Guía de administración de consolas

AWS re:Post Private

AWS re:Post Private: Guía de administración de consolas

Table of Contents

¿Qué es AWS Re:post Private?

AWS Re:Post Private es una versión privada de AWS Re:post para empresas con planes Enterprise Support o Enterprise On-Ramp Support. Proporciona acceso a conocimientos y expertos para acelerar la adopción de la nube y aumentar la productividad de los desarrolladores. Con Re:post privado específico para su organización, puede crear una comunidad de desarrolladores específica para cada organización que impulse la eficiencia a gran escala y brinde acceso a valiosos recursos de conocimiento. Además, Re:post Private centraliza el contenido AWS técnico confiable y ofrece foros de debate privados para mejorar la forma en que sus equipos colaboran internamente y con AWS para eliminar los obstáculos técnicos, acelerar la innovación y escalar de manera más eficiente en la nube.

Para obtener más información, consulte AWS Re:Post Private.

Acceda a Re:post Private

Los administradores utilizan la consola AWS Re:post Private para crear su Re:post privado específico de la organización. Cuando los administradores crean un Re:post privado, pueden asignarle un nombre a su Re:post privado y definir un subdominio en él. `*.private.repost.aws` Los administradores del Re:post privado de una organización pueden configurar el acceso de los usuarios mediante AWS IAM Identity Center y especificar una de las siguientes fuentes de identidad para la autenticación: el directorio del Centro de Identidad, Active Directory o un proveedor de identidad externo. Tras configurar los usuarios, los administradores de la consola pueden asignar una función de administrador de Re:post Private a uno o más usuarios. Los administradores de re:post Private pueden personalizar su aplicación privada de Re:post en función de la marca de la organización y de las necesidades de conocimiento. Los miembros del equipo de AWS cuentas, como los directores técnicos de cuentas, que están familiarizados con la arquitectura y las cargas de trabajo de la organización, se añaden automáticamente al Re:post privado de la organización para facilitar su colaboración.

Los administradores de la aplicación Re:post Private pueden personalizar la marca, añadir etiquetas para clasificar el contenido y seleccionar temas de interés para que sus desarrolladores rellenen automáticamente el contenido técnico y de formación. También pueden invitar a los usuarios a unirse a su Re:post privado para aumentar la colaboración. Para obtener más información, consulte la Guía de administración privada de AWS Re:post.

Los usuarios no administrativos utilizan la aplicación Re:post Private para iniciar sesión con las credenciales configuradas por su administrador. Tras iniciar sesión en un Re:post privado, los usuarios pueden explorar o buscar el contenido existente, incluida la formación personalizada y el contenido técnico que se ajuste a sus temas de interés. Los usuarios también pueden buscar contenido técnico AWS público directamente desde su Re:post privado y crear hilos privados para debates internos sobre contenido público. AWS Los usuarios pueden resolver problemas AWS técnicos de forma colaborativa y obtener orientación técnica de otros usuarios del Re:post privado haciendo una pregunta, dando una respuesta o publicando un artículo. Los usuarios también pueden convertir un hilo de discusión en un caso. AWS Support Los usuarios pueden optar por añadir las respuestas desde AWS Support al Re:post privado. Para obtener más información, consulte la Guía del usuario privado de AWS Re:post.

Precios

Solo los clientes con planes Enterprise Support (ES) y Enterprise On-Ramp (EOP) Support pueden suscribirse al servicio Re:post Private. Puede elegir entre los dos niveles de precios disponibles: el nivel gratuito y el nivel estándar. El nivel gratuito le permite explorar y probar todas las funcionalidades del nivel estándar durante seis meses antes de pasar sin problemas a un nivel de pago. Si utilizas el nivel Estándar, puedes pagar una suscripción mensual por usuario para usar Re:post Private. Para obtener más información, consulte Precios.

Cómo comenzar

Para empezar a usar Re:post Private, consulte. Requisitos previos

Requisitos previos

Debe cumplir los siguientes requisitos previos para poder crear un nuevo Re:post privado o administrar un Re:post privado existente en AWS Re:post Private:

- Debe suscribirse a un plan Enterprise o Enterprise On-Ramp Support Plan.
- Debe habilitarlo AWS IAM Identity Center en la misma región en la que desee configurar su Re:post privado.
- Debes crear un AWS Identity and Access Management rol que tenga los permisos necesarios para crear, gestionar y resolver AWS Support los casos por ti. El servicio re:post Private usa este rol para realizar llamadas a la API a. AWS Support Para obtener más información, consulte Administrar el acceso a la creación y administración de AWS Support casos en Re:post Private.

Inicie sesión en Re:Post Private a través del IAM Identity Center

Re:post Private se integra AWS IAM Identity Center para proporcionar una federación de identidades para su fuerza laboral. A través del Centro de Identidad de IAM, se redirige a los usuarios al directorio de su empresa actual para que inicien sesión con sus credenciales actuales. Luego, inician sesión sin problemas en su Re:post privado. Esto garantiza que se apliquen los ajustes de seguridad, como las políticas de contraseñas y la autenticación de dos factores. El uso del Centro de identidad de IAM no afecta a la configuración de IAM actual.

Si no tiene un directorio de usuarios existente o prefiere no federarlo, el Centro de Identidad de IAM ofrece un directorio de usuarios integrado que puede usar para crear usuarios y grupos para Re:Post Private. re:Post Private no admite el uso de usuarios y roles de IAM para asignar permisos dentro de un Re:Post privado. Los permisos de usuario dentro de un Re:post privado los configura un administrador en su aplicación Re:post privada.

Para obtener más información sobre el Centro de identidades de IAM, consulte Qué es AWS IAM Identity Center (sucesor de AWS Single Sign-On). Para obtener más información sobre cómo empezar a utilizar el Centro de identidades de IAM, consulte Introducción. Para utilizar el Centro de identidades de IAM, también debe haber AWS Organizations activado la cuenta.

> **Important**
>
> Re:post Private solo admite instancias organizativas del IAM Identity Center.

