Guía del usuario

Explorador de recursos de AWS

Explorador de recursos de AWS: Guía del usuario

Table of Contents

¿Qué es Explorador de recursos de AWS?

Explorador de recursos de AWS es un servicio de búsqueda y descubrimiento de recursos. Con Resource Explorer, puede explorar sus recursos, como las instancias de Amazon Elastic Compute Cloud, las transmisiones de Amazon Kinesis o las tablas de Amazon DynamoDB, a través de una experiencia similar a la de un motor de búsqueda en Internet. Puede buscar sus recursos mediante meta-datos de recursos, como nombres, etiquetas e ID. Resource Explorer funciona en todas las Regiones de AWS de su cuenta para simplificar las cargas de trabajo entre regiones.

Resource Explorer brinda respuestas rápidas a sus consultas de búsqueda mediante el uso de índices que el servicio de Explorador de recursos de AWS crea y mantiene. Resource Explorer utiliza una variedad de orígenes de datos para recopilar información sobre los recursos de su Cuenta de AWS. Resource Explorer almacena esa información en los índices para poder realizar la búsqueda.

> Nos gustaría recibir sus comentarios sobre esta documentación
>
> Nuestro objetivo es ayudarlo a explotar al máximo Resource Explorer. Si esta guía lo ayuda a hacerlo, háganoslo saber. Si la guía no lo ayuda, queremos escucharlo para poder abordar el problema. Utilice el enlace de Comentarios ubicado en la esquina superior derecha de cada página. Esto envía sus comentarios directamente a los redactores de esta guía. Revisamos cada aporte para poder mejorar la documentación. ¡Gracias de antemano por su ayuda!

Temas

¿Es la primera vez que usa Resource Explorer?

Si es la primera vez que usa Resource Explorer, le recomendamos leer primero los siguientes temas en la sección Comenzar:

- Términos y conceptos de Resource Explorer
- Configuración de Resource Explorer mediante Configuración Rápida

Características de Resource Explorer

Resource Explorer posee las siguientes características:

- Los usuarios pueden buscar recursos en su Región de AWS o entre las regiones de su Cuenta de AWS.
- Los usuarios pueden usar palabras clave, operadores de búsqueda y atributos, como etiquetas, para filtrar los resultados de la búsqueda y ver solo los recursos que coincidan.
- Cuando los usuarios encuentran un recurso en los resultados de la búsqueda, pueden ir inmediatamente a la consola nativa del recurso para trabajar con ese recurso.
- Los administradores pueden crear vistas que definan qué recursos se encuentran disponibles en los resultados de la búsqueda. Los administradores pueden crear distintas vistas para distintos grupos de usuarios en función de sus tareas y conceder permisos de visualización únicamente a los usuarios que los necesiten.
- Resource Explorer, como muchos otros Servicios de AWS, es eventualmente coherente. Resource Explorer alcanza una alta disponibilidad al replicar los datos entre varios servidores ubicados en los centros de datos de Amazon de todo el mundo. Si se realiza correctamente una solicitud para cambiar algunos datos, el cambio se confirma y se almacena de forma segura. Sin embargo, el cambio debe replicarse en Resource Explorer, lo que puede demorar. Por ejemplo, Resource Explorer busca un recurso en una región y lo replica en la región que contiene el índice agregador de la cuenta.

Servicios de AWS relacionados

Los siguientes son otros Servicios de AWS cuya finalidad principal es ayudarlo a administrar los recursos de AWS:

AWS Resource Access Manager (AWS RAM)

Comparta los recursos de una Cuenta de AWS con otras Cuentas de AWS. Si AWS Organizations gestiona su cuenta, puede utilizar AWS RAM para compartir recursos con las cuentas de una unidad organizativa o con todas las cuentas de la organización. Los recursos

compartidos funcionan para los usuarios de esas cuentas como si se hubieran creado en la cuenta local.

AWS Resource Groups

Crear grupos para sus recursos de AWS. Luego, puede usar y administrar cada grupo como una unidad en lugar de tener que hacer referencia a cada recurso individualmente. Los grupos pueden consistir en recursos que formen parte de la misma pila de AWS CloudFormation o que estén etiquetados con las mismas etiquetas. Algunos tipos de recursos también admiten la aplicación de una configuración a un grupo de recursos para afectar a todos los recursos relevantes de ese grupo.

Editor de etiquetas y AWS Resource Groups Tagging API

Las etiquetas son meta-datos definidos por el cliente que puede adjuntar a sus recursos. Puede clasificar sus recursos para fines como la asignación de costos y el control de acceso basado en atributos.

Acceso a Resource Explorer

Puede interactuar con Resource Explorer de las siguientes maneras:

Consola de Resource Explorer

Resource Explorer cuenta con una interfaz de usuario basada en web, la consola del Resource Explorer. Si se registró en una Cuenta de AWS, podrá obtener acceso a la consola de Resource Explorer al iniciar sesión en la AWS Management Console y al seleccionar Resource Explorer desde la página de inicio de la consola.

También puede navegar en su buscador directamente a la página del panel de Resource Explorer, o a la página de búsqueda de recursos. Si todavía no se ha registrado, se le pedirá que lo haga antes de que aparezca la consola.

> **Note**
>
> La consola de Resource Explorer es una consola global, lo que significa que no tiene que seleccionar ninguna Región de AWS para trabajar en ella. Sin embargo, al utilizar Resource Explorer para crear un índice o una vista, debe especificar en qué región se almacena el índice o la vista. Al utilizar Resource Explorer para realizar las búsquedas, puede elegir cualquier vista a la que tenga acceso. Los resultados proceden

automáticamente de la región asociada a la vista seleccionada. Si la vista proviene de la región que contiene el índice agregador, los resultados incluyen los recursos de todas las regiones en las que creó los índices de Resource Explorer

Búsqueda unificada de la AWS Management Console

En la parte superior de cada página en la AWS Management Console hay una barra de búsqueda. Puede configurar Resource Explorer para que participe en la búsqueda unificada. Luego, los usuarios pueden usar la sintaxis de consulta de búsqueda de Resource Explorer en el cuadro de texto de búsqueda unificada y ver los recursos asociados en esos resultados de búsqueda. Al activar esta característica, los usuarios pueden buscar recursos desde la consola de cualquier Servicio de AWS sin tener que cambiar primero a la consola de Resource Explorer.

> **Important**
>
> La búsqueda unificada siempre busca mediante el uso de la vista predeterminada en la Región de AWS que contiene el índice agregador.

Comandos del Explorador de recursos en AWS CLI y Herramientas para Windows PowerShell

Los AWS CLI y las herramientas PowerShell proporcionan acceso directo a las operaciones de la API pública de Resource Explorer. Estas herramientas funcionan en Windows, macOS y Linux. Para obtener más información acerca de cómo empezar, consulte la Guía del usuario de la AWS Command Line Interface o la Guía del usuario de AWS Tools for Windows PowerShell. Para obtener más información acerca de los comandos de Resource Explorer, consulte la Referencia de comandos de la AWS CLI o la Referencia cmdlet de AWS Tools for Windows PowerShell.

Operaciones de Resource Explorer en los AWS SDK

AWS cuenta con comandos de API para una amplia gama de lenguajes de programación. Si necesita más información sobre cómo comenzar, consulte Explorador de recursos de AWS Utilización con un AWS SDK.

API de consulta

Si no utiliza uno de los lenguajes de programación compatibles, la API de consulta HTTPS de Resource Explorer le proporciona acceso programático a Resource Explorer. Con la API de Resource Explorer, puede emitir solicitudes HTTPS directamente al servicio. Cuando use la API

de Resource Explorer, debe incluir el código que pueda firmar digitalmente las solicitudes al utilizar sus credenciales de AWS. Para obtener más información, consulte la Referencia de la API de Explorador de recursos de AWS.

Precios

La búsqueda de recursos mediante Explorador de recursos de AWS es gratuita, lo que incluye la creación de vistas, la activación de regiones o la búsqueda de recursos. Durante el proceso de creación de su inventario de recursos, Resource Explorer llama a las API en su nombre, lo que puede generar cargos. La interacción con los recursos que encuentres en los resultados de la búsqueda puede generar cargos por uso que varían en función del tipo de recurso y del mismoServicio de AWS. Para obtener más información acerca de cómo AWS factura por el uso normal de un tipo de recurso específico, consulte la documentación del servicio de propiedad de dicho tipo de recurso.

Introducción a Resource Explorer

Los temas de esta sección lo ayudarán a asimilar las nociones esenciales de los conceptos y términos utilizados por Explorador de recursos de AWS. Conozca los requisitos previos que debe cumplir para utilizar correctamente Resource Explorer y cómo activarlo en su Cuenta de AWS.

Temas

Términos y conceptos de Resource Explorer

Explorador de recursos de AWS es un servicio de búsqueda y descubrimiento de recursos. Con Resource Explorer puede explorar sus recursos mediante el uso de una experiencia similar a la de un motor de búsqueda en Internet. Puede buscar los recursos, como instancias de Amazon Elastic Compute Cloud, transmisiones de Amazon Kinesis o tablas de Amazon DynamoDB, mediante el uso de metadatos de recursos como nombres, etiquetas e ID. Resource Explorer funciona en todas las Regiones de AWS en su cuenta para simplificar las cargas de trabajo entre regiones.

Resource Explorer brinda respuestas rápidas a sus consultas de búsqueda mediante el uso de índices que el servicio de Explorador de recursos de AWS crea y mantiene. Resource Explorer utiliza una variedad de orígenes de datos para recopilar información sobre los recursos de su Cuenta de AWS. Resource Explorer almacena esa información en sus índices para la búsqueda.

Debe comprender los siguientes conceptos para administrar y configurar correctamente Explorador de recursos de AWS para los usuarios.

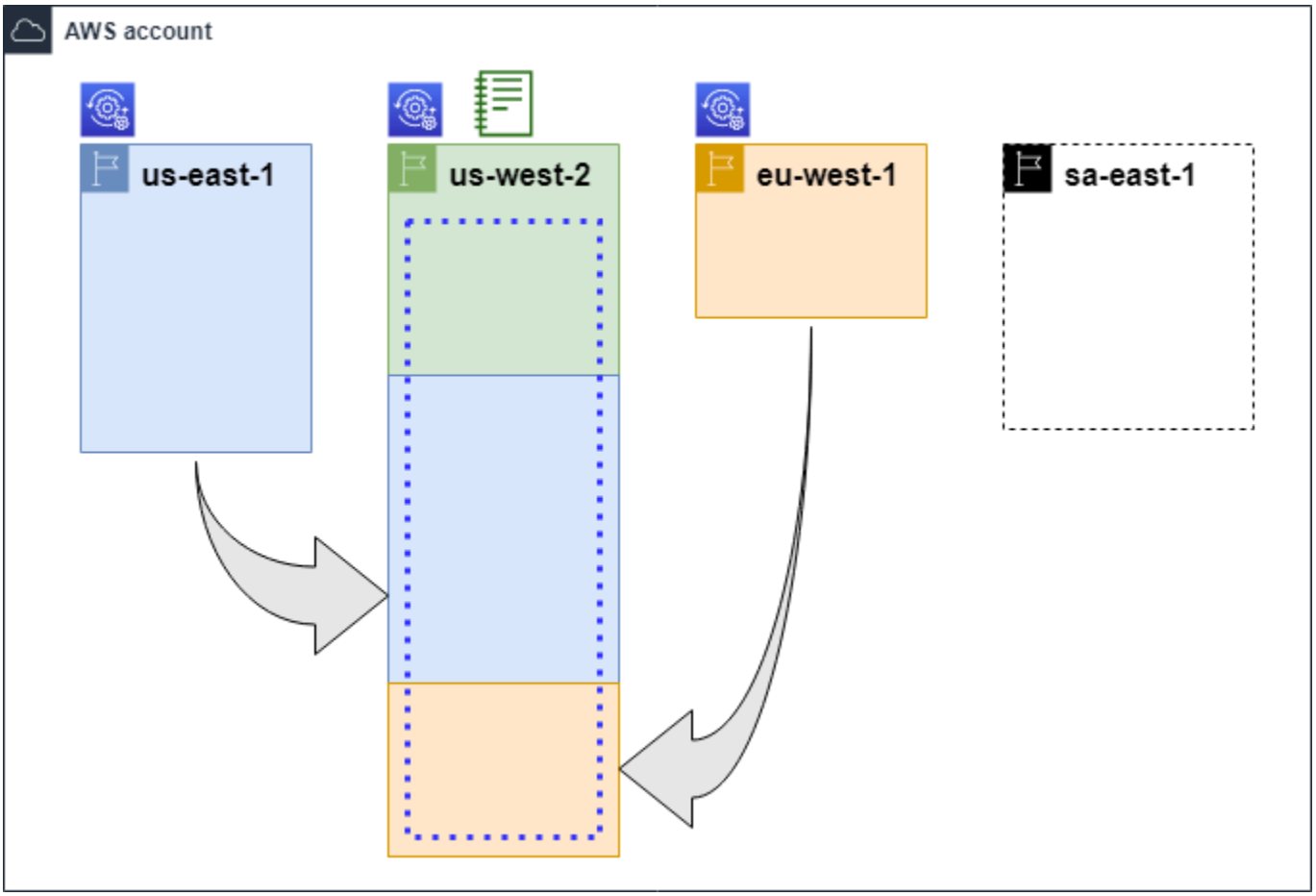
Conceptos

- Búsqueda unificada en la AWS Management Console
- Búsqueda multicuenta

En el siguiente diagrama, se muestran tres Regiones de AWS en las que el administrador activó Resource Explorer, y una región que el administrador decidió no activar. La región en la que no está activado Resource Explorer no cuenta con un índice. Por lo tanto, no se puede buscar sus recursos a través de las consultas de Resource Explorer.

En este escenario de ejemplo, el administrador eligió la región Oeste de EE. UU. (Oregón) (`us-west-2`) para contener el índice agregador de la cuenta. Todas las regiones que active replican sus índices locales en la región con el índice agregador.

La vista predeterminada creada por Resource Explorer no tiene ningún filtro. Por lo tanto, los resultados de las búsquedas con esta vista pueden incluir recursos de cualquier tipo en todas las regiones de la cuenta en las que se activó Resource Explorer.



Leyenda

	Se activó Resource Explorer en esta Región de AWS y la información sobre los recursos de la región se almacena en un índice local de esa región. El índice local de cada región también se replica (indicado con las flechas) en la región que contiene el índice agregador.
	El índice que contiene esta Región de AWS se encuentra configurado para ser el índice agregador de la cuenta. Resource Explorer replica la información de recursos recopilada en los índices locales de todas las demás regiones en las que se encuentra activado en el índice agregador de esta región. Las búsquedas realizadas en esta región pueden incluir los resultados de todas las regiones de la cuenta.
	La vista predeterminada creada por la Configuración Rápida incluye la totalidad de los recursos de todas las Regiones de AWS.

Administrador de Resource Explorer

El administrador de Resource Explorer es una AWS Identity and Access Management entidad principal (IAM) que tiene permiso para administrar Resource Explorer y su configuración en la Cuenta de AWS . El administrador de Resource Explorer puede configurar las siguientes características:

- Active Resource Explorer para las Regiones de AWS individuales en la Cuenta de AWS mediante la creación de índices en esas regiones. Esto permite a Resource Explorer descubrir los recursos y rellenar el índice con información sobre esos recursos para que los usuarios puedan buscarlos en esa región.
- Actualice el tipo de índice en una Región de AWS para convertirlo en el índice agregador de su Cuenta de AWS. El índice agregador de esta región recibe copias replicadas de la información de los recursos de todas las demás regiones de la cuenta en la que está activado Resource Explorer.
- Cree vistas que definan el subconjunto de información indexada que los usuarios pueden buscar y descubrir en Resource Explorer.
- Si bien no forma parte de las acciones de Resource Explorer, el administrador de este también debe poder conceder permisos de búsqueda a las entidades principales de la cuenta. El administrador puede conceder estos permisos a las entidades principales al añadir los permisos pertinentes a las políticas de permisos de IAM existentes o mediante el uso de la política administrada de AWS de solo lectura de Resource Explorer.

  Para brindar acceso, añada permisos a sus usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.

- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidades de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones de Adición de permisos a un usuario (consola) en la Guía del usuario de IAM.

El administrador normalmente tiene todos los permisos de Resource Explorer (`resource-explorer-2:*`) en todos los recursos de Resource Explorer, incluidos los índices y las vistas. Estos permisos se pueden conceder mediante la política administrada de AWS de acceso total a Resource Explorer.

