Guia de administração do console

AWS re:Post privado

AWS re:Post privado: Guia de administração do console

Table of Contents

O que é o AWS re:Post Private? 1
Acesse re:Post Private 1
Definição de preço 2
Como começar a usar 2
Pré-requisitos 3
A bordo do Re:post Private 4
Segurança 5
Proteção de dados 5
Proteger dados com criptografia 7
Criptografia em trânsito 7
Gerenciamento de chaves 7
Como o re:Post Private funciona com o IAM 7
Re:post Políticas baseadas em identidade privada 7
Re:post Políticas baseadas em recursos privados 9
Autorização baseada em tags do 9
re:postar funções privadas do IAM 9
Funções vinculadas a serviço 10
Perfis de serviço 10
Usar funções vinculadas ao serviço 10
Exemplos de políticas baseadas em identidade 14
Políticas em linha 17
AWS políticas gerenciadas 19
Solução de problemas 22
Validação de conformidade 24
Resiliência 25
Segurança da infraestrutura 25
Cotas 27
Service Quotas 27
Limites de limitação da API 27
Crie, configure e personalize seu re:post privado 29
Crie um novo re:post privado 29
Gerenciando o acesso à criação e gerenciamento de AWS Support casos no re:Post Private 31
Use uma política AWS gerenciada ou crie uma política gerenciada pelo cliente 32
Exemplo de política do IAM 33

Criar um perfil do IAM 34
Solução de problemas 35
Configurar e gerenciar o acesso do usuário 36
Personalize seu re:post privado 36
Convide usuários para seu re:post privado 37
Gerencie seu re:post privado 38
Adicionar usuários e grupos 38
Adicionar usuários a um grupo 39
Convide usuários e grupos 39
Promova um usuário a administrador 40
Remover usuários e grupos 40
Adicionar ou remover um AWS funcionário 41
Excluir um re:post privado 41
Monitoramento re:post Private 43
Monitoramento com CloudWatch 43
Registrando chamadas de API privadas re:post usando AWS CloudTrail 44
re:Publique informações privadas em CloudTrail 45
Compreendendo as entradas do arquivo de log privado do re:POST 46
Solução de problemas 52
Não consigo configurar meu re:post privado em uma região específica AWS 52
Não consigo configurar o re:post privado na minha conta 52
Não consigo gerenciar usuários ou grupos em um re:post privado 52
Histórico do documento 53
..... liv

O que é o AWS re:Post Private?

O AWS re:Post Private é uma versão privada do AWS re:Post para empresas com planos Enterprise Support ou Enterprise On-Ramp Support. Ele fornece acesso a conhecimentos e especialistas para acelerar a adoção da nuvem e aumentar a produtividade do desenvolvedor. Com o re:post privado específico da sua organização, você pode criar uma comunidade de desenvolvedores específica da organização que impulsiona a eficiência em grande escala e fornece acesso a valiosos recursos de conhecimento. Além disso, o re:Post Private centraliza conteúdo AWS técnico confiável e oferece fóruns de discussão privados para melhorar a forma como suas equipes colaboram internamente e com a AWS para remover obstáculos técnicos, acelerar a inovação e escalar com mais eficiência na nuvem.

Para obter mais informações, consulte AWS re:Post Private.

Acesse re:Post Private

Os administradores usam o console privado do AWS re:Post para criar o re:POST privado específico da organização. Quando os administradores criam um re:POST privado, eles podem nomear seu re:POST privado e definir um subdomínio em. `*.private.repost.aws` Os administradores do re:POST privado de uma organização podem configurar o acesso do usuário usando AWS IAM Identity Center e especificar uma das seguintes fontes de identidade para autenticação: diretório do Identity Center, Active Directory ou um provedor de identidade externo. Depois de configurar os usuários, os administradores do console podem atribuir uma função de administrador privado do re:POST a um ou mais usuários. Os administradores privados do re:POST podem personalizar seu aplicativo privado do re:POST de acordo com a marca organizacional e as necessidades de conhecimento. Os membros da equipe da AWS conta, como gerentes técnicos de contas, que estão familiarizados com a arquitetura e as cargas de trabalho da organização, são automaticamente adicionados ao re:post privado da organização para colaboração.

Os administradores do aplicativo re:Post Private podem personalizar a marca, adicionar tags para classificar o conteúdo e selecionar tópicos de interesse para que seus desenvolvedores preencham automaticamente o conteúdo técnico e de treinamento. Eles também podem convidar usuários a participarem de seu re:post privado para aumentar a colaboração. Para obter mais informações, consulte o AWS re:Post Private Administration Guide.

Usuários não administrativos usam o aplicativo re:POST Private para entrar usando credenciais configuradas pelo administrador. Depois de fazer login em um re:POST privado, os usuários podem

navegar ou pesquisar conteúdo existente, incluindo treinamento personalizado e conteúdo técnico que tenha como escopo seus tópicos de interesse. Os usuários também podem pesquisar conteúdo técnico AWS público diretamente de seu re:post privado e criar tópicos privados para discussões internas sobre conteúdo AWS público. Os usuários podem resolver problemas AWS técnicos de forma colaborativa e obter orientação técnica de outros usuários do re:post privado fazendo uma pergunta, fornecendo uma resposta ou publicando um artigo. Os usuários também podem converter um tópico de discussão em um AWS Support caso. Os usuários podem optar por adicionar as respostas do AWS Support re:post privado. Para obter mais informações, consulte o Guia do usuário privado do AWS re:Post.

Definição de preço

Somente clientes com os planos Enterprise Support (ES) e Enterprise On-Ramp (EOP) podem assinar o serviço re:POST Private. Você pode escolher entre os dois níveis de preços disponíveis: nível gratuito e nível padrão. O nível gratuito permite que você explore e experimente os recursos do nível Standard em toda a extensão por seis meses antes de fazer a transição perfeita para um nível pago. Se você usar o nível Standard, poderá pagar uma taxa de assinatura mensal por usuário para usar o re:Post Private. Para obter mais informações, consulte Preços do .