Seguridad en Re:post Private

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento que se aplican a AWS Re:post Private, consulte AWS Servicios dentro del alcance por programa de cumplimiento AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar Re:post Private. Los siguientes temas le muestran cómo configurar Re:post Private para cumplir sus objetivos de seguridad y cumplimiento. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Re:post Private.

Temas

Protección de datos en AWS Re:post Private

El modelo de se aplica a protección de datos en AWS Re:post Private. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los. Nube de

AWS Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte el modelo de responsabilidad AWS compartida y la entrada del GDPR blog sobre AWS seguridad.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UseSSL/TLSpara comunicarse con AWS los recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder a AWS través de una interfaz de línea de comandos o unaAPI, utilice un FIPS terminal. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la Norma federal de procesamiento de información () FIPS 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando se trabaja con Re:post Private u otro dispositivo Servicios de AWS mediante la consola,, API o. AWS CLI AWS SDKs Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar su solicitud a ese servidor.

Protección de los datos mediante el cifrado

Cifrado en reposo

Re:post Private utiliza buckets de Amazon Simple Storage Service, bases de datos de Amazon DynamoDB, bases de datos de Amazon Neptune OpenSearch y dominios de Amazon Service que se cifran en reposo mediante claves gestionadas por Amazon o claves gestionadas por el cliente.

Cifrado en tránsito

Re:post Private utiliza el protocolo para comunicarse con la aplicación clienteHTTPS. Utiliza HTTPS y AWS firma para comunicarse con otros servicios en nombre de su aplicación.

Administración de claves

Re:post Private está integrado con claves AWS Key Management Service y es compatible AWS KMS con ellas. Puede personalizar la configuración de cifrado de datos de su Re:post privado al crearlo. Para ello, puedes elegir una AWS KMS clave existente o crear una nueva AWS KMS clave.

Cómo funciona Re:post Private con IAM

Antes de utilizar Re:post Private IAM para gestionar el acceso a AWS Re:post Private, debes saber qué IAM funciones están disponibles para su uso con Re:post Private. Para obtener una visión general de cómo funcionan Re:post Private y otros AWS serviciosIAM, consulta los servicios con los que funcionan en la AWS Guía del usuario. IAM IAM

Políticas de Re:post Private basadas en la identidad

Con las políticas IAM basadas en la identidad, puede especificar las acciones permitidas o denegadas. re:Post Private admite acciones específicas. Para obtener más información sobre los elementos que se utilizan en una JSON política, consulte la referencia sobre los elementos de la IAM JSON política en la Guía del usuario. IAM

Acciones

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones políticas en Re:post Private usan el siguiente prefijo antes de la acción:. `repostspace:` Por ejemplo, para conceder permiso a alguien para ejecutar la `CreateSpace` API operación Re:post Private, debes incluir la `repostspace:CreateSpace` acción en su política. Las declaraciones de política deben incluir un `NotAction` elemento `Action` o. re:Post Private define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

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

Puede utilizar caracteres comodín para especificar varias acciones (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

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

Para ver una lista de las acciones de Re:post Private, consulta las acciones definidas por Re:post Private en la Guía del usuario. IAM

Recursos

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Claves de condición

Re:post Private no proporciona ninguna clave de condición específica del servicio, pero admite el uso de claves de condición globales. Para ver todas las claves de condición AWS globales, consulta las claves de contexto de condición AWS globales en la Guía del usuario. IAM

Ejemplos

Para ver ejemplos de políticas de Re:post Private basadas en la identidad, consulte. AWSEjemplos de políticas basadas en la identidad privada de Re:post

Re:post Políticas basadas en recursos privados

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios. AWS Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puede usar políticas AWS administradas desde una política IAM basada en recursos.

Re:post Private no admite políticas basadas en recursos.

Autorización basada en etiquetas

Re:post Private permite etiquetar los recursos o controlar el acceso en función de las etiquetas. Para obtener más información, consulte Controlar el acceso a AWS los recursos mediante etiquetas.

Roles privados de Re:post IAM

Un IAMrol es una entidad de tu AWS cuenta que tiene permisos específicos.

Usar credenciales temporales con Re:post Private

Recomendamos encarecidamente utilizar credenciales temporales para iniciar sesión con la federación, asumir un IAM rol o asumir un rol multicuenta. Para obtener credenciales de seguridad temporales, llame a AWS STS API operaciones como AssumeRoleo GetFederationToken.

Re:post Private admite el uso de credenciales temporales.

Roles vinculados al servicio

Los roles vinculados al servicio permiten a AWS los servicios acceder a los recursos de otros servicios para completar una acción por ti. Los roles vinculados al servicio aparecen en tu IAM cuenta y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

Roles de servicio

Esta función permite que un servicio asuma una función de servicio por usted. Esta función permite al servicio acceder a los recursos de otros servicios para completar una acción por usted. Para obtener más información, consulte Crear un rol para delegar permisos a un AWS servicio. Los roles de servicio aparecen en su IAM cuenta y son propiedad de la cuenta. Esto significa que un IAM administrador puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

Uso de roles vinculados a servicios para Re:post Private

AWSRe:post Private usa () roles vinculados al servicio. AWS Identity and Access Management IAM
Un rol vinculado al servicio es un tipo de rol único que está vinculado directamente a IAM Re:post Private. Re:post Private predefine los roles vinculados al servicio e incluyen todos los permisos que el servicio necesita para llamar a otros servicios en tu nombre. AWS

Un rol vinculado al servicio facilita la configuración de Re:Post Private, ya que no es necesario añadir manualmente los permisos necesarios. re:Post Private define los permisos de sus roles vinculados al servicio y, a menos que se defina lo contrario, solo Re:Post Private puede asumir sus roles.
Los permisos definidos incluyen la política de confianza y la política de permisos, y esa política de permisos no se puede adjuntar a ninguna otra entidad. IAM

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulta los AWS servicios que funcionan con funciones vinculadas a servicios IAM y busca los

servicios con la palabra Sí en la columna Funciones vinculadas a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de rol vinculados al servicio para Re:post Private

Re:post Private usa el rol vinculado al servicio denominado AWSServiceRoleForrePostPrivate. re:Post Private usa este rol vinculado al servicio para publicar datos en. CloudWatch

El rol AWSServiceRoleForrePostPrivate vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `repostspace.amazonaws.com`

La política de permisos del rol denominada `AWSrePostPrivateCloudWatchAccess` permite a Re:post Private realizar las siguientes acciones en los recursos especificados:

- Acción sobre: `cloudwatch PutMetricData`

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte los permisos de funciones vinculadas a un servicio en la Guía del IAMusuario.