Usuario de Resource Explorer

El usuario de Resource Explorer es una entidad principal de IAM que tiene permiso para realizar una o más de las siguientes tareas:

- Realizar una búsqueda de recursos con una vista para consultar al Resource Explorer. Un usuario de Resource Explorer desea descubrir y encontrar recursos de AWS y, por lo general, utiliza la consola de Resource Explorer o las operaciones de `Search` de Resource Explorer que proporcionan los AWS SDK o la AWS CLI.

  Un rol o un usuario pueden usar IAM para obtener permiso para buscar mediante uno de estos dos métodos:

  - La política administrada de AWS de solo lectura de Resource Explorer para el rol de IAM, grupo o usuario.
  - Una política de permisos de IAM con una declaración que contiene los siguientes permisos mínimos para el rol de IAM, grupo o usuario.

```
{
    "Effect": "Allow",
    "Action": [
        "resource-explorer-2:Search",
        "resource-explorer-2:GetView",
    "Resource": "<ARN of the view>"
}
```

- Aunque normalmente se considera una tarea del administrador, puede delegar en usuarios de confianza la capacidad de definir las vistas de creación. Para ello, el administrador puede conceder permiso para llamar a la operación de `resource-explorer-2:CreateView` mediante una política de permisos de IAM asociada a los roles, grupos o usuarios pertinentes. Si la vista requiere permisos específicos, entonces, debe preverse la posibilidad de añadir o modificar las políticas de IAM para los usuarios pertinentes.

Para obtener información acerca de cómo buscar recursos con Resource Explorer, consulte Uso de Explorador de recursos de AWS para buscar recursos.

Índice

El índice es la recopilación de información que mantiene Resource Explorer sobre todos los recursos de AWS que contiene una Región de AWS en la Cuenta de AWS. Resource Explorer mantiene un índice en cada región en la que active Resource Explorer. Resource Explorer actualiza el índice automáticamente a medida que crea y elimina recursos en su Cuenta de AWS. En el diagrama anterior, los cuadros situados debajo de los nombres de la Región de AWS representan los índices de Resource Explorer que se mantienen en cada Región de AWS. El índice de una región es la fuente de información de cualquier vista creada en esa región. Los usuarios no pueden consultar el índice directamente. En cambio, siempre deben realizar consultas mediante una vista.

Existen dos tipos de índices:

Índice local

Hay un índice local en cada Región de AWS en la que activa Resource Explorer. El índice local contiene información sobre los recursos de la misma región solamente.

Índice agregador

El administrador de Resource Explorer también puede designar el índice en una Región de AWS para que actúe como índice agregador de la Cuenta de AWS. El índice agregador recibe

y almacena una copia del índice para todas las demás regiones en las que Resource Explorer esté activado para la cuenta. El índice agregador también recibe y almacena información sobre los recursos de su propia región. En el diagrama anterior, la región `us-west-2` contiene el índice agregador de la cuenta. La razón principal para designar un índice agregador para la cuenta es poder crear vistas que puedan incluir los recursos de todas las regiones de la cuenta. Solo puede haber un índice agregador en una Cuenta de AWS.

Al activar Resource Explorer, puede especificar la Región de AWS que debe contener el índice agregador. También puede cambiar la Región de AWS que se utiliza para el índice agregador más adelante. Para obtener información sobre cómo promover un índice local para convertirlo en el índice agregador para su Cuenta de AWS, consulte Activación de la búsqueda entre regiones mediante la creación de un índice agregador.

El índice es un recurso con un nombre de recurso de Amazon (ARN). Sin embargo, puede usar este ARN solo en las políticas de permisos para conceder acceso a las operaciones que interactúan directamente con el índice. Con estas operaciones, puede crear vistas y configurarlas como predeterminadas en una región, activar o desactivar Resource Explorer en una región y crear un índice agregador para la cuenta. El ARN del índice tiene un aspecto similar al del siguiente ejemplo:

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd11111111
```

Visualización

Una vista es el mecanismo que se utiliza para consultar los recursos que figuran en un índice. La vista define qué información del índice se encuentra visible y disponible para los fines de búsqueda y descubrimiento. Un usuario nunca consulta directamente el índice de Resource Explorer. Por el contrario, las consultas siempre deben pasar por una vista que permita a su creador limitar los recursos que el usuario puede ver en los resultados de la búsqueda.

Al crear una vista, se especifican filtros que restringen los recursos que se incluyen en los resultados de la búsqueda. Por ejemplo, puede optar por incluir solo los recursos de unos pocos tipos de recursos específicos que utilizan las personas a las que concede acceso a esta vista. Los resultados de las consultas que realizan los usuarios con una vista se filtran siempre automáticamente para incluir solo los recursos que coinciden con los criterios de la vista.

Para conceder acceso para usar una vista, puede utilizar asignar permisos mediante uno de los siguientes métodos.

Para proporcionar acceso, agregar permisos a sus usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.

- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidades de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones de Adición de permisos a un usuario (consola) en la Guía del usuario de IAM.

Conceda permiso para permitir que sus roles, grupos o usuarios invoquen el `resource-explorer-2:GetView` y las operaciones de `resource-explorer-2:Search` en una vista identificada por su nombre de recurso de Amazon (ARN). Como alternativa, puede utilizar la política administrada de AWS de solo lectura de Resource Explorer para todas las entidades principales que necesiten utilizar la vista para realizar búsquedas. Puede crear varias vistas con distintos filtros y ámbitos y, por lo tanto, devolver distintos subconjuntos de la información de sus recursos. Luego, puede conceder permisos para cada vista a los usuarios que necesiten ver la información incluida en los resultados de esa vista.

Para realizar búsquedas con Resource Explorer, cada usuario debe tener permiso para usar al menos una vista. No puede realizar una búsqueda en Resource Explorer sin usar una vista.

Las vistas se almacenan por región. Una vista solo puede acceder al índice de Resource Explorer en esa Región de AWS. Para acceder a los resultados de búsqueda de toda la cuenta, debe utilizar una vista de la región que contenga el índice agregador de la cuenta. La opción de Configuración Rápida crea una vista predeterminada de la Región de AWS con el índice agregador y con filtros que incluyen todos los recursos de todas las Regiones de AWS que utilizó la cuenta.

Para obtener información acerca de cómo crear vistas, consulte Cómo administrar las vistas de Resource Explorer para proporcionar acceso a la búsqueda. Para obtener información acerca

de cómo utilizar vistas en una consulta, vea Uso de Explorador de recursos de AWS para buscar recursos.

Cada vista tiene un nombre de recurso de Amazon (ARN) al que puede hacer referencia en las políticas de permisos para conceder acceso a vistas individuales. También puede pasar el ARN de una vista como parámetro a cualquier API u operación de la AWS CLI que interactúe con una vista. El ARN de una vista es similar al siguiente ejemplo:

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View-
Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> Cada ARN de vista incluye un UUID generado por AWS al final. Esto ayuda a garantizar que los usuarios que puedan haber tenido acceso a vistas con un nombre específico que se haya eliminado, no puedan acceder automáticamente a una vista nueva creada con el mismo nombre.

Resource

Un recurso es una entidad en AWS con la que puede trabajar. Los recursos se crean mediante los Servicios de AWS a medida que utiliza las características del servicio. Entre los ejemplos se incluyen una instancia Amazon EC2, un bucket de Amazon S3 o una pila de AWS CloudFormation. Algunos tipos de recursos pueden contener datos de clientes. Todos los tipos de recursos tienen atributos o metadatos para describir el recurso, incluidos un nombre, una descripción y el nombre de recurso de Amazon (ARN) que utiliza para hacer referencia única a un recurso. La mayoría de los tipos de recursos también admiten etiquetas. Las etiquetas son metadatos personalizados que puede adjuntar a sus recursos con diversos fines, como la asignación de costos en la facturación, la autorización de seguridad mediante el control de acceso basado en atributos o para satisfacer otras necesidades de categorización.

El objetivo principal de Resource Explorer es ayudarlo a encontrar los recursos que existen en su Cuenta de AWS. Resource Explorer utiliza una variedad de técnicas para descubrir todos sus recursos y colocar la información sobre ellos en un índice. A continuación, puede consultar el índice a través de cualquier vista que el administrador ponga a su disposición.

Important

Resource Explorer excluye intencionadamente a aquellos tipos de recursos cuya inclusión podría exponer los datos de los clientes. Los siguientes tipos de recursos no están indexados por Resource Explorer y, por lo tanto, nunca aparecen en los resultados de búsqueda.

- Objetos de Amazon S3 contenidos en un bucket
- Artículos de la tabla Amazon DynamoDB
- Valores de atributo de DynamoDB

Búsqueda unificada en la AWS Management Console

En la parte superior de la AWS Management Console, en cada Servicio de AWS, hay una barra de búsqueda que puede utilizar para buscar una variedad de cosas relacionadas con AWS. Puede buscar servicios y características, y obtener enlaces directamente a la página correspondiente en la consola de ese servicio. También puede buscar documentación y artículos de blog relacionados con el término de búsqueda.

Tras activar Resource Explorer y crear un índice agregador y una vista predeterminada, la búsqueda unificada también puede incluir los recursos de su cuenta en los resultados de la búsqueda. La búsqueda unificada utiliza automáticamente la vista predeterminada en la Región de AWS que contiene el índice agregador de la cuenta. Esto le permite buscar un recurso desde cualquier página de la AWS Management Console, sin tener que abrir primero Resource Explorer. Si no promociona un índice local como índice agregador de la cuenta o si no crea una vista predeterminada en la región del índice de agregación, la búsqueda unificada no incluye los recursos en los resultados de búsqueda. Además, cualquier entidad principal que realice una búsqueda debe tener permiso para usar la vista predeterminada de la región que contiene el índice agregador; de lo contrario, la búsqueda unificada no incluye los recursos en sus resultados de búsqueda.

Important

La búsqueda unificada inserta automáticamente un operador de caracteres comodín (*) al final de la primera palabra clave de la cadena. Esto significa que los resultados de la búsqueda unificada incluyen recursos que coinciden con cualquier cadena que comience por la palabra clave especificada.
La búsqueda realizada mediante el cuadro de texto Consulta de la página de Búsqueda de recursos de la consola de Resource Explorer no añade automáticamente un carácter

comodín. Puede insertar un * manualmente después de cualquier término de la cadena de búsqueda.

Para obtener más información sobre la búsqueda unificada y su integración con Resource Explorer, consulte Uso de la búsqueda unificada en la AWS Management Console.

Búsqueda multicuenta

Con la búsqueda multicuenta, puede buscar y descubrir recursos en AWS Organizations y en las Regiones de AWS con una sola búsqueda por palabra clave.

Para obtener más información sobre la búsqueda multicuenta y cómo habilitarla en Resource Explorer, consulte Activación de la búsqueda multicuenta.

Requisitos previos para usar Resource Explorer

Antes de usarlo Explorador de recursos de AWS por primera vez, complete las siguientes tareas según sea necesario.

Tareas

- Inscríbase en una Cuenta de AWS
- Creación de un usuario con acceso administrativo

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como

práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .
2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Instalación y configuración de Resource Explorer

Antes de poder realizar la instalación y la configuración Explorador de recursos de AWS, asegúrese primero de cumplir con los requisitos previos. Después, inicie sesión como un rol o usuario de IAM que tenga los permisos necesarios para realizar las operaciones del explorador de recursos mediante el siguiente procedimiento.

Puede utilizar este procedimiento de instalación y configuración para configurar el Explorador de recursos en las cuentas existentes y en cualquier cuenta nueva que se añada a su organización.

Existen dos formas de configurar Resource Explorer:

- Configuración Rápida
- Configuración avanzada

Important

Si decide configurar el Explorador de recursos con cualquier opción que diga Regiones de AWS «todas», solo se activarán las Regiones de AWS que existan y que estén habilitadas en el Cuenta de AWS momento de realizar el procedimiento. El Explorador de recursos no se activa automáticamente en ninguno de los Regiones de AWS que se AWS agreguen en el futuro. Cuando AWS introduzcas una nueva región, puedes activar el Explorador de recursos en la región manualmente cuando aparezca en la página de configuración de la consola del Explorador de recursos, o bien activando la CreateIndexoperación.

Note

Al configurar Resource Explorer también se puede activar la posibilidad de buscar recursos mediante el uso de la barra de búsqueda unificada de la AWS Management Console. Para que los usuarios vean los recursos en los resultados de búsqueda unificados, debe configurar Resource Explorer con un índice de agregación entre regiones y una vista predeterminada. Para obtener más detalles, consulte los siguientes procedimientos. También debe asegurarse de que los usuarios que realizan la búsqueda tengan permiso para usar la vista predeterminada en la Región de AWS que se incluye el índice del agregador. Para obtener más información, consulte Uso de la búsqueda unificada en la AWS Management Console.

Configuración de Resource Explorer mediante Configuración Rápida

Si elige la opción Configuración Rápida, Resource Explorer realiza lo siguiente:

- Crea un índice en cada uno Región de AWS de tus. Cuenta de AWS
- Actualiza el índice de la región que especifique como índice agregador de la cuenta.
- Crea una vista predeterminada en la región del índice de agregador. Esta vista no posee filtros, por lo que devuelve todos los recursos que se encuentran en el índice.

Permisos mínimos

Para realizar los siguientes pasos, debe tener los siguientes permisos:

- Acción: `resource-explorer-2:*` — Recurso: ningún recurso específico (*)
- Acción: `iam:CreateServiceLinkedRole` — Recurso: ningún recurso específico (*)

AWS Management Console

Configuración de Resource Explorer mediante Configuración Rápida

1. Abra la consola de Explorador de recursos de AWS en https://console.aws.amazon.com/resource-explorer.
2. Seleccione Activar Resource Explorer.
3. En la página Activar Resource Explorer, elija Configuración Rápida.
4. Elige cuál Región de AWS quieres que contenga el índice del agregador. Debe seleccionar la región adecuada para la ubicación geográfica de los usuarios.
5. En la parte inferior de la página, elija Activar Resource Explorer.
6. En la página Progreso, puede supervisar cada Región de AWS a medida que Resource Explorer crea su índice. La página muestra el estado de la creación del índice agregador y de la creación de la vista predeterminada.

Una vez que se hayan completado todos los pasos correctamente, usted y sus usuarios podrán ir a la página de búsqueda de recursos y comenzar a buscar recursos.

> **Note**
>
> Los recursos etiquetados locales en el índice aparecen en los resultados de búsqueda luego de unos minutos. Los recursos sin etiquetar suelen demorar menos de dos horas en aparecer, pero cuando hay una gran demanda, ese tiempo puede extenderse. También puede tardar hasta una hora en completarse la réplica inicial en un nuevo índice agregador desde todos los índices locales existentes.

Próximos pasos: antes de que sus usuarios puedan buscar con la vista predeterminada que acaba de crear, debe concederles permisos para buscar en ella. Para obtener más información, consulte Otorgar acceso a las vistas de Resource Explorer para la búsqueda.

AWS CLI

Configurar el Explorador de recursos en su Cuenta de AWS ordenador mediante el uso de la misma AWS CLI equivale, por definición, a la opción de configuración avanzada. Esto se debe a que las operaciones de la CLI de Resource Explorer, en contraposición a la consola de Resource Explorer, no realizan ninguno de los pasos automáticamente. Consulte la AWS CLI pestaña de la Configuración de Resource Explorer mediante la configuración avanzada para ver qué comandos equivalen a usar la consola.

Configuración de Resource Explorer mediante la configuración avanzada

Si elige la opción Configuración avanzada, puede hacer lo siguiente:

- Seleccione la opción Regiones de AWS en la que desea activar el Explorador de recursos.
- Elegir si desea configurar una región con un índice agregador. Si lo hace, especifique el lugar en el que Región de AWS desea colocarlo. Este índice le permite crear vistas que pueden incluir recursos de todas las regiones de la cuenta. Para obtener más información, consulte Activar la búsqueda entre regiones mediante la creación de un índice agregador.
- Elegir si desea crear una vista predeterminada. Esta vista permite buscar automáticamente cualquier AWS recurso en las regiones en las que se active el Explorador de recursos. Debe asegurarse de que todas las entidades principales que necesiten usar la vista predeterminada para buscar en Resource Explorer tengan permisos para acceder a la vista. Para obtener más información, consulte Otorgar acceso a las vistas de Resource Explorer para la búsqueda.

> **Note**
>
> Puede configurar Resource Explorer para incluir sus recursos en los resultados de búsqueda proporcionados por la característica de búsqueda unificada de la AWS Management Console. Para activar esta característica, debe configurar Resource Explorer con un índice agregador y una vista predeterminada con la que puedan buscar todos los roles y usuarios. La opción Configuración Rápida crea tanto el índice agregador como la vista predeterminada, y es la forma recomendada para activar Resource Explorer.

Permisos mínimos

Para realizar los siguientes pasos, debe tener los siguientes permisos:

- Acción: `resource-explorer-2:*` — Recurso: ningún recurso específico (*)
- Acción: `iam:CreateServiceLinkedRole` — Recurso: ningún recurso específico (*)

AWS Management Console

Activación de Resource Explorer mediante la configuración avanzada

1. Abra la consola de Explorador de recursos de AWS en https://console.aws.amazon.com/resource-explorer.
2. Elija Activar Resource Explorer.
3. En la página Activar Resource Explorer, elija Configuración avanzada.
4. En el Regiones de AWScuadro, en Regiones, elige si quieres activar el Explorador de recursos en todas las Regiones de AWS regiones o solo en determinadas regiones.

   Si elige Activar Resource Explorer solo en las Regiones de AWS especificadas en esta cuenta, seleccione cada región cuyos recursos desee incluir en los resultados de la búsqueda.
5. En el índice agregador, elija si desea crear un índice agregador. Si decide crear un índice agregador, todas las demás Regiones de AWS replicarán sus índices en esta región. Esto permite a los usuarios buscar recursos en todas las regiones seleccionadas de. Cuenta de AWS Elija la Región de AWS que contenga el índice del agregador. Recomendamos especificar la región en la que los usuarios pasan la mayor parte del tiempo o, al menos, en la que espera que realicen la mayoría de sus búsquedas de recursos.
6. En el cuadro Vista predeterminada, debajo de Creación de vistas, elija si desea crear una vista predeterminada. Esta opción solo está disponible si elige crear un índice agregador. Si decide crear una vista predeterminada, el Explorador de recursos coloca esta vista en el mismo lugar que el Región de AWS índice del agregador. Esto permite que la vista predeterminada incluya los resultados de todas las páginas Regiones de AWS en las que haya registrado Resource Explorer. Cuando un usuario realiza una búsqueda en una región con una vista predeterminada y no especifica una vista de forma explícita, la búsqueda utiliza la vista predeterminada de esa región.

> **Note**
>
> Antes de que sus usuarios puedan buscar con una vista, debe concederles permisos para usarla. Para obtener más información, consulte Otorgar acceso a las vistas de Resource Explorer para la búsqueda.

7. Elija Activar Resource Explorer.

> **Note**
>
> Los recursos etiquetados locales en el índice aparecen en los resultados de búsqueda luego de unos minutos. Los recursos sin etiquetar suelen demorar menos de dos horas en aparecer, pero cuando hay una gran demanda, ese tiempo puede extenderse. También puede tardar hasta una hora en completarse la réplica inicial en un nuevo índice agregador desde todos los índices locales existentes.

AWS CLI

Configuración de Resource Explorer mediante la configuración avanzada

La consola de Resource Explorer realiza muchas llamadas a operaciones API en su nombre en función de las elecciones que realice. Los siguientes AWS CLI comandos de ejemplo ilustran cómo realizar los mismos procedimientos básicos fuera de la consola mediante el AWS CLI.

Example Paso 1: activar Resource Explorer mediante la creación de índices en las Regiones de AWS deseadas

Ejecute el siguiente comando en cada una de las Región de AWS aplicaciones en las que desee activar el Explorador de recursos. El siguiente comando de ejemplo activa Resource Explorer en la Región de AWS predeterminada de la AWS CLI.