Como começar a usar

Para começar a usar o re:Post Private, consulte. Pré-requisitos

Pré-requisitos

Você deve atender aos seguintes pré-requisitos antes de criar um novo re:POST privado ou gerenciar um re:POST privado existente no AWS re:Post Private:

- Você deve se inscrever em um plano Enterprise ou Enterprise On-Ramp Support Plan.
- Você deve habilitar AWS IAM Identity Center na mesma região em que deseja configurar seu re:post privado.
- Você deve criar uma AWS Identity and Access Management função que tenha as permissões necessárias para criar, gerenciar e resolver AWS Support casos para você. O serviço re:Post Private usa essa função para fazer chamadas de API para. AWS Support Para obter mais informações, consulte Gerenciando o acesso à criação e gerenciamento de AWS Support casos no re:Post Private.

Integre-se ao re:Post Private por meio do IAM Identity Center

O re:POST Private se integra AWS IAM Identity Center para fornecer federação de identidade para sua força de trabalho. Por meio do IAM Identity Center, os usuários são redirecionados para o diretório atual da empresa para fazer login com suas credenciais existentes. Em seguida, eles se conectam perfeitamente ao seu re:post privado. Isso garante que as configurações de segurança, como políticas de senha e autenticação de dois fatores, sejam aplicadas. Usar o IAM Identity Center não afeta sua configuração atual do IAM.

Se você não tem um diretório de usuários existente ou prefere não federar, o IAM Identity Center oferece um diretório de usuários integrado que você pode usar para criar usuários e grupos para o re:Post Private. O re:Post Private não suporta o uso de usuários e funções do IAM para atribuir permissões em um re:POST privado. As permissões de usuário em um re:POST privado são configuradas por um administrador em seu aplicativo re:POST privado.

Para obter mais informações sobre o IAM Identity Center, consulte O que é o AWS IAM Identity Center (sucessor do AWS Single Sign-On). Para obter mais informações sobre como começar a usar o IAM Identity Center, consulte Introdução. Para usar o IAM Identity Center, você também deve ter AWS Organizations ativado a conta.

> **Important**
>
> O re:Post Private é compatível somente com instâncias organizacionais do IAM Identity Center.

Segurança em re:Post Private

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao AWS re:Post Private, consulte AWS Services in Scope by Compliance Program AWS Program.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o re:Post Private. Os tópicos a seguir mostram como configurar o re:Post Private para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do re:POST Private.

Tópicos

- Proteção de dados no AWS re:Post Private
- Como o re:Post Private funciona com o IAM
- Validação de conformidade para AWS re:Post Private
- Resiliência na AWS re:Post Private
- Segurança da infraestrutura na AWS re:Post Private

Proteção de dados no AWS re:Post Private

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no AWS re:Post Private. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global

que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o re:Post Private ou outro Serviços da AWS usando o console, a API ou AWS os AWS CLI SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Proteger dados com criptografia

Criptografia em repouso

O re:post Private usa buckets do Amazon Simple Storage Service, bancos de dados Amazon DynamoDB, bancos de dados Amazon Neptune OpenSearch e domínios do Amazon Service que são criptografados em repouso usando chaves gerenciadas pela Amazon ou chaves gerenciadas pelo cliente.

Criptografia em trânsito

O re:post Private usa o protocolo HTTPS para se comunicar com seu aplicativo cliente. Ele usa HTTPS e AWS assinaturas para se comunicar com outros serviços em nome do seu aplicativo.

Gerenciamento de chaves

O re:post Private é integrado AWS Key Management Service e suporta AWS KMS chaves. Você pode personalizar as configurações de criptografia de dados para seu re:post privado ao criá-lo. Para fazer isso, você pode escolher uma AWS KMS chave existente ou criar uma nova AWS KMS chave.

Como o re:Post Private funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao AWS re:Post Private, você deve entender quais recursos do IAM estão disponíveis para uso com o re:Post Private. Para ter uma visão de alto nível de como o re:Post Private e outros AWS serviços funcionam com o IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Re:post Políticas baseadas em identidade privada

Com as políticas baseadas em identidade do IAM, você pode especificar ações permitidas ou negadas. O re:Post Private suporta ações específicas. Para saber mais sobre os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Manual do usuário do IAM.

Ações

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações de política em re:Post Private usam o seguinte prefixo antes da ação:. `repostspace:` Por exemplo, para conceder permissão a alguém para executar a operação da `CreateSpace` API re:post Private, você inclui a `repostspace:CreateSpace` ação na política dessa pessoa. As declarações de política devem incluir um `NotAction` elemento `Action` ou. O re:Post Private define seu próprio conjunto de ações que descrevem as tarefas que você pode executar com esse serviço.

Para especificar várias ações em uma única instrução, separe-as com vírgulas, como segue:

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

Você também pode especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a seguinte ação:

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

Para ver uma lista de ações privadas do re:Post, consulte Ações definidas por re:Post Private no Guia do usuário do IAM.

Recursos

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu nome do recurso da Amazon (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Chaves de condição

O re:post Private não fornece nenhuma chave de condição específica do serviço, mas suporta o uso de chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia do usuário do IAM.

Exemplos

Para ver exemplos de políticas baseadas em identidade privada do re:POST, consulte. AWS re:Post Exemplos de políticas baseadas em identidade privada

Re:post Políticas baseadas em recursos privados

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou AWS serviços. Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

O re:post Private não oferece suporte a políticas baseadas em recursos.

Autorização baseada em tags do

O re:Post Private suporta a marcação de recursos ou o controle de acesso com base em tags. Para obter mais informações, consulte Controle do acesso aos recursos da AWS usando tags.

re:postar funções privadas do IAM

Uma função do IAM é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usando credenciais temporárias com re:Post Private

Recomendados fortemente usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como AssumeRoleou GetFederationToken.

O re:POST Private suporta o uso de credenciais temporárias.

Funções vinculadas a serviço

As funções vinculadas ao serviço permitem que AWS os serviços acessem recursos em outros serviços para concluir uma ação para você. Os perfis vinculados a serviço aparecem em sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados a serviço.