Para obtener más información, consulte AWSrePostPrivateCloudWatchAccess.

Crear un rol vinculado a un servicio para Re:post Private

No necesita crear manualmente un rol vinculado a servicios. Cuando creas tu primer Re:post privado en el AWS Management Console, el o el AWS CLI, Re:post Private crea automáticamente el AWS API rol vinculado al servicio.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Además, si utilizabas el servicio Re:post Private antes del 1 de diciembre de 2023, cuando comenzó a admitir funciones vinculadas al servicio, Re:post Private creó el rol en tu cuenta. `AWSServiceRoleForrePostPrivate` Para obtener más información, consulte Apareció un nuevo rol en mi. Cuenta de AWS

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando creas tu primer Re:post privado, Re:post Private vuelve a crear el rol vinculado al servicio para ti.

En AWS CLI o en AWS API, crea un rol vinculado a un servicio con el nombre del servicio. `repostspace.amazonaws.com` Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario. IAM Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición de un rol vinculado a un servicio para Re:post Private

Re:post Private no permite editar el rol vinculado al servicio. `AWSServiceRoleForrePostPrivate` Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol utilizando. IAM Para obtener más información, consulte Edición de un rol vinculado a un servicio en la Guía del IAMusuario.

Eliminar un rol vinculado a un servicio para Re:post Private

No es necesario eliminar manualmente el rol de `AWSServiceRoleForrePostPrivate`. Cuando eliminas tu Re:post privado en el AWS Management Console, el o el AWS CLI, Re:post Private elimina automáticamente el AWS API rol vinculado al servicio.

También puedes usar la IAM consola, el o el para eliminar manualmente el AWS CLI rol vinculado al AWS API servicio.

Para eliminar manualmente el rol vinculado al servicio mediante IAM

Utilice la IAM consola AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForrePostPrivate servicio. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario. IAM

Regiones compatibles con los roles vinculados al servicio de Re:post Private

Re:post Private admite el uso de funciones vinculadas al servicio en las regiones en las que el servicio está disponible. AWS

Nombres de las regiones	Identidad de la región	Support in Re:post Private
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Este de EE. UU. (Ohio)	us-east-2	No
Oeste de EE. UU. (Norte de California)	us-west-1	No
Oeste de EE. UU. (Oregón)	us-west-2	Sí
África (Ciudad del Cabo)	af-south-1	No
Asia-Pacífico (Hong Kong)	ap-east-1	No
Asia-Pacífico (Yakarta)	ap-southeast-3	No
Asia-Pacífico (Bombay)	ap-south-1	No
Asia Pacífico (Osaka)	ap-northeast-3	No
Asia Pacífico (Seúl)	ap-northeast-2	No
Asia-Pacífico (Singapur)	ap-southeast-1	Sí
Asia Pacífico (Sídney)	ap-southeast-2	Sí
Asia-Pacífico (Tokio)	ap-northeast-1	No
Canadá (centro)	ca-central-1	Sí
Europe (Fráncfort)	eu-central-1	Sí
Europa (Irlanda)	eu-west-1	Sí
Europa (Londres)	eu-west-2	No
Europa (Milán)	eu-south-1	No
Europa (París)	eu-west-3	No
Europa (Estocolmo)	eu-north-1	No

Nombres de las regiones	Identidad de la región	Support in Re:post Private
Medio Oriente (Baréin)	me-south-1	No
Medio Oriente () UAE	me-central-1	No
América del Sur (São Paulo)	sa-east-1	No

AWSEjemplos de políticas basadas en la identidad privada de Re:post

> **Note**
>
> Para mayor seguridad, cree usuarios federados en lugar de IAM usuarios siempre que sea posible.

De forma predeterminada, AWS Identity and Access Management los usuarios y los roles no tienen permiso para crear o modificar los recursos privados de AWS Re:post. Tampoco pueden realizar tareas con AWS Management Console AWS CLI, o. AWS API IAMEl administrador debe crear IAM políticas que concedan a los usuarios y roles permisos para realizar API operaciones específicas en los recursos específicos que necesitan. A continuación, el administrador debe adjuntar esas políticas a los IAM usuarios o grupos que requieran esos permisos.

Para obtener información sobre cómo crear una política IAM basada en la identidad con estos documentos de JSON política de ejemplo, consulte Creación de IAM políticas en la Guía del IAMusuario.

Temas

- Prácticas recomendadas sobre las políticas
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, eliminar o acceder a los recursos de Re:post Private de tu cuenta. Estas acciones pueden generar costos adicionales para

su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Para obtener más información, consulte las políticas AWS gestionadas o las políticas AWS gestionadas para las funciones laborales en la Guía del IAM usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación de políticas de IAM Access Analyzer en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte Configuración del API acceso MFA protegido en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadasIAM, consulte las prácticas recomendadas de seguridad IAM en la Guía del IAM usuario.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo se muestra cómo se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la tecla o. AWS CLI AWS API

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

Políticas insertadas

Las políticas integradas son políticas que usted crea y administra. Puede integrar políticas integradas directamente en un usuario, grupo o rol. Los siguientes ejemplos de políticas muestran cómo asignar permisos para realizar acciones de AWS Re:post Private. Para obtener información general sobre las políticas integradas, consulte Administración de IAM políticas en la AWS IAM Guía del usuario. Puede usar AWS Management Console, AWS Command Line Interface (AWSCLI) o AWS Identity and Access Management API para crear e incrustar políticas integradas.