```
$ aws resource-explorer-2 create-index
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-27T16:17:12.130000+00:00",
    "State": "CREATING"
}
```

Example Paso 2: Actualice el índice en uno Región de AWS para que sea el índice agregador de la cuenta

Ejecute el siguiente comando Región de AWS en el que desee que Resource Explorer actualice el índice local al índice agregador de la cuenta. El siguiente comando de ejemplo actualiza el índice agregador en el Este de EE. UU. (Norte de Virginia) (`us-east-1`).

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt": "2022-07-27T16:29:49.231000+00:00",
    "State": "UPDATING",
    "Type": "AGGREGATOR"
}
```

Example Paso 3: Cree una vista en la Región de AWS que contenga el índice del agregador

Ejecute el siguiente comando Región de AWS en el que creó el índice del agregador. El siguiente comando de ejemplo crea una vista idéntica a la creada por el proceso de configuración de la consola de Resource Explorer. Esta nueva vista incluye etiquetas adjuntas al recurso como parte de la información indexada y permite buscar recursos por clave o valor de etiqueta.

```
$ aws resource-explorer-2 create-view \
    --view-name My-New-View \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-07-27T16:34:14.960000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
```

```
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222"
    }
}
```

Example Paso 4: Establezca su nueva vista como la predeterminada para su Región de AWS

En el siguiente ejemplo, se establece la vista que ha creado en el paso anterior como predeterminada para la región. Debe ejecutar el siguiente comando en la misma ubicación Región de AWS en la que creó la vista predeterminada.

```
$ aws resource-explorer-2 associate-default-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

Antes de que los usuarios puedan buscar con una vista, debe concederles permisos para utilizar esa vista. Para obtener más información, consulte Otorgar acceso a las vistas de Resource Explorer para la búsqueda.

Tras ejecutar esos comandos, se ejecutará Resource Explorer en las regiones especificadas de su Cuenta de AWS. Resource Explorer crea y mantiene un índice en cada región con detalles de los recursos que se encuentran allí. Resource Explorer replica cada uno de los índices de región individuales en el índice agregador de la región especificada. Esa región también contiene una vista que permite a cualquier usuario o rol de IAM en la cuenta buscar recursos en todas las regiones indexadas.

> **Note**
>
> Los recursos etiquetados locales en el índice aparecen en los resultados de búsqueda en unos minutos. Los recursos sin etiquetar suelen demorar menos de dos horas en aparecer, pero cuando hay una gran demanda, ese tiempo puede extenderse. También puede tardar hasta una hora en completarse la réplica inicial en un nuevo índice agregador desde todos los índices locales existentes.

Cómo administrar Resource Explorer para facilitar la búsqueda de recursos

Después de activar Explorador de recursos de AWS inicialmente en al menos una Región de AWS en su Cuenta de AWS, hay tareas administrativas que puede que tenga que realizar de vez en cuando. En esta sección, se describen las tareas de mantenimiento y configuración que lo ayudarán a hacer que Resource Explorer funcione de la manera que desee a medida que evolucione el uso de su Cuenta de AWS y de los recursos.

Temas

Comprobar cuáles Regiones de AWS tienen activado el explorador de recursos

Puedes averiguar qué Regiones de AWS tienen activado el Explorador de recursos de AWS al comprobar qué regiones contienen un índice para el explorador de recursos. Para ver qué regiones tienen un índice, utilice los procedimientos de esta página.

> **Important**
>
> Los usuarios solo pueden buscar recursos en las regiones que tengan activado el explorador de recursos. También puede crear un índice agregador en una región para facilitar

la búsqueda de recursos en todas sus regiones. El explorador de recursos replica la información sobre los recursos en la región con el índice agregador de todas las demás regiones que contienen un índice del Explorador de recursos. Los usuarios no pueden usar el explorador de recursos para descubrir recursos en regiones que no tienen un índice.

Comprobar el estado del explorador de recursos en una región

Para comprobar qué regiones tienen índices para el explorador de recursos AWS Management Console, utilice los comandos del AWS Command Line Interface (AWS CLI) o utilice las operaciones de la API en un AWS SDK.

AWS Management Console

Para comprobar qué regiones tienen índices para el explorador de recursos

1. Abra la página de Configuraciones en la consola del explorador de recursos.
2. La lista de la sección Índices incluye solo las regiones que contienen un índice del explorador de recursos. El valor de la columna Tipo indica si el índice es un índice Local para su región o el índice de Agregación para la Cuenta de AWS.
3. Para ver qué regiones no contienen un explorador de recursos, elija Crear índices. Si una región no está presente, la región no contiene un explorador de recursos.

AWS CLI

Para comprobar qué regiones tienen índices para un explorador de recursos

Ejecute el siguiente comando para ver qué Regiones de AWS tienen índices para el explorador de recursos.

```
$ aws resource-explorer-2 list-indexes
{
    "Indexes": [
        {
            "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Region": "us-east-1",
            "Type": "AGGREGATOR"
        },
```

```
        {
            "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
            "Region":"us-west-2",
            "Type":"LOCAL"
        }
    ]
}
```

Activación de la búsqueda multicuenta

Con la búsqueda multicuenta, puedes buscar recursos en todas las cuentas con índices activos en tu unidad organizativa (OU) AWS Organizations o en tu unidad organizativa (OU).

Temas

Requisitos previos

Para activar la búsqueda de varias cuentas en tu organización, sigue estos pasos:

- En el caso de las regiones con suscripción voluntaria, compruebe que su cuenta de administración también esté habilitada y active la búsqueda de varias cuentas.
- Crear un usuario administrativo.
- Crear un rol vinculado a un servicio en la cuenta de administrador con `aws iam create-service-linked-role --aws-service-name resource-explorer-2.amazonaws.com`.
- Habilite el acceso confiable en. AWS Organizations Esto permite la integración total con Resource Explorer para enumerar los recursos de todas las cuentas de su organización.
- Asigne un administrador delegado (recomendado). Para obtener más información, consulte Administrador delegado para ver AWS los servicios que funcionan con Organizations en la Guía del AWS Organizations usuario.
  - Resource Explorer solo admite un administrador delegado que realice acciones similares a las de la cuenta de administración.

- Al eliminar o cambiar el administrador delegado de su organización, se eliminarán todas las vistas multicuenta creadas en su cuenta.

Cómo habilitar la búsqueda multicuenta

Para buscar y descubrir recursos en las cuentas de su organización, debe llevar a cabo los siguientes pasos:

1. Explorador de recursos de AWS Actívalos en una o más cuentas de tu. AWS Organizations
2. Registrar una región para incluir el índice agregador.
3. Elegir una región en la que desee crear un índice agregador. Esta región debe ser coherente en todas sus partes AWS Organizations.
4. Crea una vista del explorador de recursos que se adapte a tu unidad organizativa AWS Organizations o a tu organización. Cree esta vista en la región de agregador del paso anterior.
5. Comparta la vista con las cuentas de toda la organización.

Configuración Rápida de multicuenta

Active Resource Explorer en varias cuentas de su organización con Configuración Rápida.

> **Note**
>
> Este proceso no despliega ningún recurso en la cuenta de administración. Si utiliza la cuenta de administración y desea incluir índices en la cuenta, debe añadirlos manualmente con el flujo de incorporación de Resource Explorer.

1. Vaya a Configuración Rápida de Resource Explorer en la consola del Administrador del sistema.
2. Elija su región de índice agregador. Esto le permite buscar recursos ubicados en todas las regiones de las cuentas objetivo seleccionadas. Si alguna de las cuentas objetivo seleccionadas ya tiene un índice agregador configurado en otra región, el índice agregador existente se sustituirá automáticamente por esta nueva región.
3. Elija los Objetivos de su cuenta. Puede habilitar Resource Explorer para toda la organización o para las unidades organizativas (OU) especificadas.

> **Note**
>
> Puedes desplegar hasta un máximo de 50 000 AWS CloudFormation pilas a la vez. Si tiene una organización grande que abarca varias regiones, debe realizar la implementación a nivel de unidad organizativa en lotes más pequeños.

4. Lea el resumen de los agradecimientos antes de elegir Crear.

Activar el explorador de recursos en una Región de AWS para indexar sus recursos

Al activar su servicio Explorador de recursos de AWS inicialmente en su Cuenta de AWS, habrá creado índices para el servicio en una Regiones de AWS o más. Si utilizó la opción Quick setup, el explorador de recursos creará índices automáticamente en todas las Regiones de AWS que estén activadas en su Cuenta de AWS. El servicio explorador de recursos también promovió el índice de la región especificada como índice agregador de la cuenta. Si utilizó la opción Configuración avanzada, especificó las regiones en las que crearía los índices.

Para activar el explorador de recursos en otras regiones, utilice los procedimientos de este tema.

Al activar el explorador de recursos en una Región de AWS, el servicio realiza las siguientes acciones:

- Al iniciar el explorador de recursos en la primera región en una Cuenta de AWS, el explorador de recursos crea un rol vinculado al servicio en la cuenta denominada `AWSServiceRoleForResourceExplorer`. Esta función otorga permisos para que el explorador de recursos descubra e indexe los recursos de su cuenta mediante servicios como AWS CloudTrail y el servicio de etiquetado. La creación del rol vinculado al servicio solo se produce cuando se registra la primera Región de AWS en la cuenta. El explorador de recursos utiliza el mismo rol vinculado a servicios para todas las regiones adicionales que agregue más adelante.
- El explorador de recursos crea un índice en la región especificada para almacenar los detalles sobre los recursos de esa región.
- El explorador de recursos comienza a descubrir los recursos de la región especificada y agrega la información que encuentra sobre ellos al índice de esa región.

- Si su cuenta ya contiene un índice agregador en otra región, el explorador de recursos comienza a replicar la información del índice de la nueva región en el índice agregador para permitir la búsqueda entre regiones.

Una vez completados estos pasos, los usuarios podrán descubrir la información sobre sus recursos. Pueden buscar mediante una de las vistas definidas en la misma región o en la región que contiene el índice agregador.

Crear un índice del explorador de recursos en una región

Puede crear un índice del explorador de recursos en una Región de AWS adicional mediante el AWS Management Console, a través de los comandos del AWS Command Line Interface (AWS CLI) o de las operaciones de la API en un AWS SDK. Solo puede crear un índice en una región.

Permisos mínimos

Para realizar los siguientes pasos, debe tener los siguientes permisos:

- Acción: `resource-explorer-2:*` — Recurso: ningún recurso específico (`*`)
- Acción: `iam:CreateServiceLinkedRole` — Recurso: ningún recurso específico (`*`)

AWS Management Console

Para crear un índice del explorador de recursos en una Región de AWS

1. En la página de Configuración del explorador de recursos.
2. Seleccione Crear índices en la sección Índices.
3. En la página Crear índices, active las casillas de verificación situadas junto a la Regiones de AWS en la que desee crear un índice para facilitar la búsqueda de los recursos de esa región. Las casillas de verificación no disponibles indican las regiones que ya contienen un índice del explorador de recursos.
4. (Opcional) En la sección Etiquetas, puede especificar las claves de etiqueta y valor de la etiqueta para el índice.
5. Elija Crear índices.

   El explorador de recursos muestra un cartel verde en la parte superior de la página para indicar que se ha realizado correctamente, o uno rojo si hubo un error al crear un índice en una o más de las regiones seleccionadas.

> **Note**
>
> Los recursos etiquetados locales en el índice aparecen en los resultados de búsqueda en unos minutos. Los recursos sin etiquetar suelen demorar menos de dos horas en aparecer, pero cuando hay una gran demanda, ese tiempo puede extenderse. También puede tardar hasta una hora en completarse la replicación inicial en un nuevo índice agregador desde todos los índices locales existentes.

Siguiente paso: si ya ha creado un índice agregador, las nuevas regiones comenzarán automáticamente a replicar la información de su índice en el índice agregador. Si ahí es donde los usuarios realizan todas sus búsquedas, los recursos de la nueva región aparecen en los resultados de la búsqueda y listo.

Sin embargo, si quiere que los usuarios solo puedan buscar recursos en la región recién indexada, también debe crear una vista para los usuarios de esa región y concederles permisos para acceder a ella. Para obtener instrucciones acerca de cómo crear una vista, consulte Cómo administrar las vistas de Resource Explorer para proporcionar acceso a la búsqueda.

AWS CLI

Para crear un índice del explorador de recursos en un Región de AWS

Ejecute el siguiente comando para cada Región de AWS en las que desee crear un índice que permita buscar los recursos de esa región. El comando de ejemplo siguiente registra el explorador de recursos en el Este de EE. UU. (Norte de Virginia) (`us-east-1`).