Perfis de serviço

Esse recurso permite que um serviço assuma uma função de serviço para você. Essa função permite que o serviço acesse recursos em outros serviços para concluir uma ação para você. Para obter mais informações, consulte Criação de uma função para delegar permissões a um serviço da AWS. Os perfis de serviço aparecem em sua conta do IAM e são de propriedade da conta. Isso significa que um administrador do IAM pode alterar as permissões para esse perfil. Porém, fazer isso pode alterar a funcionalidade do serviço.

Usando funções vinculadas ao serviço para re:Post Private

O AWS re:Post Private usa funções vinculadas a serviços AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao re:Post Private. As funções vinculadas ao serviço são predefinidas pelo re:Post Private e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração do re:Post Private porque você não precisa adicionar manualmente as permissões necessárias. O re:Post Private define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, somente o re:Post Private pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros produtos que oferecem suporte às funções vinculadas a serviços, consulte AWS services that work with IAM (Produtos da compatíveis com o IAM) e procure

os serviços que apresentam Yes (Sim) na coluna Service-linked roles (Funções vinculadas a serviços). Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculadas ao serviço para re:Post Private

re:Post Private usa a função vinculada ao serviço chamada AWSServiceRoleForrePostPrivate. re:Post Private usa essa função vinculada ao serviço para publicar dados em. CloudWatch

A função AWSServiceRoleForrePostPrivate vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `repostspace.amazonaws.com`

A política de permissões de função nomeada `AWSrePostPrivateCloudWatchAccess` permite que o re:Post Private conclua as seguintes ações nos recursos especificados:

- Ação sobre`cloudwatch`: `PutMetricData`

Você deve configurar permissões para permitir que seus usuários, grupos ou perfis criem, editem ou excluam um perfil vinculado ao serviço. Para ter mais informações, consulte Service-linked role permissions (Permissões de nível vinculado a serviços) no Guia do usuário do IAM.

Para ter mais informações, consulte AWSrePostPrivateCloudWatchAccess.

Criação de uma função vinculada ao serviço para re:Post Private

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você cria seu primeiro re:Post privado na, na ou na AWS API AWS Management Console AWS CLI, o re:Post Private cria a função vinculada ao serviço para você.

> **Important**
>
> Essa função vinculada ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com essa função. Além disso, se você estava usando o serviço re:Post Private antes de 1º de dezembro de 2023, quando ele começou a oferecer suporte a funções vinculadas ao serviço, o re:Post Private criou a função em sua conta. `AWSServiceRoleForrePostPrivate` Para saber mais, consulte Uma nova função apareceu no meu Conta da AWS.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você poderá usar esse mesmo processo para recriar a função em sua conta. Quando você cria seu primeiro re:POST privado, o re:post Private cria a função vinculada ao serviço para você novamente.

Na AWS CLI ou na AWS API, crie uma função vinculada ao serviço com o nome do `repostspace.amazonaws.com` serviço. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Manual do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Editando uma função vinculada ao serviço para re:Post Private

O re:post Private não permite que você edite a função vinculada ao `AWSServiceRoleForrePostPrivate` serviço. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você poderá editar a descrição do perfil usando o IAM. Para ter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para re:Post Private

Você não precisa excluir manualmente a função `AWSServiceRoleForrePostPrivate`. Quando você exclui seu re:Post privado na, na ou na AWS API AWS Management Console AWS CLI, o re:Post Private exclui a função vinculada ao serviço para você.

Você também pode usar o console do IAM AWS CLI, o ou a AWS API para excluir manualmente a função vinculada ao serviço.

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleForrePostPrivate vinculada ao serviço. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões suportadas para funções vinculadas ao serviço re:Post Private

O re:Post Private oferece suporte ao uso de funções vinculadas ao serviço AWS nas regiões em que o serviço está disponível.

Nome da região	Identidade da região	Support em re:Post Private
Leste dos EUA (Norte da Virgínia)	us-east-1	Sim
Leste dos EUA (Ohio)	us-east-2	Não
Oeste dos EUA (N. da Califórnia)	us-west-1	Não
Oeste dos EUA (Oregon)	us-west-2	Sim
África (Cidade do Cabo)	af-south-1	Não
Ásia-Pacífico (Hong Kong)	ap-east-1	Não
Ásia-Pacífico (Jacarta)	ap-southeast-3	Não
Ásia-Pacífico (Mumbai)	ap-south-1	Não
Ásia-Pacífico (Osaka)	ap-northeast-3	Não
Ásia-Pacífico (Seul)	ap-northeast-2	Não
Ásia-Pacífico (Singapura)	ap-southeast-1	Sim
Ásia-Pacífico (Sydney)	ap-southeast-2	Sim
Ásia-Pacífico (Tóquio)	ap-northeast-1	Não
Canadá (Central)	ca-central-1	Sim
Europa (Frankfurt)	eu-central-1	Sim
Europa (Irlanda)	eu-west-1	Sim
Europa (Londres)	eu-west-2	Não
Europa (Milão)	eu-south-1	Não
Europa (Paris)	eu-west-3	Não
Europa (Estocolmo)	eu-north-1	Não

Nome da região	Identidade da região	Support em re:Post Private
Oriente Médio (Barém)	me-south-1	Não
Oriente Médio (Emirados Árabes Unidos)	me-central-1	Não
América do Sul (São Paulo)	sa-east-1	Não

AWS re:Post Exemplos de políticas baseadas em identidade privada

> **Note**
>
> Para maior segurança, crie usuários federados em vez de usuários do IAM sempre que possível.

Por padrão, AWS Identity and Access Management usuários e funções não têm permissão para criar ou modificar recursos privados do AWS re:Post. Eles também não podem realizar tarefas usando a AWS API AWS Management Console AWS CLI, ou. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte Criar políticas do IAM no Guia do usuário do IAM.

Tópicos

- Melhores práticas de política
- Permitir que usuários visualizem suas próprias permissões

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos privados do re:POST em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e passe para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do Usuário do IAM.
- Aplique permissões de privilégio mínimo –- ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do Usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso –- você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica Serviço da AWS, como AWS CloudFormation. Para obter mais informações, consulte Elementos da política JSON do IAM: Condição no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais –- o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas Recomendadas de Segurança no IAM no Guia do Usuário do IAM.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Políticas em linha

Políticas em linha são políticas que você cria e gerencia. Você pode incorporar políticas em linha diretamente em um usuário, grupo ou função. Os exemplos de políticas a seguir mostram como atribuir permissões para realizar ações privadas do AWS re:POST. Para obter informações gerais sobre políticas em linha, consulte Gerenciamento de políticas do IAM no Guia do usuário do AWS IAM. Você pode usar o AWS Management Console, AWS Command Line Interface (AWS CLI) ou a AWS Identity and Access Management API para criar e incorporar políticas em linha.