Temas

Acceso de solo lectura a Re:post Private

La siguiente política otorga acceso de lectura a un usuario para IAM Identity Center y la consola Re:post Private. Esta política permite al usuario realizar acciones de Re:post Private que son de solo lectura.

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

Acceso completo a Re:post Private

La siguiente política otorga acceso total a un usuario a IAM Identity Center y a la consola Re:post Private. Esta política permite al usuario realizar todas las acciones de Re:post Private.

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

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

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

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

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

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

AWS políticas gestionadas para AWS Re:post Private

El uso de políticas AWS administradas hace que añadir permisos a los usuarios, grupos y roles sea más fácil que escribir las políticas usted mismo. Crear políticas gestionadas por los IAM clientes que proporcionen a tu equipo solo los permisos que necesita requiere tiempo y experiencia. Usa políticas AWS administradas para empezar rápidamente. Estas políticas cubren casos de uso comunes y están disponibles en tu AWS cuenta. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del IAM usuario.

AWS los servicios mantienen y AWS actualizan las políticas administradas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios pueden añadir permisos adicionales a una política AWS gestionada para admitir nuevas funciones. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Lo más probable es que los servicios actualicen una política AWS administrada cuando se lanza una nueva función o cuando hay nuevas operaciones disponibles. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no infringen los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener más información, consulte las políticas AWS administradas en la Guía del IAMusuario.

Temas

- AWS política gestionada: AWSRepostSpaceSupportOperationsPolicy
- AWS política gestionada: AWSrePostPrivateCloudWatchAccess

- AWSRe:post Private actualiza las políticas gestionadas AWS

AWS política gestionada: AWSRepostSpaceSupportOperationsPolicy

Esta política permite al servicio AWS Re:post Private crear, administrar y resolver AWS Support los casos que se crean a través de la aplicación 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 gestionada: AWSrePostPrivateCloudWatchAccess

Esta política permite al servicio Re:post Private publicar datos en. CloudWatch

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "CloudWatchPublishMetrics",
   "Effect": "Allow",
   "Action": [
    "cloudwatch:PutMetricData"
   ],
   "Resource": "*",
   "Condition": {
```