```
$ aws resource-explorer-2 create-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-11-01T20:00:59.149Z",
    "State": "CREATING"
}
```

Repita este comando para cada región en la que desee activar el explorador de recursos y sustituya el código de región adecuado para el parámetro `--region`.

Como el explorador de recursos realiza parte de la creación de índices como tareas asincrónicas en segundo plano, la respuesta puede ser `CREATING`, lo que indica que los procesos en segundo plano aún no se han completado.

> **Note**
>
> Los recursos etiquetados locales en el índice aparecen en los resultados de búsqueda en unos minutos. Los recursos sin etiquetar suelen demorar menos de dos horas en aparecer, pero cuando hay una gran demanda, ese tiempo puede extenderse. También puede demorar hasta una hora en completarse la replicación inicial en un nuevo índice agregador desde todos los índices locales existentes.

Puede comprobar si se ha completado definitivamente ejecutando el siguiente comando y comprobando el estado `ACTIVE`.

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

Siguiente paso: si ya ha creado un índice agregador, las nuevas regiones comenzarán automáticamente a replicar la información de su índice en el índice agregador. Si ahí es donde los usuarios realizan todas sus búsquedas, los recursos de la nueva región aparecen en los resultados de la búsqueda y listo.

Sin embargo, si quiere que los usuarios solo puedan buscar recursos en la región recién indexada, también debe crear una vista para los usuarios de esa región y concederles permisos para acceder a ella. Para obtener instrucciones acerca de cómo crear una vista, consulte Cómo administrar las vistas de Resource Explorer para proporcionar acceso a la búsqueda.

Consideraciones para las regiones que AWS optan por participar

Las regiones registradas tienen requisitos de seguridad más estrictos que las regiones comerciales en lo que respecta al intercambio de datos de IAM a través de cuentas en las regiones registradas. Todos los datos gestionados a través del servicio de IAM se consideran datos de identidad.

Puede activar las regiones registradas mediante la consola de Explorador de recursos de AWS. Consulte Activar el explorador de recursos en una página Región de AWS para indexar sus recursos para obtener más información.

Comportamientos de desactivación

Tenga en cuenta los siguientes comportamientos antes de desactivar una región registrada:

> **Important**
>
> Antes de desactivar una región con un índice agregador, le sugerimos que elimine el índice de agregador o lo baje a un índice local. Resource Explorer admite un índice agregador en todas las regiones de la partición.

- El índice no se elimina, solo se inhabilita. Si decide volver a registrarse más tarde, la configuración se revertirá.
- IAM desactiva el acceso de IAM a los recursos de la región.
- Resource Explorer desactiva el índice de la región cancelada y deja de incorporar datos. La API de `ListIndexes` ya no mostrará el índice de la región.
- Si el índice de agregador se encuentra en una región diferente, Resource Explorer detiene la replicación de los datos de la región cancelada y limpia los datos en un plazo de 24 horas.
- Si cancela la región de su índice de agregador, tendrá que volver a registrarse para eliminar o bajar el índice.
- Si vuelve a registrarse en la región, Resource Explorer volverá a habilitar el índice y empezará a incorporar datos.
- Cualquier cambio en el estado de una región registrada tarda unas 24 horas en entrar en vigencia.

Activación de la búsqueda entre regiones mediante la creación de un índice agregador

Temas

Acerca del índice agregador

Explorador de recursos de AWS almacena la información que recopila sobre los recursos de una Región de AWS a un índice local que Resource Explorer crea y mantiene en esa región. Por ejemplo, suponga que tiene una instancia de Amazon EC2 en la región oeste de EE. UU. (Oregón). Resource Explorer almacena los detalles de ese recurso en el índice local de la región oeste de EE. UU. (Oregón).

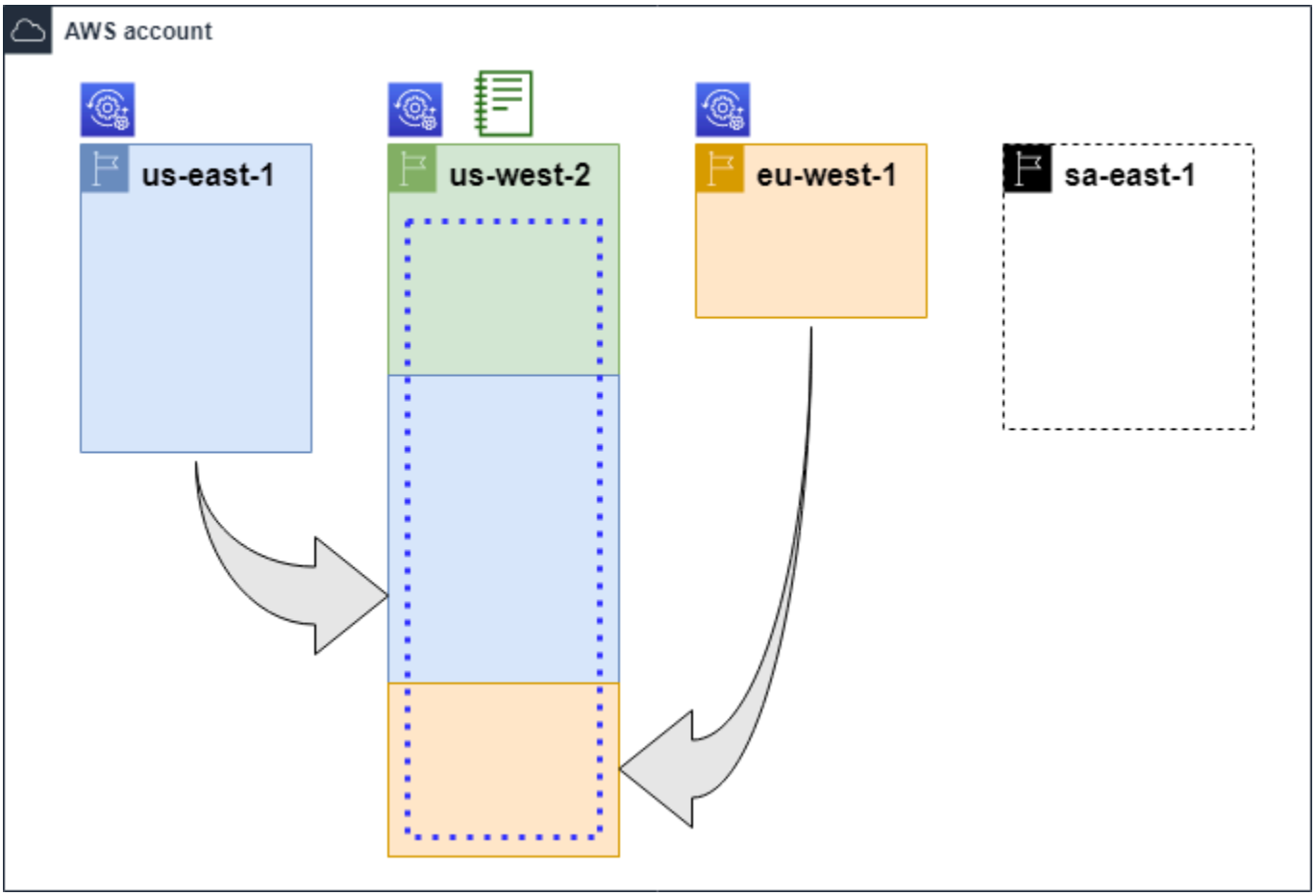
Para facilitar la búsqueda de recursos en todas las Regiones de AWS de su cuenta, puede convertir el índice local de una región en el índice agregador de su cuenta.

El índice agregador contiene una copia replicada del índice local en todas las demás regiones en las que haya activado Resource Explorer. Esto le permite crear vistas en la región que contiene el índice agregador, cuyos resultados pueden incluir recursos de todas las Regiones de AWS de la cuenta.

El siguiente diagrama muestra un ejemplo de cómo funciona el índice agregador. En esta Cuenta de AWS de ejemplo, el administrador hace lo siguiente:

- Activa Resource Explorer en tres Regiones de AWS (`us-east-1`, `us-west-2` y `eu-west-1`) mediante la creación de índices en esas regiones. Cada región contiene su propio índice local.
- Elija no crear un índice en la región `sa-east-1`. Los usuarios no pueden realizar búsquedas en `sa-east-1` y no aparecen recursos de esa región en los resultados de búsqueda.
- Cree el índice agregador de la cuenta en la región `us-west-2`. Esto hace que Resource Explorer replique la información de los índices locales de todas las demás regiones en las que Resource Explorer está activado en el índice agregador. Esto permite que las búsquedas que se realicen en `us-west-2` incluyan recursos de las tres regiones en las que Resource Explorer está activado.

Esta configuración significa que un usuario solo puede realizar búsquedas entre regiones `us-west-2`, que contienen el índice agregador. Solo las vistas de esa región pueden arrojar resultados de todas las regiones de la cuenta.



Leyenda	
	Resource Explorer está activado en esta Región de AWS, y sus recursos se catalogan en un índice de esa región. El índice de esta región también se replica (indicado con las flechas) en la Región de AWS que contiene el índice agregador.
	Esta Región de AWS contiene el índice agregador. Resource Explorer replica la información de recursos recopilada en todas las demás Regiones de AWS en esta región.
	La vista predeterminada creada por Configuración Rápida incluye todos los recursos en todas las Regiones de AWS.

Promover un índice local para que sea el índice agregador de la cuenta

Tiene la opción de crear un índice agregador en una Región de AWS cuando configuró Explorador de recursos de AWS por primera vez. Para obtener más información, consulte Instalación y configuración de Resource Explorer. Este procedimiento consiste en promover uno de los índices locales como índice agregador de la cuenta si no lo hizo en la configuración inicial.

Important

- Solo se puede tener un índice agregador en una Cuenta de AWS. Si la cuenta ya tiene un índice agregador, primero debes degradarlo a un índice local o eliminarlo.
- Tras eliminar o cambiar la región que contiene el índice agregador, debe esperar 24 horas antes de poder promocionar otro índice como índice agregador.

AWS Management Console

Promover un índice local para que sea el índice agregador de la cuenta

1. Abra la página de Configuraciones en la consola del Explorador de recursos.
2. En la sección Índices, selecciona la casilla de verificación situada junto al índice que deseas promocionar y, a continuación, selecciona Cambiar tipo de índice.
3. En el cuadro de diálogo Cambiar el tipo de índice para < Nombre de región >, selecciona el índice agregador y, a continuación, selecciona Guardar cambios.

AWS CLI

Promover un índice local para que sea el índice agregador de la cuenta

El siguiente comando de ejemplo actualiza el índice del Región de AWS especificado de un tipo `LOCAL` al tipo `AGGREGATOR`. Debe llamar a la operación desde la Región de AWS que desee que contenga el índice agregador.

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR \
```

```
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"AGGREGATOR"
}
```

La operación funciona de forma asincrónica y comienza con el `State` configurado como `UPDATING`. Para comprobar si la operación se ha completado, puede ejecutar el siguiente comando y buscar el valor `ACTIVE` en el campo de respuesta `State`. Debe ejecutar este comando en la región que contiene el índice que desea comprobar.

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "AGGREGATOR"
}
```

Degradar el índice agregador a un índice local

Puede degradar un índice agregador a un índice local, por ejemplo, cuando desea mover el índice agregador a otra Región de AWS diferente.

Al degradar un índice agregador a un índice local, Resource Explorer deja de replicar los índices de otras Regiones de AWS. También inicia una tarea asincrónica en segundo plano para eliminar cualquier información replicada de otras regiones. Hasta que se complete esa tarea asincrónica, algunos resultados entre regiones pueden seguir apareciendo en los resultados de búsqueda.

Notas

- Tras degradar un índice agregador, debe esperar 24 horas antes de poder promocionar el mismo índice o el índice de una región diferente para que se convierta en el nuevo índice agregador de la cuenta.
- Tras degradar un índice agregador, los procesos en segundo plano pueden demorar hasta 36 horas en completarse y toda la información sobre los recursos de otras regiones en desaparecer de los resultados de las búsquedas realizadas en esta región.
- Si degrada una cuenta de miembro en una visión global de la organización, es posible que se elimine al miembro de la búsqueda de varias cuentas.

Puede comprobar el estado de la tarea en segundo plano consultando la lista de índices en la página de configuración o mediante la GetIndexoperación. Cuando se completan las tareas asincrónicas, el `Status` campo del índice cambia de `UPDATING` a `ACTIVE`. En ese momento, solo los resultados de la región local aparecen en los resultados de la consulta.

AWS Management Console

Cómo degradar el índice agregador a un índice local

1. Abra la página de Configuración de Resource Explorer.
2. En la sección Índices, seleccione la casilla de verificación situada junto al índice que deseas promocionar y, a continuación, elija Cambiar tipo de índice.
3. En el cuadro de diálogo Cambiar el tipo de índice para <Nombre de región>, elija el índice agregador y, a continuación, elija Guardar cambios.

AWS CLI

Cómo degradar el índice agregador a un índice local

En el siguiente ejemplo, se degrada el índice agregador especificado a un índice local. Debe llamar a la operación desde la Región de AWS que desee que contenga el índice agregador.

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
```

```
    --type LOCAL \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"LOCAL"
}
```

La operación funciona de forma asincrónica y comienza con el `State` configurado como `UPDATING`. Para comprobar si la operación se ha completado, puede ejecutar el siguiente comando y buscar el valor `ACTIVE` en el campo de respuesta `State`. Debe ejecutar este comando en la región que contiene el índice que desea comprobar.

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

Búsqueda unificada de respaldo en AWS Management Console

AWS Management Console tiene una barra de búsqueda en la parte superior de cada página de la consola. Esto proporciona una experiencia de búsqueda unificada en todos los Servicios de AWS. Los resultados de búsqueda unificados pueden incluir:

- Servicio de AWS y cuentan con páginas de consola.
- Páginas de documentación AWS.
- Artículos del blog y de la base de conocimientos AWS

- Recursos en sus cuentas: si sigue los pasos que se indican a continuación.

Para ver los recursos de su cuenta en los resultados de búsqueda unificados, debe realizar los siguientes pasos. Puede hacerlo durante la configuración inicial de Explorador de recursos de AWS. Todo ocurre automáticamente si utiliza la opción Quick Setup.

- Debe crear un índice agregador en una Región de AWS para la Cuenta de AWS.
- Debe crear una vista predeterminada en la Región de AWS que contenga el índice agregador.
- Debe conceder permiso a la entidad principal que necesiten buscar recursos en la barra de búsqueda unificada para que realicen búsquedas con esa vista predeterminada.

La búsqueda unificada siempre utiliza la vista predeterminada de la Región de AWS que contiene el índice agregador para realizar todas las búsquedas.

Efecto de las acciones de la cuenta en la búsqueda multicuenta de Resource Explorer

> **Note**
>
> Se demora hasta 24 horas en eliminar cuentas y recursos de los resultados de búsqueda multicuenta.

Las acciones de la cuenta tienen los siguientes efectos en la búsqueda de multicuentas de Explorador de recursos de AWS.

Resource Explorer desactivado

Cuando se deshabilita Resource Explorer de una cuenta, se deshabilita solo para esa cuenta en la Región de AWS que esté seleccionada cuando lo deshabilite.

Debe deshabilitar Resource Explorer por separado en cada región donde se ha habilitarlo.

Transcurridas 24 horas, los recursos de esta cuenta no aparecerán en los resultados de búsqueda.

Los demás datos y configuraciones de Resource Explorer no se eliminan.

Cómo eliminar una cuenta miembro de una organización

Cuando se elimina una cuenta miembro de una organización, la cuenta de administrador de Resource Explorer pierde los permisos para ver los recursos de esa cuenta.

Si la cuenta eliminada es una cuenta de administrador o de administrador delegado, también se eliminarán todas las vistas multicuenta creadas anteriormente por estas cuentas.

Resource Explorer sigue ejecutándose en ambas cuentas.

Los resultados de la búsqueda de recursos ya no incluyen los recursos de esta cuenta.

Cuenta suspendida

Cuando se suspende una cuenta en AWS, pierde los permisos para ver los recursos en Resource Explorer. La cuenta de administrador de una cuenta suspendida puede ver los recursos existentes.

En el caso de una cuenta de organización, el estado de la cuenta de miembro también puede cambiar a Cuenta suspendida. Esto sucede si la cuenta se suspende al mismo tiempo que la cuenta del administrador intenta habilitarla. La cuenta de administrador de una Cuenta suspendida no puede ver los recursos de esa cuenta.

De lo contrario, el estado suspendido no afectará al estado de la cuenta miembro.

Transcurridos 90 días, la cuenta se desactiva o se reactiva. Cuando se reactiva la cuenta, se restauran los permisos de Resource Explorer. Si el estado de la cuenta de miembro es Cuenta suspendida, la cuenta del administrador debe habilitar la cuenta manualmente.