Tópicos

- Acesso somente para leitura ao re:Post Private
- Acesso total ao re:Post Private

Acesso somente para leitura ao re:Post Private

A política a seguir concede acesso de leitura a um usuário para o IAM Identity Center e o console privado re:Post. Essa política permite que o usuário execute ações privadas do re:POST que são somente para leitura.

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

Acesso total ao re:Post Private

A política a seguir concede acesso total a um usuário para o IAM Identity Center e o console privado re:POST. Essa política permite que o usuário execute todas as ações privadas do re:POST.

```
{
    "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 políticas gerenciadas para AWS re:Post Private

O uso de políticas AWS gerenciadas facilita a adição de permissões a usuários, grupos e funções do que a criação de políticas por conta própria. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam. Use políticas AWS gerenciadas para começar rapidamente. Essas políticas abrangem casos de uso comuns e estão disponíveis em sua AWS conta. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Ocasionalmente, os serviços podem adicionar permissões adicionais a uma política AWS gerenciada para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política AWS gerenciada quando um novo recurso é lançado ou quando novas operações são disponibilizadas. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violam suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política `ReadOnlyAccess` AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter mais informações, consulte Políticas gerenciadas pela AWS no Guia do usuário do IAM.

Tópicos

- AWS política gerenciada: AWSRepostSpaceSupportOperationsPolicy

- AWS política gerenciada: AWSrePostPrivateCloudWatchAccess
- AWS re:Post Atualizações privadas de políticas gerenciadas AWS

AWS política gerenciada: AWSRepostSpaceSupportOperationsPolicy

Essa política permite que o serviço AWS re:Post Private crie, gerencie e resolva AWS Support casos criados por meio do aplicativo web re:Post Private.

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

AWS política gerenciada: AWSrePostPrivateCloudWatchAccess

Essa política permite que o serviço re:POST Private publique dados em. 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 Atualizações privadas de políticas gerenciadas AWS

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do re:Post Private desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página Histórico do documento.

A tabela a seguir descreve atualizações importantes nas políticas gerenciadas do re:POST Private desde 26 de novembro de 2023.

Alteração	Descrição	Data
Nova política - AWSrePost PrivateCloudWatchAccess	Nova política gerenciada para publicação de dados em CloudWatch	26 de novembro de 2023
Nova política - AWSRepost SpaceSupportOperationsPolicy	Nova política gerenciada para o recurso AWS Support no AWS re:Post Private	26 de novembro de 2023
re:POST Private iniciou o rastreamento de alterações	O re:POST Private começou a monitorar as mudanças em suas AWS políticas gerenciadas	26 de novembro de 2023

Solução de problemas de identidade e acesso privados do AWS re:Post

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o re:Post Private e o IAM.

Tópicos

- Não estou autorizado a realizar uma ação no re:Post Private
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos privados do re:POST

Não estou autorizado a realizar uma ação no re:Post Private

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `repostPrivate:`*`GetWidget`* fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `repostPrivate:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para re:Post Private.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no re:Post Private. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos privados do re:POST

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o re:Post Private suporta esses recursos, consulte. Como o re:Post Private funciona com o IAM
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

Validação de conformidade para AWS re:Post Private

Para saber se um Serviço da AWS está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

  > **Note**
  >
  > Nem todos Serviços da AWS são elegíveis para a HIPAA. Para mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.

- AWS Security Hub— Isso Serviço da AWS fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso Serviço da AWS detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso Serviço da AWS ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência na AWS re:Post Private

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Segurança da infraestrutura na AWS re:Post Private

Como um serviço gerenciado, o AWS re:Post Private é protegido pelos procedimentos AWS globais de segurança de rede descritos no whitepaper Amazon Web Services: Overview of Security Processes.

Você usa chamadas de API AWS publicadas para acessar o re:Post Private pela rede. Os clientes devem oferecer compatibilidade com Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos usar o TLS 1.2 ou posterior. Os clientes também devem ter suporte a conjuntos de

criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um AWS Identity and Access Management principal. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Re:post Cotas privadas

O AWS re:Post Private fornece re:posts privados que você pode usar em sua conta em uma determinada região. AWS Quando você se inscreve no re:Post Private, AWS define cotas padrão (anteriormente chamadas de limites) no número de re:posts privados que você pode criar e no tamanho dos re:posts privados.

Service Quotas

A seguir estão as cotas padrão do re:Post Private para sua conta. AWS Você pode usar o console Service Quotas para ver a cota padrão. Nenhuma dessas cotas é ajustável. Você não pode solicitar um aumento de cota.

Recurso	Padrão	Descrição	Ajustável
Número de re:posts privados	3	O número máximo de re:posts privados nesta conta na região atual.	Não
Tamanho privado gratuito do Re:post	10	O tamanho máximo (em GB) de um re:POST privado gratuito.	Não
Tamanho padrão do Re:post privado	100	O tamanho máximo (em GB) de um re:POST privado padrão.	Não

Limites de limitação da API

Os seguintes limites de limitação se aplicam por conta, por região no re:Post Private. Essas cotas não podem ser aumentadas.

Ações	Taxa de recarga de tokens	Taxa de solicitações	
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	

Crie, configure e personalize seu re:post privado

Tópicos

- Crie um novo re:post privado
- Gerenciando o acesso à criação e gerenciamento de AWS Support casos no re:Post Private
- Configurar e gerenciar o acesso do usuário usando AWS IAM Identity Center
- Personalize seu re:post privado
- Convide usuários para seu re:post privado

Crie um novo re:post privado

Para criar um novo re:post privado, siga estas etapas:

1. Abra o console privado do re:POST em https://console.aws.amazon.com/repost-private/.
2. Na página inicial do console, escolha Criar re:post privado.
3. Se você ainda não tem o IAM Identity Center configurado para sua conta, escolha Open Identity Center. Siga as instruções em Conceitos básicos no Guia do usuário do AWS IAM Identity Center.