```
    "StringEquals": {
     "cloudwatch:namespace": [
      "AWS/rePostPrivate",
      "AWS/Usage"
     ]
    }
   }
  }
 ]
}
```

AWSRe:post Private actualiza las políticas gestionadas AWS

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Re:post Private desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase al RSS feed de la página. Historial del documento

En la siguiente tabla se describen las actualizaciones importantes de las políticas gestionadas por Re:post Private desde el 26 de noviembre de 2023.

Cambio	Descripción	Fecha
Nueva política - AWSrePost PrivateCloudWatchAccess	Nueva política gestionad a para publicar datos en CloudWatch	26 de noviembre de 2023
Nueva política - AWSRepost SpaceSupportOperationsPolic y	Nueva política gestionada para la función AWS Support en AWS Re:post Private	26 de noviembre de 2023
Re:post Private comenzó a rastrear los cambios	Re:post Private comenzó a rastrear los cambios en sus políticas gestionadas AWS	26 de noviembre de 2023

Solución de problemas de AWS identidad y acceso a Re:post Private

Usa la siguiente información para ayudarte a diagnosticar y solucionar los problemas comunes que pueden surgir al trabajar con Re:post Private y. IAM

Temas

No estoy autorizado a realizar ninguna acción en Re:post Private

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

El siguiente ejemplo de error se produce cuando el `mateojackson` IAM usuario intenta usar la consola para ver detalles sobre un *`my-example-widget`* recurso ficticio pero no tiene los permisos ficticios`repostPrivate:`*`GetWidget`*.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `repostPrivate:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con AWS el administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a Re:post Private.

Algunas te Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario llamado `marymajor` intenta usar la consola para realizar una acción en Re:post Private. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Re:post Private

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que respaldan las políticas basadas en recursos o las listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para más información, consulte lo siguiente:

- Para saber si Re:post Private admite estas funciones, consulta. Cómo funciona Re:post Private con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su propiedad, consulte Proporcionar acceso a un IAM usuario en otro de su Cuenta de AWS propiedad en la Guía del IAMusuario. Cuentas de AWS
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo permitir el acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del IAM usuario.
- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a recursos entre cuentas IAM en la Guía del usuario. IAM

Validación del cumplimiento de Re:post Private AWS

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseñando una arquitectura basada en la HIPAA seguridad y el cumplimiento en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar las empresas AWS para crear HIPAA aplicaciones aptas.

  > **Note**
  >
  > No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulta la Referencia de servicios HIPAA aptos.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de las Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.

- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, por ejemplo PCIDSS, cumpliendo con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS Re:post Private

La infraestructura AWS global se basa Regiones de AWS en zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS Re:post Private

Como servicio gestionado, AWS Re:post Private está protegido por los procedimientos de seguridad de red AWS global que se describen en el documento técnico Amazon Web Services: Overview of Security Processes.

Utiliza las API llamadas AWS publicadas para acceder a Re:post Private a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.0 o una versión posterior. Recomendamos la versión TLS 1.2 o una versión posterior. Los clientes también deben utilizar

conjuntos de cifrado con total confidencialidad (PFS), como (Ephemeral Diffie-Hellman) o DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben firmarse con un identificador de clave de acceso y una clave de acceso secreta que esté asociada a un director. AWS Identity and Access Management También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Cuotas privadas de Re:post

AWS Re:post Private proporciona re:post privados que puede usar en su cuenta en una región determinada. AWS Cuando se registra en Re:post Private, AWS establece cuotas predeterminadas (anteriormente denominadas límites) en cuanto al número de Re:posts privados que puede crear y al tamaño de los Re:posts privados.

Service Quotas

Las siguientes son las cuotas predeterminadas de Re:post Private en tu cuenta. AWS Puede usar la consola Service Quotas para ver la cuota predeterminada. Ninguna de estas cuotas es ajustable. No puedes solicitar un aumento de cuota.

Recurso	Valor predeterminado	Descripción	Ajustable
Número de publicaciones privadas de Re:posts	3	El número máximo de re:posts privados en esta cuenta en la región actual.	No
Re:Post privado gratuito (tamaño de publicación)	10	El tamaño máximo (en GB) de un Re:post privado gratuito.	No
Tamaño de Re:post privado estándar	100	El tamaño máximo (en GB) de un Re:post privado estándar.	No

Límites de limitación de la API

Los siguientes límites de limitación se aplican por cuenta y por región en Re:post Private. Estas cuotas no se pueden aumentar.

Acciones	Tasa de recarga de fichas	Tasa de solicitudes	
CreateSpace	1	1	
ListSpaces	10	10	
GetSpace	10	10	
UpdateSpace	10	10	
DeleteSpace	1	1	
RegisterAdmin	10	100	
DeRegisterAdmin	10	100	
SendInvites	1	1	
TagResource	10	10	
UnTagResource	10	10	
ListTagsForResource	10	10	

Crea, configura y personaliza tu Re:post privado

Temas

Crea un nuevo Re:post privado

Para crear un nuevo Re:post privado, sigue estos pasos:

1. Abre la consola privada de Re:post en https://console.aws.amazon.com/repost-private/.
2. En la página de inicio de la consola, selecciona Crear Re:post privado.
3. Si aún no ha configurado el Centro de identidad de IAM para su cuenta, elija Abrir centro de identidad. Siga las instrucciones de la Guía del usuario de AWS IAM Identity Center que se encuentra en la Guía del usuario de AWS IAM Identity Center.
4. En la página Crear un re:post privado, en la sección de precios, seleccione el nivel gratuito o el nivel estándar según su caso de uso. Si ya utilizaste el nivel gratuito en tu cuenta, la opción del nivel gratuito no está disponible para ti.
5. En Detalles, haz lo siguiente:

   En Nombre, introduce un nombre único para tu Re:post privado.

   (Opcional) En la sección Descripción, introduce una breve descripción de tu Re:post privado.

   En Subdominio personalizado, introduce un nombre personalizado para tu subdominio.
6. (Opcional) Para personalizar la configuración de cifrado de datos, en Cifrado de datos, selecciona Personalizar la configuración de cifrado. A continuación, realiza una de las siguientes acciones:

   En Elija una clave de AWS KMS, seleccione una AWS Key Management Service clave o un nombre de recurso de Amazon (ARN).

   -o bien-

Elija Crear una clave de AWS KMS. A continuación, cree la AWS KMS clave.

7. (Opcional) En Acceso al servicio para la integración de casos de Support, selecciona Habilitar el acceso al servicio para este Re:post.

> **Note**
>
> También puedes activar esta opción después de crear el Re:post privado.

Para seleccionar una función de IAM existente a continuación o crear una nueva función en la consola de IAM, utilice la barra de búsqueda para encontrar su función de IAM actual.

-o bien-

Seleccione crear un nuevo rol en la consola de IAM.

Si decide crear un nuevo rol, siga las instrucciones que se indican enCreación de un rol de IAM.

Si decide usar un rol de servicio existente, en la barra de búsqueda, introduzca el ARN del rol que quiere usar. Elija el rol en la lista desplegable.

Para obtener más información, consulte Administrar el acceso a la creación y administración de AWS Support casos en Re:post Private.

8. (Opcional) En Etiquetas, selecciona Añadir nueva etiqueta. A continuación, introduzca la siguiente información:

En Key, introduce tu clave de etiqueta personalizada.

En Value, introduce el valor de tu etiqueta personalizada.

Para añadir más etiquetas, elija Añadir nueva etiqueta.

9. Elige Crear este Re:post.

Una página de confirmación te permitirá saber que se está creando tu Re:post privado. Puedes ver el estado del Re:post privado en el campo Estado. Cuando se crea tu Re:post privado, en el campo Estado aparece Creando.

La creación del Re:post privado tarda aproximadamente 30 minutos. Cuando tu Re:post privado esté listo, aparecerá el campo Estado en línea. Puede usar el subdominio generado por AWS para su Re:post privado que aparece en la pestaña Configuración para acceder a su Re:post privado. Una vez finalizada la revisión, podrá ver el subdominio personalizado de su Re:post privado en la pestaña Configuración.

Administrar el acceso a la creación y administración de AWS Support casos en Re:post Private

Debe crear un rol AWS Identity and Access Management (IAM) para administrar el acceso a la creación y administración de AWS Support casos desde AWS Re:post Private. Este rol realiza las siguientes AWS Support acciones por usted:

- CreateCase
- AddCommunicationToCase
- ResolveCase

Después de crear el rol de IAM, asocie una política de IAM a este rol para que el rol tenga los permisos necesarios para realizar estas acciones. Este rol lo eliges al crear tu Re:post privado en la consola de Re:post Private.

Los usuarios de tu Re:post privado tienen los mismos permisos que tú concedes al rol de IAM.

> **Important**
>
> Si cambias la función de IAM o la política de IAM, los cambios se aplicarán al Re:post privado que hayas configurado.

Siga estos procedimientos para crear su política y rol de IAM.

Temas

- Utilice una política AWS gestionada o cree una política gestionada por el cliente
- Política de IAM de ejemplo
- Creación de un rol de IAM
- Solución de problemas

Utilice una política AWS gestionada o cree una política gestionada por el cliente

Para conceder los permisos a su función, puede utilizar una política AWS gestionada o una política gestionada por el cliente.

> **Tip**
>
> Si no desea crear una política manualmente, le recomendamos que utilice una política AWS administrada en su lugar y omita este procedimiento. Las políticas administradas disponen automáticamente de los permisos necesarios para ello AWS Support. No es necesario actualizar las políticas manualmente. Para obtener más información, consulte AWS política gestionada: AWSRepostSpaceSupportOperationsPolicy.

Siga este procedimiento para crear una política administrada por el cliente para su rol. Este procedimiento usa el editor de políticas JSON en la consola de IAM.

Para crear una política gestionada por el cliente para Re:post Private

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Create Policy (Crear política).
4. Seleccione la pestaña JSON.
5. Ingrese su JSON y, a continuación, sustituya el JSON predeterminado en el editor. Puede usar la política de ejemplo.
6. Elija Siguiente: etiquetas.
7. (Opcional) Puede usar etiquetas como pares clave-valor para agregar metadatos a la política.
8. Elija Siguiente: Revisar.
9. En la página Review policy (Revisar política), ingrese un Name (Nombre), como *`rePostPrivateSupportPolicy`*, y una Description (Descripción) (opcional).
10. Revise la página de resumen para ver los permisos que permite la política y, a continuación, seleccione Crear política.

Esta política define las acciones que puede llevar a cabo el rol. Para obtener más información, consulte Creación de políticas de IAM (Consola) en la Guía del usuario de IAM.

Política de IAM de ejemplo

Puede asociar la siguiente política de ejemplo a su rol de IAM. Esta política permite que el rol tenga todos los permisos necesarios para realizar todas las acciones necesarias AWS Support. Después de configurar un Re:post privado con el rol, todos los usuarios de tu Re:post privado tendrán los mismos permisos.