Cuenta cerrada

Cuando se cierra una cuenta de AWS, Resource Explorer responde al cierre de la siguiente manera:

- Resource Explorer conserva los recursos de la cuenta durante 90 días a partir de la fecha de entrada en vigor del cierre de la cuenta. Al final del periodo de 90 días, Resource Explorer eliminará de forma permanente todos los recursos de la cuenta.
- Para conservar los recursos durante más de 90 días, puede utilizar una acción personalizada con una EventBridge regla para almacenar los recursos en un bucket de Amazon S3. Mientras Resource Explorer retiene los recursos, cuando vuelva a abrir la cuenta cerrada, restaurará los recursos de la cuenta.

- Si la cuenta es una cuenta del administrador de Resource Explorer, se elimina como administrador y se eliminan todas las cuentas de los miembros. Si la cuenta es una cuenta miembro, se desasocia y se elimina como miembro de la cuenta del administrador de Resource Explorer.
- Para obtener más información, consulte Cerrar una cuenta.

Exclusión de cuenta

Si una cuenta opta por excluirse de una región, seguirá viendo sus recursos en los resultados de búsqueda durante un máximo de 24 horas.

Transcurridas 24 horas, los recursos de esta cuenta no aparecerán en los resultados de búsqueda. Para obtener más información, consulte Comportamientos de desactivación.

Cómo desactivar Resource Explorer en una Región de AWS

Cuando ya no necesite buscar recursos en una Región de AWS específica, puede desactivar Explorador de recursos de AWS solo en esa región al eliminar su índice. Al hacerlo, Resource Explorer deja de buscar recursos nuevos o actualizados en esa región. Si su cuenta contiene un índice agregador, la replicación del índice eliminado se detiene y la información del índice eliminado se elimina del índice agregador y deja de aparecer en los resultados de búsqueda. Todos los recursos del índice eliminado pueden demorar hasta 24 horas en desaparecer de los resultados de búsqueda en la región con el índice agregador.

> **Note**
>
> Al registrar la primera Región de AWS, Resource Explorer crea un rol vinculado a un servicio (SLR) llamado `AWSServiceRoleForResourceExplorer` en la Cuenta de AWS. Resource Explorer no elimina esta SLR automáticamente. Tras eliminar el índice de Resource Explorer en todas las regiones de la cuenta, podrá utilizar la consola de IAM para eliminar la SLR si no volverá a utilizar el Resource Explorer en el futuro. Si elimina el rol y, a continuación, elige iniciar Resource Explorer de nuevo en al menos una Región de AWS, Resource Explorer volverá a crear el rol vinculado al servicio automáticamente.

Puede desactivar Resource Explorer en una Región de AWS mediante el uso de la AWS Management Console, el uso de los comandos en la AWS Command Line Interface (AWS CLI) o el uso de las operaciones de la API en un AWS SDK.

Si desactiva Resource Explorer para una cuenta de miembro y el miembro está en una vista de toda la organización, se eliminará de los resultados de búsqueda multicuenta.

Si ya no desea admitir la búsqueda de recursos en uno o más de las Regiones de AWS en su cuenta, siga los pasos del siguiente procedimiento.

> **Note**
>
> Si el índice que elimina es el índice agregador de la Cuenta de AWS, debe esperar 24 horas antes de que pueda promover otro índice agregador para que se convierta en el índice agregador de la cuenta. Los usuarios no pueden realizar búsquedas en toda la cuenta con Resource Explorer hasta que se configure otro índice agregador.

AWS Management Console

Cómo eliminar el índice de Resource Explorer en una Región de AWS

1. Abra la página de Configuración de Resource Explorer.
2. En la sección Índices, seleccione la casilla de verificación situada junto a las Regiones de AWS con los índices que desee eliminar y, a continuación, elija Eliminar.
3. En la página Eliminar índices, compruebe que haya seleccionado únicamente índices que desee eliminar. Escriba **`delete`** en la casilla de texto Confirmar y, a continuación, elija Eliminar índices.

   Resource Explorer muestra un cartel verde en la parte superior de la página para indicar que se ha realizado correctamente, o un cartel rojo si hay un error en una o más de las regiones seleccionadas.

AWS CLI

Cómo eliminar el índice de Resource Explorer en una Región de AWS

Si ya no desea admitir la búsqueda de recursos en uno o más de las Regiones de AWS en su cuenta, ejecute los siguientes comandos.

Ejecute el siguiente comando para cada región con los índices que desee eliminar. Debe ejecutar este comando en la región que contiene el índice que desea eliminar. El comando del siguiente ejemplo elimina el índice de Resource Explorer en el Oeste de EE. UU. (Oregón) (`us-west-2`).

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222 \
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
    "State": "DELETING"
}
```

Dado que Resource Explorer realiza parte de la limpieza como tareas asincrónicas en segundo plano, la respuesta podría indicar que la operación es `DELETING`. Este estado indica que los procesos en segundo plano aún no se han completado. Puede comprobar si se ha completado definitivamente ejecutando el siguiente comando y comprobando el cambio de `State` a `DELETED`.

```
$ aws resource-explorer-2 get-index \
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

Desactivar el explorador de recursos en todas las Regiones de AWS

Si desea desactivar Explorador de recursos de AWS por completo, lleve a cabo el siguiente procedimiento.

> **Note**
>
> El explorador de recursos crea un rol vinculado a un servicio denominado AWSServiceRoleForResourceExplorer en la cuenta al crear un índice en la primera Región

de AWS de una cuenta. El explorador de recursos no elimina automáticamente este rol vinculado al servicio. Tras eliminar el índice del explorador de recursos en todas las regiones, podrá utilizar la consola de IAM para eliminar el rol si está seguro de que no volverá a utilizar el explorador de recursos en el futuro. Si eliminas el rol y, a continuación, decide iniciar el explorador de recursos en al menos una Región de AWS, el explorador de recursos volverá a crear el rol vinculado al servicio.

Desactivar el explorador de recursos en todas las Regiones de AWS

Puede desactivar el explorador de recursos con el comando AWS Management Console, con los comandos del AWS Command Line Interface (AWS CLI) o con las operaciones de la API en un AWS SDK.

AWS Management Console

Si ya no quiere permitir la búsqueda de recursos en ninguna Región de AWS de su Cuenta de AWS, siga los pasos del siguiente procedimiento.

Para desactivar el explorador de recursos por completo Regiones de AWS

1. Abra la página de Configuraciones del explorador de recursos.
2. En la sección Índices, seleccione las casillas de verificación situadas junto a todas las Regiones de AWS registradas, a continuación, seleccione Eliminar.

   > **Tip**
   >
   > Puede marcar la casilla de la fila del encabezado de la tabla situada junto al Índice para marcar las casillas de todas las regiones en un solo paso.

3. En la página Eliminar índices, compruebe que desea eliminar todos los índices. Escriba **`delete`** en el cuadro de texto Confirmar y, a continuación, elija Eliminar índices.

   El explorador de recursos muestra un cartel verde en la parte superior de la página para indicar que se ha realizado correctamente, o un cartel rojo si hay un error en una o más de las regiones seleccionadas.

AWS CLI

Para desactivar el explorador de recursos en todas las Regiones de AWS

Si ya no quiere permitir la búsqueda de recursos en ninguna Regiones de AWS de su cuenta, ejecuta el siguiente comando para buscar el ARN de todos los índices de cada Región de AWS en las que activó anteriormente el explorador de recursos.

```
$ aws resource-explorer-2 list-indexes --query Indexes[*].Arn[
"arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
"arn:aws:resource-explorer-2:us-west-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
"arn:aws:resource-explorer-2:us-west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd33333333"
]
```

Para cada respuesta, ejecuta el siguiente comando para eliminar el índice del explorador de recursos en esa región.