4. Na página Criar re:post privado, em Preços, selecione Nível gratuito ou nível padrão com base no seu caso de uso. Se você já usou o nível gratuito em sua conta, a opção de nível gratuito não está disponível para você.
5. Em Detalhes, faça o seguinte:

   Em Nome, insira um nome exclusivo para seu re:post privado.

   (Opcional) Em Descrição, insira uma breve descrição para seu re:post privado.

   Em Subdomínio personalizado, insira um nome personalizado para seu subdomínio.
6. (Opcional) Para personalizar suas configurações de criptografia de dados, em Criptografia de dados, selecione Personalizar configurações de criptografia. Em seguida, execute uma das seguintes ações:

   Em Escolha uma chave do AWS KMS, selecione uma AWS Key Management Service chave ou um nome de recurso da Amazon (ARN).

   - ou -

Escolha Criar uma chave do AWS KMS. Em seguida, crie a AWS KMS chave.

7. (Opcional) Em Acesso ao serviço para integração de casos de suporte, selecione Habilitar acesso ao serviço para este re:POST.

> **Note**
>
> Você também pode ativar essa opção depois de criar o re:POST privado.

Em Selecione uma função do IAM existente abaixo ou crie uma nova função no console do IAM, use a barra de pesquisa para encontrar sua função do IAM existente.

- ou -

Escolha criar uma nova função no console do IAM.

Se você optar por criar uma nova função, siga as instruções emCriar um perfil do IAM.

Se você optar por usar uma função de serviço existente, na barra de pesquisa, insira o ARN da função que você deseja usar. Escolha a função na lista suspensa.

Para ter mais informações, consulte Gerenciando o acesso à criação e gerenciamento de AWS Support casos no re:Post Private.

8. (Opcional) Em Tags, escolha Adicionar nova tag. Em seguida, insira as seguintes informações:

Em Chave, insira sua chave de tag personalizada.

Em Valor, insira o valor da etiqueta personalizada.

Para adicionar mais tags, escolha Adicionar nova tag.

9. Escolha Criar este re:POST.

Uma página de confirmação informará que seu re:post privado está sendo criado. Você pode ver o status do re:post privado no campo Status. Quando seu re:post privado é criado, o campo Status exibe Criando.

Demora aproximadamente 30 minutos para que o re:post privado seja criado. Quando seu re:post privado estiver pronto, o campo Status será exibido Online. Você pode usar o subdomínio gerado

pela AWS para seu re:POST privado, que está listado na guia Configurações, para acessar seu re:POST privado. Você pode ver o subdomínio personalizado do seu re:post privado na guia Configurações após a conclusão da revisão.

Gerenciando o acesso à criação e gerenciamento de AWS Support casos no re:Post Private

Você deve criar uma função AWS Identity and Access Management (IAM) para gerenciar o acesso à criação e ao gerenciamento de AWS Support casos a partir do AWS re:Post Private. Essa função executa as seguintes AWS Support ações para você:

- CreateCase
- AddCommunicationToCase
- ResolveCase

Depois de criar a função do IAM, anexe uma política do IAM a essa função para que a função tenha as permissões necessárias para concluir essas ações. Você escolhe essa função ao criar seu re:POST privado no console privado do re:POST.

Os usuários em seu re:post privado têm as mesmas permissões que você concede à função do IAM.

> **Important**
>
> Se você alterar a função do IAM ou a política do IAM, suas alterações se aplicarão ao re:post privado que você configurou.

Siga esses procedimentos para criar seu perfil e sua política do IAM.

Tópicos

- Use uma política AWS gerenciada ou crie uma política gerenciada pelo cliente
- Exemplo de política do IAM
- Criar um perfil do IAM
- Solução de problemas

Use uma política AWS gerenciada ou crie uma política gerenciada pelo cliente

Para conceder permissões à sua função, você pode usar uma política AWS gerenciada ou uma política gerenciada pelo cliente.

> **Tip**
>
> Se você não quiser criar uma política manualmente, recomendamos que você use uma política AWS gerenciada em vez disso e ignore esse procedimento. As políticas gerenciadas têm automaticamente as permissões necessárias para AWS Support. Não é necessário atualizar as políticas manualmente. Para obter mais informações, consulte AWS política gerenciada: AWSRepostSpaceSupportOperationsPolicy.

Siga esse procedimento para criar uma política gerenciada pelo cliente para seu perfil. Esse procedimento usa o editor de política do JSON no console do IAM.

Para criar uma política gerenciada pelo cliente para o re:Post Private

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
3. Escolha Criar política.
4. Escolha a guia JSON.
5. Insira seu JSON e, em seguida, substitua o JSON padrão no editor. Você pode usar o example policy (exemplo de política).
6. Escolha Próximo: tags.
7. (Opcional) É possível usar tags como pares de chave-valor para adicionar metadados à política.
8. Escolha Próximo: revisar.
9. Na página Review policy (Revisar política), insira um Name (Nome), como *`rePostPrivateSupportPolicy`*, e uma Description (Descrição) (opcional).
10. Examine a página Resumo para ver as permissões que a política permite e, em seguida, escolha Criar política.

Essa política define as ações que o perfil pode realizar. Para obter mais informações, consulte a seção Creating IAM policies (console) [Como criar políticas do IAM (console)] no Guia do usuário do IAM.

Exemplo de política do IAM

Você pode anexar o exemplo de política a seguir ao seu perfil do IAM. Essa política permite que a função tenha permissões completas para todas as ações necessárias para AWS Support. Depois de configurar um re:post privado com a função, qualquer usuário em seu re:post privado tem as mesmas permissões.

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

> **Note**
>
> Para obter uma lista de políticas AWS gerenciadas para re:Post Private, consulte. AWS políticas gerenciadas para AWS re:Post Private

Você pode atualizar a política para remover uma permissão do AWS Support.

Para obter as descrições de cada ação, consulte os seguintes tópicos em Service Authorization Reference (Referência de autorização do serviço):

- Ações, recursos e chaves de condição para o AWS Support
- Actions, resources, and condition keys for Service Quotas (Ações, recursos e chaves de condição para o Service Quotas)
- Ações, recursos e chaves de condição para AWS Identity and Access Management

Criar um perfil do IAM

Após criar a política, crie um perfil do IAM e anexe a política a esse perfil. Você escolhe essa função ao criar um re:POST privado no console privado do re:POST.

Para criar uma função para criação e gerenciamento de AWS Support casos

1. Faça login AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Roles (Funções) e Criar função.
3. Em Trusted entity type (Tipo de entidade confiável), escolha Custom trust policy (Política de confiança personalizada).
4. Em Política de confiança personalizada, insira o seguinte:

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

5. Escolha Próximo.
6. Em Políticas de permissões, na barra de pesquisa, insira a política AWS gerenciada ou uma política gerenciada pelo cliente que você criou, como *rePostPrivateSupportPolicy*.

Marque a caixa de seleção ao lado das políticas de permissões que você deseja que o serviço tenha.

7. Escolha Próximo.
8. Na página Nome, revisão e criação, em Nome da função, insira um nome, como *rePostPrivateSupportRole*.