```
{
 "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 obtener una lista de las políticas AWS administradas de Re:post Private, consulte. AWS políticas gestionadas para AWS Re:post Private

Puedes actualizar la política para eliminar un permiso de. AWS Support

Para obtener descripciones de cada medida, consulte los siguientes temas en la referencia de autorizaciones de servicio:

- Acciones, recursos y claves de condiciones para AWS Support
- Acciones, recursos y claves de condición para Service Quotas
- Claves de condiciones, recursos y acciones para AWS Identity and Access Management

Creación de un rol de IAM

Después de crear esta política, debe crear el rol de IAM y, a continuación, asociar la política a ese rol. Este rol lo eliges al crear un Re:post privado en la consola de Re:post Private.

Para crear un rol para la creación y administración de casos AWS Support

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Roles y luego seleccione Crear rol.
3. En Trusted entity type (Tipo de entidad de confianza), elija Custom trust policy (Política de confianza personalizada).
4. Para la política de confianza personalizada, introduce lo siguiente:

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

5. Elija Siguiente.
6. En Políticas de permisos, en la barra de búsqueda, introduce la política AWS gestionada o una política gestionada por el cliente que hayas creado, por ejemplo *rePostPrivateSupportPolicy*. Selecciona la casilla de verificación que se encuentra junto a las políticas de permisos que quieres que tenga el servicio.

7. Elija Siguiente.
8. En la página Nombre, revisión y creación, en Nombre del rol, escriba un nombre, por ejemplo *rePostPrivateSupportRole*.
9. (Opcional) En Descripción, ingrese una descripción para el rol.
10. Revise la política de confianza y los permisos.
11. (Opcional) Puede usar etiquetas como valores clave-valor para agregar metadatos al rol. Para obtener más información acerca del uso de etiquetas en IAM, consulte Etiquetado de los recursos de IAM.
12. Seleccione Crear rol. Ahora puedes elegir este rol al configurar un Re:post privado en la consola de Re:post Private. Consulte Crea un nuevo Re:post privado.

Para obtener más información, consulte Creación de un rol para un AWS servicio (consola) en la Guía del usuario de IAM.

Solución de problemas

Consulte los siguientes temas para administrar el acceso a Re:post Private.

Contenido

Quiero restringir el acceso a determinadas acciones a usuarios específicos de mi Re:post privado

De forma predeterminada, los usuarios de tu Re:post privado tienen los mismos permisos especificados en la política de IAM que tú adjuntas a la función de IAM que has creado. Esto significa que cualquier usuario del Re:post privado tiene acceso de lectura o escritura para crear y gestionar AWS Support casos, tenga o no un usuario de IAM. Cuenta de AWS

Recomendamos que siga las siguientes prácticas recomendadas:

- Utilice una política de IAM que tenga los permisos mínimos necesarios para acceder a. AWS Support Consulte AWS política gestionada: AWSRepostSpaceSupportOperationsPolicy.

Cuando configuro un Re:post privado, no veo el rol de IAM que he creado

Si tu función de IAM no aparece en la lista de funciones de IAM de Re:post Private;, significa que la función no tiene a Re:post Private como entidad de confianza o que la función se ha eliminado. Puede actualizar el rol actual o crear otro. Consulte Creación de un rol de IAM.

A mi rol de IAM le falta un permiso

El rol de IAM que crees para tu Re:post privado necesita permisos para realizar las acciones que desees. Por ejemplo, si quieres que tus usuarios del Re:post privado creen casos de soporte, el rol debe tener el `support:CreateCase` permiso. Re:post Private asume este rol para realizar estas acciones por ti.

Si recibes un error sobre la falta de un permiso AWS Support, comprueba que la política asociada a tu rol tenga el permiso necesario.

Consulte la Política de IAM de ejemplo anterior.

Un error indica que mi función de IAM no es válida

Compruebe que ha elegido el rol correcto para su configuración privada de Re:post.

Configure y administre el acceso de los usuarios mediante AWS IAM Identity Center

Re:post Private se integra AWS IAM Identity Center para proporcionar una federación de identidades a la fuerza laboral de su organización. Utilice IAM Identity Center para crear o conectar usuarios de su organización y gestionar de forma centralizada su acceso a todas sus AWS cuentas y aplicaciones. Para obtener más información sobre el Centro de identidades de IAM, consulte Qué es AWS IAM Identity Center (sucesor de AWS Single Sign-On). Para obtener más información sobre cómo empezar a utilizar el Centro de identidades de IAM, consulte Introducción. Para utilizar el Centro de identidades de IAM, también debe haber AWS Organizations activado la cuenta.

Personalice su Re:post privado

Puedes añadir uno o más administradores a tu Re:post privado después de crearlo. Los administradores utilizan la aplicación Re:post Private para iniciar el Re:post privado y gestionar los usuarios que contiene. Pueden personalizar la imagen de marca del Re:post privado, añadir

etiquetas para clasificar el contenido y seleccionar temas de interés para rellenar automáticamente el contenido. Para obtener más información, consulte la Guía de administración privada de AWS Re:post.