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "State": "DELETING"
}
```

Repita el comando anterior en cada región adicional.

Dado que el explorador de recursos realiza parte de la limpieza como tareas asincrónicas en segundo plano, la respuesta podría indicar que la operación sí es `DELETING`. Este estado indica que los procesos en segundo plano aún no se han completado. Puede comprobar si se ha completado definitivamente ejecutando el siguiente comando y comprobando el cambio de estado a `DELETED`.

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
```

```
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```


Implementar el explorador de recursos en las cuentas de una organización

Al usar AWS CloudFormation StackSets, puedes definir e implementar en todas las cuentas administradas en una organización por AWS Organizations. Cuando define un conjunto de pilas, especifica los recursos AWS que desea que se creen en sus Regiones de AWS y en todas las cuentas de destino que especifique. Cuando todas las cuentas forman parte de la misma organización, puede aprovechar la integración con Organizaciones de AWS CloudFormation y dejar que esos servicios se encarguen de la creación de roles entre cuentas. Puede habilitar la implementación automática en una organización, que despliega automáticamente las instancias de pila en las nuevas cuentas que pueda añadir a la organización de destino o a una unidad organizativa (OU) en el futuro. Si elimina una cuenta de la organización, AWS CloudFormation eliminará automáticamente todos los recursos que se hayan desplegado como parte de una instancia de pilas de la organización. Para obtener más información acerca de StackSets, consulte Uso de AWS CloudFormation StackSets en la AWS CloudFormation Guía de usuario.

Puede usar los AWS CloudFormation StackSets para activar y Explorador de recursos de AWS configurar todas las cuentas de su organización, crear índices en cada región habilitada y crear vistas donde las necesite.

> **Important**
>
> Si intenta configurar un índice agregador en una región, debe asegurarse de que la cuenta no tenga un índice agregador existente en ninguna otra región. Si el índice que degrada es el índice agregador a un índice local, debe esperar 24 horas antes de que pueda promover otro índice agregador para que se convierta en el nuevo índice agregador de la cuenta.

Requisitos previos

Para usar AWS CloudFormation StackSets para implementar el explorador de recursos en las cuentas de su organización, usted o el administrador de su organización primero deben seguir los siguientes pasos para habilitar las pilas con permisos administrados por el servicio:

1. Su organización debe tener todas las características habilitadas. Si la organización únicamente ha consolidado características de facturación habilitadas, no puede crear un conjunto de pilas con permisos administrados por el servicio.
2. Active el acceso confiable entre AWS CloudFormation y Organizaciones. Esto otorga a AWS CloudFormation permiso para crear los roles necesarios en la cuenta de administración de la organización y las cuentas de los miembros AWS CloudFormation implementarán los índices y las vistas del explorador de recursos.

Ahora puede crear un conjunto de pilas con permisos administrados por el servicio

> **Important**
>
> Debe crear los conjuntos de pilas en la cuenta de administración de la organización. AWS CloudFormation es un servicio regional, por lo que puede ver y administrar los conjuntos de pilas que cree únicamente desde la región en la que los creó originalmente.

Crear los conjuntos de pilas para el explorador de recursos

Para implementar el Explorador de recursos por completo, debe implementar dos conjuntos de pilas.

- El primer conjunto de pilas crea el índice agregador y la vista predeterminada que permiten a los usuarios buscar recursos en todas las regiones de la cuenta.

  Implemente este conjunto de pilas solo en la región en la que desee crear el índice agregador.
- El segundo conjunto de pilas crea un índice local y una vista predeterminada. El índice local replica su contenido en el índice agregador.

  Implemente este conjunto de pilas en todas las regiones habilitadas de la cuenta, excepto en la región que contiene el índice agregador. No elija ninguna región que no esté habilitada en las cuentas en las que despliegue la pila. Si lo hace, se producirá un error en la implementación.

Las plantillas de ejemplo para cada una de ellas se encuentran en la siguiente sección. Para obtener instrucciones paso a paso sobre cómo crear un conjunto de pilas con estas plantillas, consulte Crear un conjunto de pilas con permisos gestionados por el servicio en la AWS CloudFormation Guía del usuario.

Tras implementar estos conjuntos de pilas en su organización, todas las cuentas del ámbito, organización o unidad organizativa que haya seleccionado, tendrán un índice agregador en la región especificada e índices locales en todas las demás regiones.

Plantillas AWS CloudFormation de ejemplo

La siguiente plantilla de ejemplo crea el índice agregador de la cuenta y una vista predeterminada que permite buscar recursos en todas las regiones de la cuenta en la que se implementa un índice.

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with an Aggregator Index, and a new Default
 View.
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with an Aggregator Index,
 and a new Default View.",
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

La siguiente plantilla de ejemplo crea un índice local en cada región habilitada en todas las cuentas, excepto en la que tiene el índice agregador. También crea una vista predeterminada en la que los

usuarios pueden buscar recursos únicamente en esa región. Los usuarios deben buscar con una vista en la región de agregación para buscar recursos en todas las regiones.

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with a Local Index, and a new Default View.
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: LOCAL
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with a Local Index, and a
 new Default View.",
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "LOCAL",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
```

```
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

Cómo administrar las vistas de Resource Explorer para proporcionar acceso a la búsqueda

Las vistas son la clave para buscar sus recursos. Cada operación de búsqueda de Explorador de recursos de AWS debe usar una vista.

Las vistas son el método que el administrador puede utilizar para controlar el acceso a la información sobre los recursos de su Cuenta de AWS.

Solo las entidades principales (roles de IAM o usuarios) que tengan permiso para usar una vista pueden usarla para acceder a ella. Para que la búsqueda se realice correctamente con Resource Explorer, la entidad principal debe tener acceso `Allow` a las operaciones tanto de `resource-explorer-2:GetView` como de `resource-explorer-2:Search` del ARN de la vista.

Las vistas contienen filtros integrados que el administrador puede usar para limitar los resultados solo a los elementos de interés. Por ejemplo, puede crear una vista que incluya solo los recursos relacionados con un proyecto determinado. Los usuarios que no necesiten ver información sobre otros proyectos pueden usar esta vista para ver solo los recursos que les interesen.

Una vista es un recurso regional. La vista se crea y almacena en una Región de AWS específica y devuelve en sus resultados solo información del índice de esa región. Para incluir los resultados de todas las regiones de la cuenta, la vista debe encontrarse en la región que contiene el índice agregador. Esa región contiene una réplica de los índices de todas las demás regiones de la cuenta.

Para obtener más información sobre cómo crear y usar vistas, consulte los temas siguientes:

Temas

Acerca de las vistas del explorador de recursos

Explorador de recursos de AWS indexa los recursos en segundo plano y, a continuación, pone ese índice a su disposición para que pueda consultarlo. Puede realizar consultas de búsqueda para sus recursos mediante la API del explorador de recursos documentada en esta guía o mediante la consola del explorador de recursos. El explorador de recursos usa su API para proporcionar una interfaz gráfica interactiva para lo que, de otro modo, solo sería una API accesible mediante programación. Los conceptos descritos en este tema se aplican tanto a la API como a la consola.

Una vista se almacena en un Región de AWS y devuelve los resultados únicamente de esa región.

Como es posible que el administrador desee limitar el acceso a la información contenida en el índice de recursos, no se puede acceder directamente a los índices en sí. En su lugar, todas las búsquedas deben pasar por una vista para la que el usuario debe tener permiso para buscarla.

Hay varios elementos clave en cada vista:

Permisos de búsqueda

Puede usar políticas de permisos de AWS estándar para controlar quién puede usar cada vista. Esto lo proporcionan las políticas de permisos basadas en la identidad adjuntas a la entidad principal, que le proporcionan un control pormenorizado sobre quién puede ver la información proporcionada por cada vista. Por ejemplo, puede conceder acceso a la vista de `Production-resources` para que solo puedan realizar búsquedas los ingenieros que operan sus servicios de producción. A continuación, puede conceder distintos permisos a la vista `Pre-production-resources` para que sus desarrolladores puedan buscar los recursos de preproducción.

Si utiliza la política administrada de AWS nombrada `AWSResourceExplorerReadOnlyAccess` junto con la entidad principal, les permite realizar búsquedas con cualquier vista de la cuenta.

También puede crear su propia política de permisos y conceder los siguientes permisos solo a determinadas vistas:

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

Para proporcionar acceso, agregue permisos a sus usuarios, grupos o roles:

- Usuarios y grupos de AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Crear un conjunto de permisos en la Guía de usuario de AWS IAM Identity Center.

- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda adoptar. Siga las instrucciones de Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones de Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Para obtener más información sobre el uso de permisos relacionados con las vistas, consulte Otorgar acceso a las vistas de Resource Explorer para la búsqueda.

Filtrar búsquedas

Una vista sirve como ventana virtual a través de la cual el usuario puede ver los recursos de la cuenta. Puede crear varias vistas, cada una de ellas presenta una vista diferente del panorama general. Por ejemplo, puede crear una vista que permita buscar únicamente los recursos asociados a su entorno de preproducción, identificados mediante las etiquetas adjuntas a sus recursos. A continuación, puede crear una vista independiente que permita buscar únicamente los recursos de su entorno de producción, en función de los distintos valores de las etiquetas. Si configura varias vistas con valores `FilterString` diferentes, no tendrá que volver a introducir esos parámetros de consulta cada vez que realice una Búsqueda.

Las vistas también pueden especificar qué datos opcionales sobre los recursos se deben incluir en los resultados. La lista de campos predeterminada siempre se incluye en los resultados. Además de la lista predeterminada, puede solicitar que la vista también incluya cualquier etiqueta adjunta al recurso .

Ámbitos de la búsqueda

- Ámbito regional: al buscar en un explorador Región de AWS de recursos, los resultados solo pueden incluir los recursos que estén indexados en esa región. En la mayoría de las regiones, el índice está etiquetado como `LOCAL` porque contiene información sobre los recursos que se encuentran únicamente en esa región. Las búsquedas en esas regiones solo pueden devolver esos recursos.
- Ámbito de cuenta: puede promover un índice local para que se convierta en el índice agregador de la cuenta. Al hacerlo, todas las demás regiones en las que esté activado el explorador

de recursos replicarán la información de su índice en la región con el índice agregador. Si busca en esa región, los resultados incluyen los recursos de todas las regiones de la cuenta. Al utilizar la opción Quick Setup para configurar el servidor, el explorador de recursos crea automáticamente un índice agregador en la región que especifique. Además, la opción Quick Setup crea una vista predeterminada en esa región para permitir la búsqueda de todos los recursos de la cuenta en todas las regiones.

Vistas predeterminadas

Si un usuario intenta buscar sin especificar una vista de forma explícita, el explorador de recursos utiliza la vista predeterminada definida para ese Región de AWS.

Si no existe una vista predeterminada para esa región y el usuario no especificó una vista para usarla, la búsqueda fallará y generará una excepción.

El explorador de recursos crea automáticamente una vista predeterminada de la siguiente manera:

- Si activa el explorador de recursos mediante AWS Management Console y elige la opción Quick Setup, debe especificar qué región contiene el índice agregador de la cuenta. El explorador de recursos crea automáticamente una vista predeterminada en la región del índice agregador especificada.
- Si registra el explorador de recursos mediante la opción Configuración avanzadaAWS Management Console y elige la opción Configuración avanzada, puede optar por crear el índice agregador para la cuenta en una región específica. Si lo hace, el explorador de recursos crea automáticamente una vista predeterminada en la región del índice agregador especificada.
- Si registra el explorador de recursos mediante la consola y decide no registrar una región del índice del agregador, el explorador de recursos crea una vista predeterminada para el índice local de cada región.
- Si registra el explorador de recursos mediante las operaciones del AWS CLI o de la API, el explorador de recursos no crea automáticamente una vista predeterminada. En su lugar, debe configurar manualmente la vista predeterminada para cada región desde la que espera que realicen búsquedas los usuarios.

Creación de vistas de Resource Explorer para usarlas en la búsqueda

Todas las búsquedas deben usar una vista. Una vista define filtros que determinan qué recursos pueden arrojar las consultas que utilizan la vista. Las vistas también controlan quién puede buscar recursos.

Una vista se almacena en un Región de AWSíndice de esa región y devuelve los resultados de búsqueda únicamente del índice de esa región. Si la región contiene el índice agregador, la vista arroja los resultados de búsqueda del índice en todas las regiones de la cuenta.

Las vistas multicuenta le permiten buscar recursos en las cuentas de toda la organización. Cualquier cuenta que desee buscar requiere índices. Solo la cuenta de administración o la cuenta del administrador delegado de la organización puede crear una vista multicuenta.

Explorador de recursos de AWS puede crear una vista predeterminada durante la configuración inicial si selecciona las opciones pertinentes en la Configuración rápida de Resource Explorer en la consola de Systems Manager o en la configuración avanzada. Más adelante, puede crear vistas adicionales con filtros diferentes para distintos conjuntos de usuarios.

Puede crear una vista mediante el uso AWS Management Console o la ejecución de AWS CLI comandos o sus operaciones de API equivalentes en un AWS SDK.

Permisos mínimos

Para ejecutar este comando, debe tener los siguientes permisos:

- Acción: `resource-explorer-2:CreateView`

  Recurso: puede utilizarse * para permitir la creación de una vista Región de AWS en cualquier parte de la cuenta.

AWS Management Console

Creación de una vista

1. Abra la página de Vistas de la consola de Resource Explorer y elija Crear vista.
2. En la página Crear vista, en Nombre, introduzca un nombre para la vista.

El nombre no debe tener más de 64 caracteres y puede incluir letras, dígitos y el carácter de guion (-). El nombre debe ser único dentro de su Región de AWS.

3. Elija el Región de AWS lugar en el que desee crear la vista. Para crear una vista que devuelva los recursos de todas las regiones de la cuenta, elija la Región de AWS que contenga el índice agregador.
4. (Opcional) En Ámbito, elija si la búsqueda proporcionará recursos de varias cuentas o solo recursos de su cuenta. El alcance a nivel de cuenta es el predeterminado.

   Solo la cuenta de administración o la cuenta del administrador delegado puede crear una vista multicuenta.
5. Elija si desea filtrar los resultados.

   - Cómo incluir todos los recursos

     No se incluyen filtros de consulta. Todos los recursos del índice asociado a la vista se pueden mostrar en los resultados de la búsqueda.
   - Cómo incluir solo los recursos que coincidan con un filtro específico

     Active la casilla de verificación Filtros de recursos, en la que puede elegir los nombres y operadores de los filtros. Para obtener una explicación de cada uno de los operadores y nombres de filtros disponibles, consulte Filtros.
   - Elija los atributos de recurso opcionales que desee incluir en los resultados de esta vista. Seleccione la casilla de verificación situada junto a Etiquetas para que los usuarios puedan buscar recursos en función de los nombres y valores de las claves de sus etiquetas. Si no incluye etiquetas en la vista, los usuarios no podrán realizar solicitudes de búsqueda que utilicen claves y valores de etiquetas para filtrar aún más los resultados.
   - Si lo desea, puede adjuntar etiquetas a la vista. Expanda la casilla Etiquetas e introduzca hasta 50 pares de clave/valor de etiqueta. Puede utilizar etiquetas para categorizar recursos o como parte de una estrategia de permisos de seguridad de control de acceso basado en atributos (ABAC). Para obtener más información, consulte Agregar etiquetas a vistas.
   - Elija Crear vista.

   La consola vuelve a la página de Búsqueda, donde puede utilizar la nueva vista para realizar una búsqueda.

Siguiente paso: concede permisos a la entidad principal de su cuenta para buscar con su nueva vista. Para obtener más información, consulte Otorgar acceso a las vistas de Resource Explorer para la búsqueda

AWS CLI

Creación de una vista

Ejecute el siguiente comando para crear una vista en la Región de AWS especificada. El siguiente ejemplo crea una vista que proporciona solo los recursos relacionados con el servicio Amazon EC2 que están etiquetados con una clave `Stage` y el valor `prod`.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name "My-EC2-Prod-Resources" \
    --filters FilterString="service:ec2 tag:stage=prod" \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
            "FilterString": "service:ec2 tag:stage=prod"
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:123456789012:view/My-EC2-
Prod-Resources/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

Crear una vista de nivel de organización

En el siguiente ejemplo se crea una vista que proporciona recursos de toda la organización. Esto debe realizarlo la cuenta de administración de la organización o una cuenta de administrador delegado.

1. Ejecute el comando `aws organizations describe-organization` para obtener el ARN de su organización.
2. Ejecute el siguiente comando para crear una vista en el área especificada.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-org-view \
    --scope "arn:aws:organizations::111111111111:organization/o-exampleorgid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "111111111111",
        "Scope": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:111111111111:view/
entire-org-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

Para crear una vista de nivel de unidad de organización

En el siguiente ejemplo, se crea una vista que devuelve los recursos de todos los miembros de esta unidad organizativa. Esta vista se comporta de forma similar a una vista a nivel organizativo. Esto debe realizarlo la cuenta de administración de la organización o una cuenta de administrador delegado.

1. Ejecute el comando `aws organizations describe-organizational-unit` para obtener el ARN de su organización.
2. Ejecute el siguiente comando para crear una vista de la unidad organizativa especificada.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-ou-view \
    --scope "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid"
{
```

```
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "222222222222",
        "Scope": "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:222222222222:view/
entire-ou-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```


Siguiente paso: concede permisos a la entidad principal de su cuenta para buscar con su nueva vista. Para obtener más información, consulte Otorgar acceso a las vistas de Resource Explorer para la búsqueda

Otorgar acceso a las vistas de Resource Explorer para la búsqueda

Antes de que los usuarios puedan realizar una búsqueda con una vista nueva, debe conceder acceso a las vistas de Explorador de recursos de AWS. Para ello, utilice una política de permisos basada en la identidad para las entidades principales de AWS Identity and Access Management (IAM) que necesiten realizar búsquedas con la vista.

Para proporcionar acceso, agregue permisos a sus usuarios, grupos o roles:

- Usuarios y grupos de AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Create a permission set (Creación de un conjunto de permisos) en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda asumir. Siga las instrucciones de Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.

- (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones de Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Puede usar cualquiera de los métodos siguientes:

- Usar una política administrada de AWS existente. Resource Explorer proporciona varias políticas administradas de AWS predefinidas para su uso. Para obtener información detallada sobre todas las políticas administradas de AWS que están disponibles, consulte AWS políticas gestionadas para Explorador de recursos de AWS.

  Por ejemplo, puede usar la política `AWSResourceExplorerReadOnlyAccess` para conceder permisos de búsqueda a todas las vistas de la cuenta.

- Cree su propia política de permisos y asígnela a las entidades principales. Si crea su propia política, puede restringir el acceso a una sola vista o a un subconjunto de las vistas disponibles especificando el nombre de recurso de Amazon (ARN) de cada vista en el elemento `Resource` de la declaración de política. Por ejemplo, puede usar la siguiente política de ejemplo para conceder a esa entidad principal la posibilidad de realizar búsquedas utilizando solo esa vista.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyTestView/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
        }
    ]
}
```

  Utilice la consola de IAM para crear esas políticas de permisos y utilizarlas con las entidades principales que necesitan esos permisos. Para obtener más información acerca de las políticas de permisos de IAM, consulte los siguientes temas:

  - Políticas y permisos en IAM

- Agregary eliminar permisos de identidad de IAM
- Comprender los permisos concedidos por una política

Uso de una autorización basada en etiquetas para controlar el acceso a sus vistas

Si opta por crear varias vistas con filtros que devuelvan resultados solo con determinados recursos, puede que también desee restringir el acceso a esas vistas únicamente a las entidades principales que necesiten ver esos recursos. Puede proporcionar este tipo de seguridad a las vistas de su cuenta mediante una estrategia de control de acceso basado en atributos (ABAC). Los atributos que utiliza ABAC son las etiquetas adjuntas tanto a las entidades principales que intentan realizar operaciones en AWS, como a los recursos a los que intentan acceder.

ABAC utiliza políticas de permisos de IAM estándar adjuntas a las entidades principales. Las políticas utilizan elementos `Condition` en las instrucciones de políticas para permitir el acceso solo cuando las etiquetas adjuntas a la entidad principal solicitante y las etiquetas adjuntas al recurso afectado coinciden con los requisitos de la política.

Por ejemplo, puede adjuntar una etiqueta `"Environment" = "Production"` a todos los AWS recursos que admiten la aplicación de producción de su empresa. Para asegurarse de que solo las entidades principales que están autorizadas a acceder al entorno de producción puedan ver esos recursos, cree una vista de Resource Explorer que utilice esa etiqueta como filtro. A continuación, para restringir el acceso a la vista únicamente a las entidades principales correspondientes, debe conceder los permisos mediante una política que tenga una condición similar a la de los siguientes elementos del ejemplo.

```
{
    "Effect": "Allow",
    "Action": [ "service:Action1", "service:Action2" ],
    "Resource": "arn:aws:arn-of-a-resource",
    "Condition": { "StringEquals": {"aws:ResourceTag/Environment":
 "${aws:PrincipalTag/Environment}"} }
}
```

Esa `Condition` en el ejemplo anterior especifica que la solicitud solo está permitida si la etiqueta `Environment` adjunta a la entidad principal que realiza la solicitud coincide con la etiqueta `Environment` adjunta al recurso especificado en la solicitud. Si esas dos etiquetas no coinciden exactamente o si falta alguna de ellas, Resource Explorer deniega la solicitud.

> **Important**
>
> Para utilizar ABAC correctamente y proteger el acceso a sus recursos, primero debe restringir el acceso a la posibilidad de añadir o modificar las etiquetas adjuntas a sus entidades principales y recursos. Si un usuario puede añadir o modificar las etiquetas adjuntas a una entidad principal o recurso de AWS, ese usuario puede afectar a los permisos controlados por esas etiquetas. En un entorno ABAC seguro, solo los administradores de seguridad aprobados tienen permiso para añadir o modificar las etiquetas adjuntas a las entidades principales, y solo los administradores de seguridad y los propietarios de los recursos pueden añadir o modificar las etiquetas adjuntas a los recursos.

Para obtener más información sobre cómo implementar correctamente una estrategia ABAC, consulte los siguientes temas en la Guía del usuario de IAM:

- Tutorial de IAM: definición de permisos para acceder a los recursos de AWS en función de etiquetas
- Control de acceso a los recursos de AWS mediante etiquetas

Una vez que tenga la infraestructura ABAC necesaria, puede comenzar a usar etiquetas para controlar quién puede realizar búsquedas con las vistas de Resource Explorer de su cuenta. Para ver ejemplos de políticas que ilustran este principio, consulte los siguientes ejemplos de políticas de permisos:

- Otorgar acceso a una vista basada en etiquetas
- Otorgar acceso para crear una vista basada en etiquetas

Establecer una vista predeterminada en un Región de AWS

En Explorador de recursos de AWS, puede definir varias vistas en una Región de AWS, donde cada vista aborde diferentes requisitos de búsqueda. Se recomienda configurar una vista en cada región como la vista predeterminada para esa región.

Resource Explorer usa la vista predeterminada toda vez que un usuario realiza una búsqueda y no especifica explícitamente qué vista usar. La barra de búsqueda unificada situada en la parte superior de cada página de la AWS Management Console también utiliza automáticamente la

vista predeterminada de la región que contiene el índice del agregador para buscar recursos que coincidan con la consulta de búsqueda del usuario.

Puede seleccionar solo una vista que exista en la región para que sea la vista predeterminada de esa región. Si otra región tiene una vista que desee utilizar, primero debe crear una copia de esa vista en la región en la que desee convertirla en la vista predeterminada.

> **Tip**
>
> No existe ninguna operación de copia de vista. Debe crear una vista en la región de destino y, a continuación, copiar la configuración de la vista existente a la nueva vista.

Puede especificar una vista como la predeterminada para esa región usando la AWS Management Console o ejecutando los comandos de AWS CLI o las operaciones equivalentes de API en un SDK de AWS.

AWS Management Console

Establecer una vista predeterminada

1. En la página de Vistas de Resource Explorer, elija el botón de opción situado junto a la vista que desea que sea predeterminada para esa región.
2. Elija Acciones, y a continuación elija Establecer como predeterminada.

AWS CLI

Establecer una vista predeterminada

Ejecute el siguiente comando para establecer la vista específica como predeterminada para la región. En el siguiente ejemplo, se establece la vista específica como predeterminada para todas las búsquedas realizadas en la región us-east-1. Esa vista debe existir en la región en la que usted ejecuta el comando.

```
$ aws resource-explorer-2 associate-default-view \
    --region us-east-1 \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
```

```
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

Agregar etiquetas a vistas

Puede agregar etiquetas a las vistas para categorizarlas. Las etiquetas son metadatos proporcionados por el cliente que adoptan la forma de una cadena de nombre clave y una cadena de valores opcionales asociada. Para obtener más información sobre cómo etiquetar recursos de AWS, consulte Etiquetado de recursos de AWS en la Referencia general de Amazon Web Services.

Añadir etiquetas a sus vistas

Puede añadir etiquetas a sus vistas de Resource Explorer mediante la AWS Management Console o ejecutando comandos AWS CLI o sus operaciones de API equivalentes en un SDK de AWS.

AWS Management Console

Para añadir etiquetas a una vista

1. Abra la página de vistas de Resource Explorer y elija el nombre de la vista que desea etiquetar para mostrar su página de Detalles.
2. En Etiquetas, elija Administrar etiquetas.
3. Para agregar una etiqueta, elija Agregar etiqueta y, a continuación, ingrese la clave y el valor opcional de la etiqueta.

   > **Note**
   >
   > También puede eliminar una etiqueta seleccionando la X que se encuentra junto a la etiqueta.

   Puede asociar hasta 50 etiquetas definidas por el usuario a un recurso. Las etiquetas que se crean y que AWS administra automáticamente no se tienen en cuenta para esta cuota.
4. Cuando termine de realizar los cambios en las etiquetas, elija Guardar.

AWS CLI

Para añadir etiquetas a una vista

Ejecute el siguiente comando para agregar etiquetas a una vista. En el siguiente ejemplo, se agregan etiquetas con el nombre clave `environment` y el valor `production` a la vista especificada.