9. (Opcional) Em Descrição, insira uma descrição para o perfil.
10. Revise a política de confiança e as permissões.
11. (Opcional) Para adicionar metadados ao perfil, use tags como pares de chave-valor. Para obter mais informações sobre como usar rótulos no IAM, consulte Recursos de etiquetas do IAM.
12. Selecione Criar função. Agora você pode escolher essa função ao configurar um re:POST privado no console privado do re:POST. Consulte Crie um novo re:post privado.

Para obter mais informações, consulte Criação de uma função para um AWS serviço (console) no Guia do usuário do IAM.

Solução de problemas

Consulte os tópicos a seguir para gerenciar o acesso ao re:POST Private.

Sumário

- Quero restringir usuários específicos em meu re:post privado de ações específicas
- Quando eu configuro um re:Post privado, não vejo a função do IAM que criei
- Falta uma permissão para o meu perfil do IAM
- Um erro diz que minha função do IAM não é válida

Quero restringir usuários específicos em meu re:post privado de ações específicas

Por padrão, os usuários em seu re:post privado têm as mesmas permissões especificadas na política do IAM que você anexa à função do IAM que você cria. Isso significa que qualquer pessoa no re:post privado tem acesso de leitura ou gravação para criar e gerenciar AWS Support casos, independentemente de ter ou não um usuário Conta da AWS do IAM.

Recomendamos seguir estas práticas recomendadas:

- Use uma política do IAM que tenha as permissões mínimas necessárias para AWS Support o. Consulte AWS política gerenciada: AWSRepostSpaceSupportOperationsPolicy.

Quando eu configuro um re:Post privado, não vejo a função do IAM que criei

Se sua função do IAM não aparecer na lista de funções do IAM para re:post Private;, isso significa que a função não tem re:post Private como entidade confiável ou que a função foi excluída. É possível atualizar um perfil existente ou criar um. Consulte Criar um perfil do IAM.

Falta uma permissão para o meu perfil do IAM

A função do IAM que você cria para seu re:post privado precisa de permissões para realizar as ações que você deseja. Por exemplo, se você quiser que seus usuários no re:POST privado criem casos de suporte, a função deve ter a `support:CreateCase` permissão. re:Post Private assume essa função para realizar essas ações para você.

Se você receber um erro sobre a falta de uma permissão para AWS Support, verifique se a política anexada à sua função tem a permissão necessária.

Veja o Exemplo de política do IAM anterior.

Um erro diz que minha função do IAM não é válida

Verifique se você escolheu a função correta para sua configuração privada do re:POST.

Configurar e gerenciar o acesso do usuário usando AWS IAM Identity Center

O re:POST Private se integra AWS IAM Identity Center para fornecer federação de identidade para a força de trabalho da sua organização. Use o IAM Identity Center para criar ou conectar usuários da sua organização e gerenciar centralmente o acesso deles em todas as AWS contas e aplicativos. Para obter mais informações sobre o IAM Identity Center, consulte O que é o AWS IAM Identity Center (sucessor do AWS Single Sign-On). Para obter mais informações sobre como começar a usar o IAM Identity Center, consulte Introdução. Para usar o IAM Identity Center, você também deve ter AWS Organizations ativado a conta.

Personalize seu re:post privado

Você pode adicionar um ou mais administradores ao seu re:post privado depois de criá-lo. Os administradores usam o aplicativo re:POST Private para iniciar o re:POST privado e gerenciar os usuários dentro dele. Eles podem personalizar a marca do re:post privado, adicionar tags para

classificar o conteúdo e selecionar tópicos de interesse para preencher automaticamente o conteúdo. Para obter mais informações, consulte o AWS re:Post Private Administration Guide.

Convide usuários para seu re:post privado

Você pode adicionar um ou mais usuários ao seu re:post privado depois de criá-lo. Você pode convidar usuários para colaborar em seu re:post privado. Os usuários usam o aplicativo re:POST Private para entrar usando as credenciais que você configurou. Depois de fazer login em um re:POST privado, os usuários podem navegar ou pesquisar conteúdo existente, incluindo treinamento personalizado e conteúdo técnico que tenha como escopo seus tópicos de interesse. Para obter mais informações, consulte o Guia do usuário privado do AWS re:Post.

Gerencie seu re:POST privado no console privado do re:POST

Esta seção explica como você pode gerenciar seu re:POST privado no console privado do AWS re:POST.

Tópicos

- Adicione usuários e grupos ao seu re:post privado
- Adicione usuários a um grupo em seu re:post privado
- Convide usuários e grupos para seu re:post privado
- Promova um usuário em seu re:post privado para administrador
- Remova usuários ou grupos do seu re:post privado
- Adicione ou remova um AWS funcionário do seu re:post privado
- Excluir um re:Post privado de re:Post Private

Adicione usuários e grupos ao seu re:post privado

Se você for administrador, poderá adicionar usuários e grupos ao seu re:post privado.

Adicione usuários ao seu re:post privado

1. Abra o console privado do re:POST em https://console.aws.amazon.com/repost-private/.
2. No painel de navegação, escolha Todos os meus re:posts privados.
3. Escolha o re:post privado que você deseja gerenciar.
4. Escolha a guia Users.
5. Em Usuários, escolha Adicionar usuários e grupos.
6. Na lista, selecione os usuários que você deseja adicionar ao seu re:post privado. Em seguida, escolha Atribuir.

Os usuários selecionados são adicionados ao seu re:post privado e listados na guia Usuários.

Adicione grupos ao seu re:post privado

1. Abra o console privado do re:POST em https://console.aws.amazon.com/repost-private/.
2. No painel de navegação, escolha Todos os meus re:posts privados.
3. Escolha o re:post privado que você deseja gerenciar.
4. Escolha a guia Groups (Grupos).
5. Escolha Adicionar usuários e grupos.
6. Na lista, selecione os grupos que você deseja adicionar ao seu re:post privado. Em seguida, escolha Atribuir.

Os grupos selecionados são adicionados ao seu re:post privado e listados na guia Grupos.

Adicione usuários a um grupo em seu re:post privado

Use o IAM Identity Center para adicionar novos usuários a um grupo existente em seu re:post privado. Para obter mais informações, consulte Adicionar usuários a grupos no Guia do usuário do AWS IAM Identity Center.

Convide usuários e grupos para seu re:post privado

Siga estas etapas para convidar usuários e grupos para seu re:post privado no AWS re:Post Private:

1. Abra o console privado do re:POST em https://console.aws.amazon.com/repost-private/.
2. No painel de navegação, escolha Todos os meus re:posts privados.
3. Escolha o re:post privado que você deseja gerenciar.
4. Para convidar usuários para seu re:post privado, escolha a guia Usuários.

   Na lista, selecione os usuários que você deseja convidar para o seu re:post privado. Em seguida, escolha Integrar usuários para re:POST.
5. Na caixa de diálogo Integrar usuários a essa caixa de diálogo privada do re:POST, insira as seguintes informações:

   Em Assunto, insira o assunto da mensagem de e-mail que você está enviando.

   Em Body, insira uma mensagem de boas-vindas para seu re:post privado.