Invite a los usuarios a su Re:post privado

Puedes añadir uno o más usuarios a tu Re:post privado después de crearlo. Puedes invitar a los usuarios a colaborar en tu Re:post privado. Los usuarios utilizan la aplicación Re:post Private para iniciar sesión con las credenciales que hayas configurado. Tras iniciar sesión en un Re:post privado, los usuarios pueden navegar o buscar contenido existente, incluida formación personalizada y contenido técnico que se ajuste a sus temas de interés. Para obtener más información, consulte la Guía del usuario privado de AWS Re:post.

Administra tu Re:post privado en la consola de Re:post Private

En esta sección se explica cómo puede administrar su re:post privado en la consola privada de AWS re:post.

Temas

Añada usuarios y grupos a su Re:post privado

Si es administrador, puede añadir usuarios y grupos a su Re:post privado.

Añade usuarios a tu Re:post privado

1. Abre la consola privada de Re:post en https://console.aws.amazon.com/repost-private/.
2. En el panel de navegación, selecciona All my private Re:posts.
3. Elige el Re:post privado que quieras gestionar.
4. Elija la pestaña Users.
5. En Usuarios, selecciona Añadir usuarios y grupos.
6. En la lista, selecciona los usuarios que quieres añadir a tu Re:post privado. Luego, elige Asignar.

Los usuarios seleccionados se añaden a tu Re:post privado y aparecen en la pestaña Usuarios.

Añade grupos a tu Re:post privado

1. Abre la consola privada de Re:post en https://console.aws.amazon.com/repost-private/.
2. En el panel de navegación, selecciona All my private Re:posts.

3. Elige el Re:post privado que quieras gestionar.
4. Seleccione la pestaña Groups (Grupos).
5. Selecciona Añadir usuarios y grupos.
6. En la lista, selecciona los grupos que quieres añadir a tu Re:post privado. Luego, elige Asignar.

Los grupos seleccionados se añaden a tu Re:post privado y aparecen en la pestaña Grupos.

Añade usuarios a un grupo en tu Re:post privado

Utilice el centro de identidad de IAM para añadir nuevos usuarios a un grupo existente en su Re:post privado. Para obtener más información, consulte Añadir usuarios a grupos en la Guía del usuario de AWS IAM Identity Center.

Invite a usuarios y grupos a su Re:post privado

Siga estos pasos para invitar a usuarios y grupos a su Re:post privado en AWS Re:post Private:

1. Abra la consola privada de Re:post en https://console.aws.amazon.com/repost-private/.
2. En el panel de navegación, selecciona All my private Re:posts.
3. Elige el Re:post privado que quieras gestionar.
4. Para invitar a los usuarios a tu Re:post privado, selecciona la pestaña Usuarios.

   En la lista, selecciona los usuarios a los que quieres invitar a tu Re:post privado. Luego, selecciona Incorporar usuarios para re:publicar.
5. En el cuadro de diálogo Incorporar usuarios a este Re:post privado, introduce la siguiente información:

   En Asunto, introduce el asunto del mensaje de correo electrónico que vas a enviar.

   En Body, introduce un mensaje de bienvenida para tu Re:post privado.

   Selecciona Enviar correo electrónico de incorporación.
6. Para invitar a grupos a tu Re:post privado, selecciona la pestaña Grupos.

   En la lista, selecciona los grupos a los que quieres invitar a tu Re:post privado. Luego, selecciona Incorporar grupos para Re:publicar.

7. En el cuadro de diálogo Incorporar grupos a este Re:post privado, introduce la siguiente información:

   En Asunto, introduce el asunto del mensaje de correo electrónico que vas a enviar.

   En Body, introduce un mensaje de bienvenida para tu Re:post privado.

   Selecciona Enviar correo electrónico de incorporación.

El mensaje de bienvenida se envía a todos los usuarios y grupos seleccionados con información sobre cómo iniciar sesión en tu Re:post privado.

Promociona a un usuario de tu Re:post privado como administrador

Para ascender a administrador a un usuario privado de Re:post, siga estos pasos:

1. Abre la consola privada de Re:post en https://console.aws.amazon.com/repost-private/.
2. En el panel de navegación, selecciona All my private Re:posts.
3. Elige el Re:post privado que quieras gestionar.
4. Elija la pestaña Users.
5. Seleccione uno o más usuarios que desee ascender a administradores.
6. Selecciona Editar rol y, a continuación, elige Convertir en administrador.

Los usuarios seleccionados ascienden a administradores. En la pestaña Usuarios, el rol de estos usuarios se actualiza a Administrador.

Elimina usuarios o grupos de tu Re:post privado

Si es administrador, puede eliminar usuarios o grupos de su Re:post privado.

Elimina usuarios de tu Re:post privado

1. Abre la consola privada de Re:post en https://console.aws.amazon.com/repost-private/.
2. En el panel de navegación, selecciona All my private Re:posts.
3. Elige el Re:post privado que quieras gestionar.
4. En Usuarios, de la lista, selecciona los usuarios que quieres eliminar de tu Re:post privado. A continuación, selecciona Eliminar.

Los usuarios seleccionados se eliminan de tu Re:post privado. La información sobre los usuarios eliminados ya no aparece en la pestaña Usuarios.

Elimina grupos de tu Re:post privado

1. Abre la consola privada de Re:post en https://console.aws.amazon.com/repost-private/.
2. En el panel de navegación, selecciona All my private Re:posts.
3. Elige el Re:post privado que quieras gestionar.
4. Seleccione la pestaña Groups (Grupos).
5. De la lista, selecciona los grupos que quieres eliminar de tu Re:post privado. Luego, elige Eliminar.

Los grupos seleccionados se eliminarán de tu Re:post privado. La información sobre los grupos eliminados ya no aparece en la pestaña Grupos.

