコンソールからの呼び出しと re: Post Private API オペレーションへのコード呼び出しが含まれます。証跡を作成すると、re: Post Private CloudTrail のイベントを含め、Amazon S3 バケットへのイベントの継続的な配信を有効にできます。トレイルを設定しなくても、 CloudTrail コンソールの [イベント履歴] に最新のイベントが表示されます。によって収集された情報を使用して CloudTrail、re: Post Private に対して行われたリクエスト、リクエストが行われた IP アドレス、リクエストの実行者、実行日時、その他の詳細情報を確認できます。

詳細については CloudTrail、『AWS CloudTrailユーザーガイド』を参照してください。

re: プライベート情報をに投稿 CloudTrail

CloudTrail AWS アカウントアカウントを作成すると有効になります。re: Post Private でアクティビティが発生すると、 CloudTrail AWSそのアクティビティはイベント履歴の他のサービスイベントと

共にイベントに記録されます。最近のイベントは、AWS アカウント で表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴の操作」を参照してください。

re: Post Private のイベントなどAWS アカウント、のイベントに関する継続的な記録については、トレイルを作成してください。トレイルを使用すると CloudTrail 、Amazon S3 バケットにログファイルを配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべてのAWS リージョン に適用されます 証跡は、AWS パーティションのすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、AWS CloudTrail ログに収集されたイベントデータをさらに分析して処理するように他のサービスを設定することもできます。詳細については、次を参照してください。

- AWS アカウントに関する証跡の作成
- CloudTrail サポート対象のサービスとインテグレーション
- の Amazon SNS 通知の設定 CloudTrail
- CloudTrail 複数のリージョンからのログファイルの受信、 CloudTrail および複数のアカウントからのログファイルの受信

re: Post Private CloudTrail アクションはすべてログに記録され、AWS re: Post プライベート API リファレンスに記載されています。re: Post Private では、以下のアクションをイベントとしてログファイルに記録できます。 CloudTrail

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

re: Post Private では、以下のアクションをイベントとしてログファイルに記録できます。AWS Support CloudTrail

- CreateCase
- AddCommunicationToCase
- ResolveCase

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストが、ルート認証情報と AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーティッドユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービスによって送信されたかどうか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

re: Post Private のログファイルエントリについて

トレイルは、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには 1 つ以上のログエントリが含まれます。イベントはあらゆるソースからの単一のリクエストを表し、リクエストされたアクションに関する情報、アクションの日時、リクエストパラメータなどが含まれます。 CloudTrail ログファイルはパブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序で表示されることはありません。

次の例は、 CloudTrail `CreateSpace`アクションを示すログエントリを示しています。

```
{
   "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"
}
```

次の例は、 CloudTrail アクションを示すログエントリを示しています。RegisterAdmin


```
{
   "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"
}
```

次の例は、 CloudTrail アクションを示すログエントリを示しています。ListSpaces

```
{
   "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"
}
```

次の例は、 CloudTrail アクションを示すログエントリを示しています。ResolveCasesourceIdentityこのログエントリの要素を使用して、ケースを解決したユーザーを特定できます。

```
 {
    "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"
    }
}
```

re:Post Private のトラブルシューティング

以下の情報は、AWS re:Post Private に関する問題のトラブルシューティングに役立ちます。

トピック

- 特定の AWS リージョンでプライベート re:Post を設定できない
- アカウントにプライベート re:Post を設定できない
- プライベート re:Post のユーザーまたはグループを管理できない

特定の AWS リージョンでプライベート re:Post を設定できない

re:Post Private は、米国東部 (バージニア北部)、米国西部 (オレゴン)、欧州 (フランクフルト)、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー)、カナダ (中部)、欧州 (アイルランド) の各リージョンでのみ利用できます。これらのリージョンのいずれかでプライベート re:Post を作成していることを確認してください。

アカウントにプライベート re:Post を設定できない

アカウント AWS IAM Identity Center で を有効にし、プライベート re:Post を作成するリージョンと同じリージョンに IAM Identity Center を設定してください。詳細については、「前提条件」を参照してください。

プライベート re:Post のユーザーまたはグループを管理できない

プライベート re:Post を編集し、プライベート re:Post 内のユーザーとグループを管理するために必要なアクセス許可があることを確認してください。詳細については、「AWS re:Post Private アイデンティティベースのポリシーの例」を参照してください。

ドキュメント履歴

次の表に、AWS re:Post Private のドキュメントリリースを示します。

変更	説明	日付
更新	サポートされているリージョンに米国東部 (バージニア北部) 、アジアパシフィック (シドニー) 、カナダ (中部) 、欧州 (アイルランド) を追加しました。	2024 年 5 月 10 日
更新	サポートされているリージョンにアジアパシフィック (シンガポール) を追加	2024 年 3 月 6 日
新しいリソース	AWS re:Post Private の AWS 管理ポリシーに関するドキュメントを追加	2023 年 11 月 26 日
初回リリース	re:Post プライベートコンソール管理ガイドの初回リリース	2023 年 11 月 26 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。