   Escolha Enviar e-mail de integração.

6. Para convidar grupos para seu re:post privado, escolha a guia Grupos.

   Na lista, selecione os grupos que você deseja convidar para o seu re:post privado. Em seguida, escolha Integrar grupos para re:POST.
7. Na caixa de diálogo Integrar grupos a essa caixa de diálogo privada re:POST, insira as seguintes informações:

   Em Assunto, insira o assunto da mensagem de e-mail que você está enviando.

   Em Body, insira uma mensagem de boas-vindas para seu re:post privado.

   Escolha Enviar e-mail de integração.

A mensagem de boas-vindas é enviada a todos os usuários e grupos selecionados com informações sobre como fazer login no seu re:POST privado.

Promova um usuário em seu re:post privado para administrador

Para promover um usuário privado do re:POST a administrador, siga estas etapas:

1. Abra o console privado do re:POST em https://console.aws.amazon.com/repost-private/.
2. No painel de navegação, escolha Todos os meus re:posts privados.
3. Escolha o re:post privado que você deseja gerenciar.
4. Escolha a guia Users.
5. Selecione um ou mais usuários que você deseja promover a administrador.
6. Escolha Editar função e, em seguida, escolha Tornar administrador.

Os usuários selecionados são promovidos a administradores. Na guia Usuários, a função desses usuários é atualizada para Administrador.

Remova usuários ou grupos do seu re:post privado

Se você for administrador, poderá remover usuários ou grupos do seu re:post privado.

Remover usuários do seu re:post privado

1. Abra o console privado do re:POST em https://console.aws.amazon.com/repost-private/.

2. No painel de navegação, escolha Todos os meus re:posts privados.
3. Escolha o re:post privado que você deseja gerenciar.
4. Em Usuários, na lista, selecione os usuários que você deseja remover do seu re:post privado. Em seguida, escolha Remover.

Os usuários selecionados são removidos do seu re:post privado. As informações sobre os usuários removidos não aparecem mais na guia Usuários.

Remova grupos do seu re:post privado

1. Abra o console privado do re:POST em https://console.aws.amazon.com/repost-private/.
2. No painel de navegação, escolha Todos os meus re:posts privados.
3. Escolha o re:post privado que você deseja gerenciar.
4. Escolha a guia Groups (Grupos).
5. Na lista, selecione os grupos que você deseja remover do seu re:post privado. Em seguida, escolha Remover.

Os grupos selecionados são removidos do seu re:post privado. As informações sobre os grupos removidos não aparecem mais na guia Grupos.

Adicione ou remova um AWS funcionário do seu re:post privado

Se você tiver um plano Enterprise ou Enterprise On-Ramp Support, poderá adicionar ou remover um funcionário da AWS do seu re:POST privado. Entre em contato com o Concierge Support ou com seu gerente técnico de contas (TAM) para obter mais informações.

Excluir um re:Post privado de re:Post Private

Para excluir um re:Post privado no AWS re:Post Private, siga estas etapas:

1. Abra o console privado do re:POST em https://console.aws.amazon.com/repost-private/.
2. No painel de navegação, escolha Todos os meus re:posts privados.
3. Escolha o re:post privado que você deseja gerenciar e, em seguida, escolha Excluir.
4. Selecione todas as opções para reconhecer e confirmar que você deseja excluir permanentemente o re:post privado e os dados associados a ele.

> **Important**
>
> Quando você exclui o re:POST privado, todas as informações de configuração relacionadas ao re:POST privado serão excluídas. Depois que o re:post privado for excluído, você não poderá restaurar nenhum conteúdo dele.

5. Insira o nome do seu re:post privado quando solicitado um consentimento adicional por escrito. Em seguida, selecione Excluir.

Leva aproximadamente 30 minutos para que seu re:post privado seja excluído.

Monitoramento do AWS re:Post Private

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do AWS re:Post Private e de suas outras AWS soluções. AWSfornece as seguintes ferramentas de monitoramento para assistir ao re:Post Private, relatar quando algo está errado e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.
- AWS CloudTrailcaptura chamadas de API e eventos relacionados feitos por ou para você Conta da AWS e entrega os arquivos de log em um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o Guia do usuário do AWS CloudTrail.

Monitorando o AWS re:Post Private com a Amazon CloudWatch

Você pode monitorar o AWS re:Post Private usando a Amazon CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. Essas estatísticas são mantidas por 15 meses para que você possa acessar informações históricas e ter uma melhor perspectiva sobre o desempenho de seu aplicativo ou serviço web. Também é possível definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o Guia CloudWatch do usuário da Amazon.

O serviço re:Post Private relata as seguintes métricas no namespace. `AWS/rePostPrivate`

Métrica	Descrição
`NumberOfSpaces`	O número de re:posts privados na conta atual. Unidades: contagem

Métrica	Descrição
`NumberOfUsers`	O número de usuários em um re:post privado. Essa métrica usa SpaceID como uma dimensão. Unidades: contagem
`ContentSize`	A quantidade de conteúdo em um re:post privado. Essa métrica usa SpaceID como uma dimensão. Unidade: bytes

As dimensões a seguir são compatíveis com as métricas do re:Post Private.

Dimensão	Descrição
`spaceId`	O identificador exclusivo para o re:POST privado.

Registro de chamadas de API privadas do AWS re:Post usando AWS CloudTrail

O AWS re:Post Private é integrado comAWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no re:Post Private. CloudTrail captura todas as chamadas de API para re:Post Private como eventos. As chamadas capturadas incluem chamadas do console privado do re:POST e chamadas de código para as operações da API privada do re:POST. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para re:Post Private. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita para re:Post Private, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

re:Publique informações privadas em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no re:Post Private, essa atividade é registrada em um CloudTrail evento junto com outros eventos de AWS serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Trabalhando com o histórico de CloudTrail eventos.

Para um registro contínuo de eventos em seuConta da AWS, incluindo eventos para re:Post Private, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte as informações a seguir.

- Criar uma trilha para a conta da AWS
- CloudTrail serviços e integrações suportados
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas as ações privadas do re:Post Private são registradas CloudTrail e documentadas na AWS re:Post Private API Reference. O re:Post Private suporta o registro das seguintes ações como eventos em arquivos de log: CloudTrail

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

- UntagResource
- UpdateSpace

O re:Post Private suporta o registro das seguintes AWS Support ações como eventos nos arquivos de CloudTrail log:

- CreateCase
- AddCommunicationToCase
- ResolveCase

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Compreendendo as entradas do arquivo de log privado do re:POST

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `CreateSpace` ação.