Agrega o elimina a un AWS empleado de tu Re:post privado

Si tiene un plan Enterprise o Enterprise On-Ramp Support, puede añadir o eliminar a un empleado de AWS de su Re:post privado. Póngase en contacto con Concierge Support o con su administrador técnico de cuentas (TAM) para obtener más información.

Elimine un Re:post privado de Re:post Private

Para eliminar un Re:post privado en AWS Re:post Private, siga estos pasos:

1. Abra la consola privada de Re:post en https://console.aws.amazon.com/repost-private/.
2. En el panel de navegación, selecciona All my private Re:posts.
3. Elige el Re:post privado que quieras gestionar y, a continuación, selecciona Eliminar.
4. Selecciona todas las opciones para confirmar y confirmar que deseas eliminar permanentemente el Re:post privado y los datos asociados a él.

> **Important**
>
> Al eliminar el Re:post privado, se eliminará toda la información de configuración relacionada con el Re:post privado. Una vez que se elimine el Re:post privado, no podrás restaurar ningún contenido del mismo.

5. Introduce el nombre de tu Re:post privado cuando se te solicite un consentimiento adicional por escrito. A continuación, elija Delete (Eliminar).

Tu Re:post privado tarda aproximadamente 30 minutos en eliminarse.

Supervisión de AWS Re:Post Private

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Re:post Private y del resto AWS de sus soluciones. AWSproporciona las siguientes herramientas de monitoreo para ver Re:post Private, informar cuando algo anda mal y tomar medidas automáticas cuando sea apropiado:

- Amazon CloudWatch monitorea sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon EC2 y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulte la Guía del CloudWatch usuario de Amazon.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por usted o para usted Cuenta de AWS y envía los archivos de registro a un bucket de Amazon S3 que especifique. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Supervisión de AWS Re:Post Private con Amazon CloudWatch

Puede monitorizar AWS Re:Post Private con Amazon CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se guardan durante 15 meses para que pueda acceder a la información histórica y obtener una mejor perspectiva del rendimiento de su aplicación o servicio web. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

El servicio Re:post Private informa de las siguientes métricas en el `AWS/rePostPrivate` espacio de nombres.

Métrica	Descripción
`NumberOfSpaces`	El número de Re:posts privados en la cuenta corriente.

Métrica	Descripción
	Unidades: recuento
`NumberOfUsers`	El número de usuarios de un Re:post privado. Esta métrica utiliza SpaceID como dimensión. Unidades: recuento
`ContentSize`	La cantidad de contenido de un Re:post privado. Esta métrica usa SpaceID como dimensión. Unidades: bytes

Las métricas de Re:post Private admiten las siguientes dimensiones.

Dimensión	Descripción
`spaceId`	El identificador único del Re:post privado.

Registro de llamadas a la API privada Re:Post de AWS mediante AWS CloudTrail

AWS Re:post Private está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Re:post Private. CloudTrail captura todas las llamadas a la API de Re:post Private como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Re:post Private y las llamadas en código a las operaciones de la API de Re:post Private. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Re:post Private. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puedes determinar la solicitud que se realizó a Re:post Private, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulta la Guía del AWS CloudTrailusuario.

Re:publique información privada en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Re:post Private, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los últimos eventos de la Cuenta de AWS. Para obtener más información, consulte Trabajar con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventosCuenta de AWS, incluidos los eventos de Re:post Private, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte lo siguiente:

- Creación de un registro de seguimiento de su cuenta de AWS
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de re:post Private se registran CloudTrail y se documentan en la referencia de la API privada de AWS re:post. re:post Private admite el registro de las siguientes acciones como eventos en los archivos de registro: CloudTrail

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

- TagResource
- UntagResource
- UpdateSpace

Re:post Private permite registrar las siguientes acciones AWS Support como eventos en los archivos de registro: CloudTrail

- CreateCase
- AddCommunicationToCase
- ResolveCase

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Comprensión de las entradas del archivo de registro privado de Re:post

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateSpace` acción.

```
{
   "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"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `RegisterAdmin` acción.

```
{
   "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"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `ListSpaces` acción.

```
 {
    "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"
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `ResolveCase` acción. Puede utilizar el `sourceIdentity` elemento de esta entrada de registro para identificar al usuario que resolvió el 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"
    }
}
```

Solución de problemas de Re:post Private

La siguiente información puede ayudarle a solucionar problemas con AWS Re:Post Private.

Temas

No puedo configurar mi Re:Post privado en una región específica AWS

Re:post Private solo está disponible en las regiones EE.UU. Este (Norte de Virginia), EE.UU. Oeste (Oregón), Europa (Fráncfort), Asia Pacífico (Singapur), Asia Pacífico (Sídney), Canadá (Central) y Europa (Irlanda). Asegúrate de crear tu Re:post privado en una de estas regiones.

No puedo configurar un Re:post privado en mi cuenta

Asegúrese de haber habilitado AWS IAM Identity Center su cuenta y configurar el Centro de Identidad de IAM en la misma región en la que desea crear el Re:post privado. Para obtener más información, consulte Requisitos previos.

No se pueden administrar usuarios o grupos en un Re:post privado

Asegúrese de tener los permisos necesarios para editar un Re:post privado y administrar los usuarios y grupos dentro del Re:post privado. Para obtener más información, consulte AWSEjemplos de políticas basadas en la identidad privada de Re:post.

Historial del documento

En la siguiente tabla se describen las versiones de documentación de AWS Re:Post Private:

Cambio	Descripción	Fecha
Actualización	Se agregaron EE. UU. Este (Norte de Virginia), Asia-Pacífico (Sídney), Canadá (Centro) y Europa (Irlanda) a las regiones compatibles	10 de mayo de 2024
Actualización	Se agregó Asia Pacífico (Singapur) a las regiones compatibles	6 de marzo de 2024
Recursos nuevos	Se agregó documentación sobre las políticas administradas por AWS para AWS Re:Post Private	26 de noviembre de 2023
Versión inicial	Versión inicial de la guía de administración de la consola privada Re:post	26 de noviembre de 2023

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.