```
$ aws resource-explorer-2 tag-resource \
    --resource-id arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --tags environment=production
```

El comando anterior no genera ningún resultado si se utiliza correctamente.

> **Note**
>
> Para eliminar una etiqueta existente de una vista, utilice el comando `untag-resource`.

Controlar los permisos con etiquetas

Un uso clave del etiquetado es para respaldar una estrategia de control de acceso basado en atributos (ABAC). ABAC puede ayudar a simplificar la gestión de permisos al permitirle etiquetar los recursos. Después, se conceden permisos a los usuarios para los recursos que estén etiquetados de una forma determinada.

Por ejemplo, considere esta situación: En el caso de una vista llamada `ViewA`, debe adjuntar la etiqueta `environment=prod` (nombre clave=valor). Otra `ViewB` podría estar etiquetada `environment=beta`. Los roles y los usuarios se etiquetan con las mismas etiquetas y valores, en función del entorno al que debe poder acceder cada rol o usuario.

A continuación, puede asignar una política de permisos de AWS Identity and Access Management (IAM) a sus roles de IAM, grupos y usuarios. La política concede permiso para acceder y buscar mediante una vista solo si el rol o el usuario que realiza la solicitud de búsqueda tiene una etiqueta `environment`con el mismo valor que la etiqueta `environment` adjunta a la vista.

La ventaja de este enfoque es que es dinámico y no requiere que se lleve una lista de quién tiene acceso a qué recursos. En su lugar, debe asegurarse de que todos los recursos (sus vistas) y las

entidades principales (roles de IAM y usuarios) estén etiquetados correctamente. Después, los permisos se actualizan automáticamente sin que tenga que cambiar ninguna política.

Hacer referencia a etiquetas en una política de ABAC

Una vez que las vistas estén etiquetadas, puede optar por utilizarlas para controlar el acceso dinámico a esas vistas. En el siguiente ejemplo de política se parte del supuesto de que tanto las entidades principales de IAM como las vistas se etiquetan con la clave de etiqueta `environment` y algún valor. Una vez hecho esto, puede asociar la siguiente política de ejemplo a sus entidades principales. Sus roles y usuarios pueden entonces `Search` usando cualquier vista que esté etiquetada con un valor de etiqueta `environment` que coincida exactamente con la etiqueta `environment` adjunta a la entidad principal.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:ResourceTag/environment": "${aws:PrincipalTag/environment}"
                }
            }
        }
    ]
}
```

Si tanto la entidad principal como la vista tienen la etiqueta `environment`, pero los valores no coinciden, o si en alguno de los dos falta la etiqueta `environment`, Resource Explorer deniega la solicitud de búsqueda.

Para obtener más información sobre el uso de ABAC para conceder acceso seguro a sus recursos, consulte ¿Qué es ABAC para AWS?

Cómo compartir vistas de Resource Explorer

Las vistas en Explorador de recursos de AWS utilizan principalmente políticas basadas en recursos para conceder el acceso. Al igual que las políticas de bucket de Amazon S3, estas políticas se adjuntan a la vista y especifican quién puede utilizarla. Esto contrasta con las políticas basadas en la identidad de AWS Identity and Access Management (IAM). Una política basada en la identidad de IAM se asigna a un rol, grupo o usuario y especifica a qué acciones y recursos puede acceder ese rol, grupo o usuario. Puede usar cualquier tipo de política con las vistas de Resource Explorer, de la siguiente manera:

- En la cuenta de administración o la cuenta de administrador delegado propietaria del recurso, utilice cualquiera de los dos tipos de política para conceder el acceso, siempre que ninguna otra política deniegue explícitamente el acceso a la vista a esa entidad principal.
- En todas las cuentas, debe usar ambos tipos de políticas. La política basada en recursos adjunta a la vista de la cuenta de uso compartido activa el uso compartido con otra cuenta consumidora. Sin embargo, esa política no concede acceso a los usuarios o roles individuales de la cuenta consumidora. El administrador de la cuenta consumidora también debe asignar una política basada en la identidad a los roles y usuarios deseados en la cuenta consumidora. Esa política concede acceso al nombre de recurso de Amazon (ARN) de la vista.

Para compartir vistas con otras cuentas, debe usar AWS Resource Access Manager (AWS RAM). AWS RAM gestiona por usted la complejidad de las políticas basadas en recursos. Antes de poder compartir, debe seguir estos pasos para activar la búsqueda en varias cuentas.

Para compartir una vista, debe ser administrador de la cuenta de la organización o un administrador delegado. Puede especificar las cuentas o identidades con las que desea compartir el recurso. AWS RAM es totalmente compatible con las vistas de Resource Explorer. AWS RAM utiliza políticas similares a las que se describen en las siguientes secciones, en función de los tipos de entidades principales con las que decida compartir. Para obtener instrucciones sobre cómo compartir recursos, consulte Compartir sus recursos de AWS en la Guía del usuario de AWS Resource Access Manager.

Los administradores y los administradores delegados pueden crear y compartir tres tipos diferentes de vistas: vista de alcance de la organización, vistas de alcance de la unidad organizativa (OU) y vistas de alcance a nivel de cuenta. Pueden compartirlas con organizaciones, unidades organizativas o cuentas. Cuando las cuentas se unen a la organización o la abandonan, AWS RAM concede o revoca automáticamente la vista compartida.

Política de permisos para compartir la vista con Cuentas de AWS

El siguiente ejemplo de política muestra cómo hacer que una vista esté disponible para las entidades principales en dos Cuentas de AWS diferentes:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [ "111122223333", "444455556666" ]
            },
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            ],
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Condition": {"StringEquals": {"aws:PrincipalOrgID": "o-123456789012"},
                "StringNotEquals": {"aws:PrincipalAccount": "123456789012"}
            }
        }
    ]
    }"
}
```

El administrador de cada una de las cuentas especificadas ahora debe especificar qué roles y usuarios pueden acceder a la vista adjuntando políticas de permisos basadas en la identidad a los roles, grupos y usuarios. Los administradores de las cuentas 111122223333 o 444455556666 pueden crear la siguiente política de ejemplo. Después, pueden asignar la política a los roles, grupos y usuarios de esas cuentas a los que se les permitirá realizar búsquedas utilizando la vista compartida desde la cuenta de origen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
```

```
                "resource-explorer-2:GetView",
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    ]
}
```

Puede utilizar estas políticas de IAM basadas en la identidad como parte de una estrategia de seguridad de control de acceso basado en atributos (ABAC). En ese paradigma, se asegura que todos sus recursos y todas sus identidades estén etiquetados. A continuación, especifique en sus políticas qué claves y valores de etiquetas deben coincidir entre la identidad y el recurso para que se permita el acceso. Para obtener información acerca de cómo etiquetar las vistas de su cuenta, consulte Agregar etiquetas a vistas. Para obtener más información sobre el control de acceso basado en atributos, consulte ¿Qué es el ABAC para AWS? y Controlar el acceso a los recursos de AWS mediante etiquetas, ambos se encuentran en la Guía del usuario de IAM.

Eliminar vistas en el explorador de recursos

Cuando ya no necesite una vista Explorador de recursos de AWS, puede eliminarla. Puede eliminar vistas con AWS Management Console o la ejecución de comandos AWS CLI o sus operaciones de API equivalentes en un SDK de AWS.

> **Note**
>
> No puede eliminar una vista que actualmente esté designada como predeterminada para su Región de AWS. Para eliminar la vista, debe eliminarla como predeterminada. Para ello, puede ejecutar la operación de la API DisassociateDefaultView en esa región.

Permisos mínimos

Para ejecutar este comando, debe tener los siguientes permisos:

- Acción: `resource-explorer-2:DeleteView`

  Recurso: El ARN de la vista que se va a eliminar

AWS Management Console

Para eliminar una vista

1. En la página de Vistas de la consola del Explorador de recursos, pulse el botón de opción situado junto a la vista que desee eliminar.
2. Elija Acciones y, a continuación, elija Eliminar.
3. En el cuadro de diálogo de confirmación, ingrese el nombre de la vista y luego elija Eliminar.

AWS CLI

Para eliminar una vista

Ejecute el siguiente comando para eliminar la vista con el nombre de recurso de Amazon (ARN) especificado.

```
$ aws resource-explorer-2 delete-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

Uso de Explorador de recursos de AWS para buscar recursos

El objetivo principal de habilitar Explorador de recursos de AWS en su Cuenta de AWS es que los usuarios puedan buscar recursos en la cuenta. Utilice la AWS Management Console o AWS Command Line Interface (AWS CLI) para buscar recursos mediante el explorador de recursos.

A continuación se enumerarán algunas de las características principales de la búsqueda en el explorador de recursos.

- Cada búsqueda debe usar una vista.

  El explorador de recursos utiliza la vista para determinar quién tiene permisos para ver ciertos recursos. Para utilizar una vista durante una búsqueda del explorador de recursos, el usuario debe tener un `Allow` en el `resource-explorer-2:Search` de la operación para la vista especificada. Este permiso proviene de una política de permisos basada en la identidad adjunta a la entidad principal que realiza la solicitud.

  La vista puede incluir un filtro que limite los recursos que se pueden incluir en los resultados. Al crear distintas vistas que utilizan filtros y al conceder el acceso a las distintas vistas a las diferentes entidades principales, usted puede configurar un entorno en el que cada grupo de usuarios pueda ver solo los recursos que le interesan.

  Para obtener más información acerca de las visualizaciones, consulte Cómo administrar las vistas de Resource Explorer para proporcionar acceso a la búsqueda.
- El explorador de recursos utiliza procesos asíncronos en segundo plano para mantener sus índices.

  Los procesos de indexación del explorador de recursos pueden demorar en detectar los recursos recién creados o modificados y añadirlos al índice local. El explorador de recursos puede tardar más tiempo de lo normal en replicar los cambios de los índices locales en el índice agregador.

  Lo mismo sucede con los recursos que elimine. Una vez eliminado un recurso, el proceso de indexación puede demorar en detectar esa acción y eliminar la información del recurso del índice local. El explorador de recursos necesita más tiempo para replicar la eliminación del índice local en el índice agregador de la cuenta.

Las adiciones, modificaciones y eliminaciones de sus recursos pueden tardar hasta un máximo de 36 horas hasta que el explorador de recursos muestre esos cambios en los resultados de búsqueda de todas las regiones donde lo haya activado.

- Las búsquedas en el explorador de recursos se realizan dentro de una Región de AWS.

  Cada región donde activa el explorador de recursos contiene un índice de los recursos almacenados en esa región solamente. Las vistas también se asocian a las regiones y solo pueden mostrar los recursos que se encuentran en el índice de esa región. La única excepción es el índice agregador, que recibe una copia replicada de todos los índices locales para poder realizar búsquedas en todas las regiones de la cuenta.

- La búsqueda entre regiones requiere un índice agregador para la cuenta.

  Para que los usuarios puedan buscar recursos en todas las cuentas de las Regiones de AWS, el administrador debe designar una región para que contenga el índice agregador de la cuenta. Una copia de cada índice local se replica automáticamente en el índice agregador.

  Por este motivo, solo las vistas de la región del índice agregador pueden proporcionar resultados que incluyan los recursos de todos los Regiones de AWS de la cuenta.

- Una consulta consiste en cualquier cantidad de filtros y palabras clave de texto de formato libre.

  Las palabras clave de formato libre se combinan en la consulta mediante operadores lógicos **OR**. Los filtros que utilizan nombres de filtro definidos por el explorador de recursos se combinan en la consulta mediante **AND** operadores lógicos. Tenga en cuenta el siguiente ejemplo de consulta.

  ```
  test instance service:EC2 region:us-west-2
  ```

  El explorador de recursos evalúa esto de la siguiente manera.

  ```
  test OR instance AND service:EC2 AND region:us-west-2
  ```

  Esta consulta requiere que los recursos equivalentes sean recursos de Amazon EC2 en la región Oeste de EE.UU. (Oregón) y que tengan al menos una de las palabras clave (prueba, instancia) adjunta de alguna manera, como en el nombre, la descripción o en las etiquetas.

> **Note**
>
> Debido al AND implícito, solo puede utilizar correctamente un filtro para un atributo que solo pueda tener un valor asociado al recurso. Por ejemplo, un recurso solo puede formar parte de una Región de AWS. Por lo tanto, la consulta subsiguiente no produce resultados.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Esta limitación no se aplica a los filtros de los atributos que pueden tener varios valores al mismo tiempo `tag:`, como `tag.key:`, y `tag.value:`.

- Una búsqueda solo puede proporcionar los primeros 1000 resultados.

  Este requisito incluye una búsqueda con una cadena de consulta vacía que coincida con todos los recursos. Para ver recursos superiores a los 1000 proporcionados por una cadena de consulta vacía, debe utilizar las consultas para restringir los resultados coincidentes a los que desee ver y limitar el número de coincidencias a menos de 1000.
- Existe una cuota por cuenta en el número de operaciones de búsqueda que puede realizar.

  Las cuotas limitan el número de consultas que puede realizar por segundo y cuántas puede realizar cada mes. Para conocer los números de cuota específicos, consulte Cuotas para Resource Explorer.

AWS Management Console

Buscar recursos mediante el explorador de recursos

1. En la página de búsqueda de recursos, comience por elegir la vista que desee usar. Solo puede elegir entre las vistas a las que tiene permiso de acceso.
2. En Query (consulta), introduzca los términos de búsqueda y los filtros que identifican los recursos que desea ver. Para obtener información sobre todas las opciones disponibles, consulte la Búsqueda de referencia de sintaxis de consulta en Resource Explorer.
3. Pulse Intro para enviar la consulta.

   El explorador de recursos muestra todos los resultados que coinciden tanto con el `Filter` definido en la vista como con la consulta que usted proporciona. Los resultados se ordenan

por relevancia: los recursos que coinciden con más términos de la consulta aparecen más arriba en la lista y los que coinciden con menos términos aparecen más abajo en la lista.

4. Elija el identificador de un recurso para ir a la consola nativa de ese tipo de recurso, donde podrá interactuar con el recurso de todas las formas que admite ese servicio.

AWS CLI

Buscar recursos mediante el explorador de recursos

Ejecute el siguiente comando para buscar recursos mediante la vista especificada. Esa vista debe existir en la región en la que ejecuta la operación. En el siguiente ejemplo se buscan instancias de Amazon EC2 etiquetadas `env=production` en el Este de EE. UU. (Ohio) (us-east-2). Para obtener información sobre todas las opciones de sintaxis disponibles para el `query-string` parámetro, consulte Búsqueda de referencia de sintaxis de consulta en Resource Explorer.

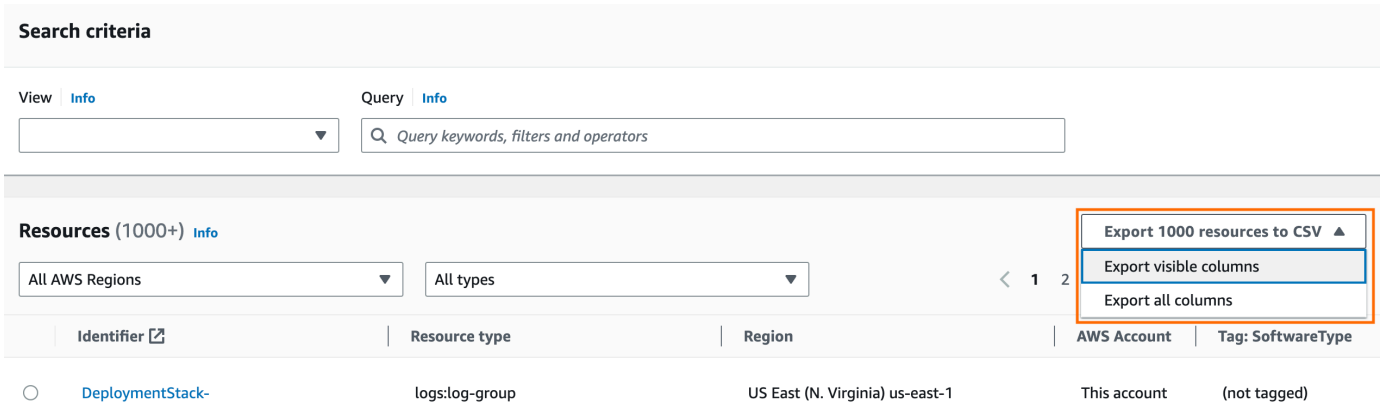
```
$ aws resource-explorer-2 search \
    --region us-east-1 \
    --query-string "resourcetype:AWS::EC2::Instance tag:env=production"
    --view-arn arn:aws:resource-explorer-2:us-east-2:123456789012:view/My-Resources-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

Exporte los resultados de la búsqueda a un archivo .csv

Puede exportar los resultados de una búsqueda de recursos a un archivo (.csv) de valores separados por comas. El archivo .csv incluye el identificador, los nombres de los recursos, la región, Cuenta de AWS, el número total de etiquetas y una columna para cada clave de etiqueta única en la recopilación. El archivo .csv puede ayudarle configurar los recursos AWS en su organización o a encontrar repeticiones o inconsistencias en el etiquetado de los distintos recursos.