```
{
   "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"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `RegisterAdmin` ação.

```
{
   "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"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `ListSpaces` ação.

```
 {
    "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"
}
```

O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `ResolveCase` ação. Você pode usar o `sourceIdentity` elemento nessa entrada de registro para identificar o usuário que resolveu o caso.

```
 {
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAQM47QIR76DQZ7N5WX:create-support-case-
Uk1iHNTWQEOLmR2BR1FDJQ",
        "arn": "arn:aws:sts::123456789012:assumed-role/AWSRepostSpaceRole/create-
support-case-Uk1iHNTWQEOLmR2BR1FDJQ",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAQM47QIR76DQZ7N5WX",
                "arn": "arn:aws:iam::123456789012:role/AWSRepostSpaceRole",
                "accountId": "123456789012",
                "userName": "AWSRepostSpaceRole"
            },
            "attributes": {
                "creationDate": "2023-11-17T21:46:42Z",
                "mfaAuthenticated": "false"
            },
```

```
            "sourceIdentity": "28e17330-10f1-705d-7cba-3a62a6b10e2e"
        }
    },
    "eventTime": "2023-11-17T21:46:44Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "ResolveCase",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "54.68.27.29",
    "userAgent": "aws-sdk-nodejs/2.1363.0 linux/v16.20.2 exec-env/AWS_ECS_FARGATE
 promise",
    "requestParameters": {
        "caseId": "case-123456789012-muen-2023-75d2c35481b96357"
    },
    "responseElements": {
        "initialCaseStatus": "unassigned",
        "finalCaseStatus": "resolved"
    },
    "requestID": "594b91c6-df1c-47e4-a834-d67d67f34b9d",
    "eventID": "7fc9cbe4-c8d5-4d61-a016-e076de272fff",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111111111111",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "support.us-west-2.amazonaws.com"
    }
}
```

Solução de problemas do re:Post Private

As informações a seguir podem ajudá-lo a solucionar problemas com o AWS re:Post Private.

Tópicos

- Não consigo configurar meu re:post privado em uma região específica AWS
- Não consigo configurar o re:post privado na minha conta
- Não consigo gerenciar usuários ou grupos em um re:post privado

Não consigo configurar meu re:post privado em uma região específica AWS

O re:post Private está disponível somente nas regiões Leste dos EUA (Norte da Virgínia), Oeste dos EUA (Oregon), Europa (Frankfurt), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Sydney), Canadá (Central) e Europa (Irlanda). Certifique-se de criar seu re:post privado em uma dessas regiões.

Não consigo configurar o re:post privado na minha conta

Verifique se você AWS IAM Identity Center ativou sua conta e configurou o IAM Identity Center na mesma região em que deseja criar o re:POST privado. Para ter mais informações, consulte Pré-requisitos.

Não consigo gerenciar usuários ou grupos em um re:post privado

Certifique-se de ter as permissões necessárias para editar um re:POST privado e gerenciar usuários e grupos dentro do re:POST privado. Para ter mais informações, consulte AWS re:Post Exemplos de políticas baseadas em identidade privada.

Histórico do documento

A tabela a seguir descreve os lançamentos da documentação do AWS re:Post Private:

Alteração	Descrição	Data
Atualização	Foram adicionados o Leste dos EUA (Norte da Virgínia) , Ásia-Pacífico (Sydney), Canadá (Central) e Europa (Irlanda) às regiões suportadas	10 de maio de 2024
Atualização	Adição da Ásia-Pacífico (Cingapura) às regiões suportadas	6 de março de 2024
Novos recursos	Documentação adicionada para políticas gerenciadas da AWS para AWS re:Post Private	26 de novembro de 2023
Lançamento inicial	Versão inicial do Guia de administração do console privado re:POST	26 de novembro de 2023

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.