1. En los resultados de la consulta de búsqueda de recursos consulta, elija Exportar recursos a un archivo .csv.

   Puede elegir entre exportar los resultados solo con las columnas que puede ver actualmente o exportarlos con todas las columnas disponibles.



2. Cuando su navegador se lo solicite, seleccione abrir el archivo .csv o guárdelo en una ubicación adecuada.

Búsqueda de referencia de sintaxis de consulta en Resource Explorer

Explorador de recursos de AWS le ayuda a encontrar AWS recursos individuales en su Cuentas de AWS. Para ayudarlo a encontrar los recursos exactos que busca, Resource Explorer acepta cadenas de consultas de búsqueda que admitan la sintaxis descrita en este tema. Para ver consultas de ejemplo que muestran cómo utilizar las características que se describen aquí, consulte Ejemplo de consultas de búsqueda del Explorador de recursos.

> **Note**
>
> En este momento, las etiquetas adjuntas a los recursos AWS Identity and Access Management (de IAM), como los roles o los usuarios, no están indexadas.

Cómo funcionan las consultas en Resource Explorer

Las consultas de búsqueda siempre utilizan una vista. Si no especificas ninguna de forma explícita, el Explorador de recursos utilizará la vista designada como predeterminada para la vista en la Región de AWS que estés trabajando.

Las vistas determinan qué recursos están disponibles para consultarlos. Puede crear vistas diferentes para que cada una proporcione un conjunto de recursos diferente.

Por ejemplo, puede crear una vista que incluya solo los recursos etiquetados con la clave `Environment` y el valor `Production`. A continuación, puede optar por conceder acceso a esa vista únicamente a los usuarios que tengan un motivo empresarial para ver esos recursos. Diferentes usuarios que necesiten ver esos recursos podrían acceder a una vista independiente que incluya los recursos del entorno `Alpha` o `Beta`. Para obtener más información sobre el control de quiénes acceden a qué vistas, consulte Otorgar acceso a las vistas de Resource Explorer para la búsqueda.

Sintaxis de cadenas de consulta

En esta sección se proporciona información sobre los aspectos básicos de la sintaxis de las consultas, los filtros y los operadores de filtro.

Conceptos básicos

En su forma más básica, un `QueryString` es un conjunto de palabras clave de texto de formato libre a las que se une implícitamente un operador lógico **`OR`**. Para separar cada palabra clave de las demás, utilice un espacio, como se muestra en el siguiente ejemplo:

```
ec2 billing test gamma
```

Resource Explorer evalúa esta lista de palabras clave en el sentido de:

```
ec2 OR billing OR test OR gamma
```

Resource Explorer ordena los resultados por relevancia, dando mayor preferencia a los recursos que coinciden con un mayor número de términos de búsqueda. Los recursos que no coincidan con uno o más de los términos no se excluyen de los resultados. Sin embargo, Resource Explorer los considera de menor relevancia y los coloca más abajo en los resultados de búsqueda.

Si especifica una cadena vacía para el parámetro `QueryString`, la consulta proporcionará los primeros 1000 recursos que estén disponibles a través de la vista utilizada para la operación. El número máximo de recursos que puede proporcionar una consulta es 1000.

> **Note**
>
> AWS se reserva el derecho de actualizar la lógica de coincidencia y los algoritmos de relevancia para evaluar las palabras clave de texto de formato libre, de modo que podamos ofrecer a los clientes los resultados más relevantes. Por lo tanto, los resultados proporcionados para las mismas consultas con palabras clave de texto de formato libre pueden cambiar con el tiempo. Si necesita resultados más determinantes, le recomendamos que utilice filtros. La lógica de coincidencia de filtros no cambia con el tiempo.

Filtros

Puede limitar los resultados de la consulta de forma más estricta mediante la inclusión de filtros. A diferencia de las palabras clave de texto, los filtros se evalúan en la consulta con el operador AND. Por ejemplo, considere la siguiente consulta, que consta de dos palabras clave de formato libre y dos filtros:

```
test instance service:EC2 region:us-west-2
```

Esta consulta se evalúa de la siguiente manera:

```
( test OR instance ) AND service:EC2 AND region:us-west-2
```

Los filtros siempre se evalúan mediante los operadores lógicos AND. Si un recurso no coincide con el filtro, no se incluye en los resultados. Los resultados de la consulta de ejemplo incluyen todos los recursos que estén asociados a Amazon EC2 y se encuentren en el oeste de EE. UU. (Oregón) Región de AWS y que tengan al menos una de las palabras clave asociada de alguna manera.

> **Note**
>
> Debido a AND implícito, solo puede utilizar correctamente un filtro para un atributo que pueda tener únicamente un valor asociado al recurso. Por ejemplo, un recurso solo puede formar parte de una Región de AWS. Por lo tanto, la consulta indica que no hay resultados.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Esta limitación no se aplica a los filtros de los atributos que pueden tener varios valores al mismo tiempo, como por ejemplo, `tag:`, `tag.key:` y `tag.value:`.

En la siguiente tabla, se muestran los nombres de filtro disponibles que puede utilizar en una consulta de búsqueda de Resource Explorer.

Nombre del filtro	Descripción y ejemplo
`accountid:`	El Cuenta de AWS propietario del recurso. Resource Explorer incluye en los resultados únicamente los recursos que pertenecen a la cuenta especificada. `accountid:123456789012`
`application:`	Este filtro le permite buscar recursos con una clave de etiqueta de `awsApplication` y un valor de grupo de recursos. Puede buscar por nombre de aplicación o por el ARN del grupo de recursos de la aplicación. `application:MyApplicationName`

Nombre del filtro	Descripción y ejemplo

	`application:arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced`
	
	`arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced`
	
	Note
	Para usar este filtro, la vista debe tener acceso a los datos de etiquetado.

`id:`	El identificador de un recurso individual, expresado como un nombre de recurso de Amazon (ARN). `id:arn:aws:license-manager: us-east-1 :123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea26EXAMPLE`
`region:`	El Región de AWS lugar donde se encuentra el recurso. El explorador de recursos incluye en los resultados solo los recursos que residen en lo especificado Región de AWS. `region:us-east-1` **Note** Si se escribe únicamente el código de región (sin filtro, por ejemplo `us-east-1`), no se obtienen los mismos resultados que `region:us-east-1` . Este resultado se debe a que, al tratarse de una palabra clave de texto de formato libre que no es un filtro, el código de región se divide en partes individuales. Por ejemplo, `us-east-1` se busca como `us`, `east` y `1`. Este desglose en component es no se produce cuando se utiliza el prefijo `region:`.

Nombre del filtro	Descripción y ejemplo
`region:global`	Un caso especial para el `region:` filtro que se puede utilizar para buscar recursos que no están asociados a una persona Región de AWS pero que se consideran de alcance global. `region:global` **Note** Si solo se escribe la palabra clave `global`, no se obtienen los mismos resultados como `region:global` , porque la palabra literal “global” no está asociada a los recursos globales. Si `global` se escribe como palabra clave, solo se muestran los recursos que tienen esa cadena literal asociada al recurso.
`resourcetype:`	El tipo de recurso en notación *`service`*`:`*`type`*. Resource Explorer incluye en los resultados únicamente los recursos que pertenecen a la cuenta especificada. `resourcetype:ec2:instance`
`resourcetype.supports:`	Este filtro le permite buscar recursos que admitan etiquetas. `tags`es el único valor admitido. El explorador de recursos incluye en los resultados solo los recursos que se pueden etiquetar. `resourcetype.supports:tags`
`service:`	El Servicio de AWS que está asociado al tipo de recurso. Resource Explorer incluye en los resultados únicamente los recursos que pertenecen a la cuenta especificada. `service:ec2`
`tag:`	Un par clave/valor de etiqueta expresado como `<key>=<value>` . Resource Explorer incluye en los resultados solo los recursos que tienen una etiqueta con una clave coincidente y el valor especificado. `tag:environment=production`

Nombre del filtro	Descripción y ejemplo
`tag:none`	Un caso especial del filtro `tag:` que permite buscar cualquier recurso que no tenga ninguna etiqueta creada por el usuario adjunta. **Note** Los recursos con etiquetas creadas por el servicio de AWS siguen apareciendo en los resultados de este filtro.
`tag.key:`	Una clave de etiqueta. Resource Explorer incluye en los resultados solo los recursos que tienen una etiqueta con una etiqueta coincidente, independi entemente del valor. `tag.key:environment`
`tag.value:`	Un valor de etiqueta. Resource Explorer incluye en los resultados solo los recursos que tienen una etiqueta con una clave coincidente, independi entemente del nombre de la clave. `tag.value:production`

Operadores de filtro

Puede modificar las palabras clave y los filtros incluyendo uno de los operadores que se muestran en la siguiente tabla como parte de la cadena.

Operador	Descripción y ejemplo
"*multiple word phrase*" o “*frase con guiones*”	Escriba una frase de varias palabras que deba tratarse como una sola palabra clave con comillas dobles (" "). Resource Explorer incluye solo los recursos que coinciden con la frase completa, con todas las palabras juntas y en el orden especificado. Si no usa comillas dobles, Resource Explorer divide la frase en sus component es mediante espacios o guiones e incluye los recursos que coinciden con los

Operador	Descripción y ejemplo

	componentes individuales, incluso si no están juntos o en un orden diferente. Las cotizaciones deben figurar en todo lo que aparece después del operador.
	
	`"This matches only resources with the whole sentence."`
	
	`This matches resources with any of the words.`
	
	`"us-east-1"` : solo coincide con los recursos que están asociados a esa región exacta.
	
	`us-east-1` : coincide con cualquier recurso que contenga las palabras “EE. UU.”, “este” o “1”.
	
	`-tag:"enviornment=production"`

keyword`*`	Coincidencia de prefijos con caracteres comodín. Puede colocar un carácter comodín (un asterisco `*`) únicamente al final de la cadena. Resource Explorer incluye en los resultados solo los recursos cuyos valores comiencen con el texto del prefijo antes de `*`. El siguiente ejemplo coincide con todos los Regiones de AWS que comienzan por. `us-east` `region:us-east*` **Important** La búsqueda unificada inserta automáticamente un operador de caracteres comodín (`*`) al final de la primera palabra clave de la cadena. Esto significa que los resultados de la búsqueda unificada incluyen recursos que coinciden con cualquier cadena que comience por la palabra clave especificada. La búsqueda realizada mediante el cuadro de texto Consulta de la página de Búsqueda de recursos de la consola de Resource Explorer no añade automáticamente un carácter comodín. Puede insertar un `*` manualmente después de cualquier término de la cadena de búsqueda.

Operador	Descripción y ejemplo

`-keyword`	Operador `Not`. Puede colocar un guion (`-`) al principio de su palabra clave o filtro para invertir los resultados de la búsqueda. Resource Explorer excluye de los resultados los recursos que coincidan con la palabra clave o el filtro que sigue a este operador. El siguiente ejemplo hace que todos los recursos asociados al servicio Amazon EC2 se excluyan de los resultados.
	
	`-service:ec2`
	
	Important
	
	Si utiliza el AWS CLI `search` comando y el valor del `--query-string` parámetro tiene el `-` operador como primer carácter, debe separar el nombre del parámetro de su valor con un signo igual (=) en lugar del habitual carácter de espacio. Si utiliza el carácter de espacio, la CLI malinterpreta la cadena. Por ejemplo, la siguiente consulta indica un error.
	
	`aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"`
	
	La siguiente consulta corregida, con un = que reemplaza el espacio, funciona según lo esperado.
	
	`aws resource-explorer-2 search --query-string ="-tag:none region:us-east-1"`
	
	Si cambia el orden de los filtros en la cadena de consulta para que `-` no sea el primer carácter del valor del parámetro, puede utilizar el carácter de espacio estándar. La siguiente cadena de consulta funciona.
	
	`aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"`

Operador	Descripción y ejemplo

`\<special character>`	Puede evitar los caracteres especiales que deben incluirse exactamente como se muestra en lugar de interpretarse. Si el texto incluye uno de los caracteres especiales (`* " - : = \`), debe colocarlo delante de una barra invertida (\) para asegurarse de que el carácter se interpreta literalmente. El siguiente ejemplo muestra cómo utilizar una palabra clave de texto de formato libre que incluya el carácter (`"my-key-word"`) de guion (`-`).
	
	Además, para evitar que Resource Explorer divida la expresión de los guiones en tres palabras clave distintas, puede escribir toda la frase entre comillas dobles.
	
	`"my\-key\-word"`
	
	Para insertar una barra invertida literal, inserte dos caracteres de barra invertida en una fila. La primera barra invertida se interpreta como el escape y la segunda barra invertida es el carácter literal que se debe insertar.
	
	`"some_text\\some_more_text"`

Note

Si la vista incluye las etiquetas adjuntas a los recursos, la operación `Search` no arroja errores de validación para las cadenas de búsqueda, ya que un filtro que no es válido también podría interpretarse como una búsqueda de texto de formato libre. Por ejemplo, aunque `cat:blue` parezca un filtro, Resource Explorer no puede analizarlo como tal porque `cat:` no es uno de los filtros definidos y válidos. En su lugar, Resource Explorer interpreta la cadena completa como una cadena de búsqueda de formato libre para permitir que coincida con elementos como el nombre de una clave de etiqueta o una parte de un ARN.
La operación arroja un error de validación si se da alguna de estas condiciones:

- La vista no incluye información sobre las etiquetas
- La consulta de búsqueda utiliza explícitamente un filtro de etiquetas (`tag.key:`, `tag.value:` o `tag:`)

Ejemplo de consultas de búsqueda del Explorador de recursos

En los ejemplos siguientes se muestra la sintaxis de los tipos de consultas comunes que puede utilizar en Explorador de recursos de AWS.

Important

Si usa el comando AWS CLI `search` y el valor del parámetro `--query-string` tiene el operador `-` como primer carácter, debe separar el nombre del parámetro de su valor con un signo igual (=) en lugar del carácter de espacio habitual. Si utiliza el carácter de espacio, la CLI malinterpretará la cadena. Por ejemplo, la siguiente consulta indica un error.

```
aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"
```

La siguiente consulta corregida, en la que = reemplaza el espacio, funciona según lo esperado.

```
aws resource-explorer-2 search --query-string="-tag:none region:us-east-1"
```

Si cambia el orden de los filtros en la cadena de consulta para que `-` no sea el primer carácter del valor del parámetro, puede utilizar el carácter de espacio estándar. La siguiente consulta funciona.

```
aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"
```

Buscar recursos sin etiquetar

Si quiere usar el control de acceso basado en atributos (ABAC) en su cuenta, utilizar una asignación basada en los costes o realizar una automatización basada en etiquetas en sus recursos, necesita saber qué recursos de su cuenta podrían carecer de etiquetas. En la siguiente consulta de ejemplo, se utiliza el filtro para casos especiales tag: none para mostrar todos los recursos a los que les faltan etiquetas generadas por los usuarios.

El filtro `tag:none` se aplica únicamente a las etiquetas creadas por el usuario. Las etiquetas generadas y mantenidas por AWS están exentas de este filtro y siguen apareciendo en los resultados.

```
tag:none
```

Para excluir también todas las etiquetas de sistema AWS creadas, añada un segundo filtro como se muestra en el ejemplo siguiente. El primer elemento de la cadena de consulta duplica el ejemplo anterior al filtrar todas las etiquetas creadas por los usuarios. Las etiquetas de sistema creadas por AWS siempre comienzan con las letras `aws`. Por lo tanto, puede utilizar el operador lógico NOT (-) con el filtro tag.key para excluir también los recursos que tengan una etiqueta cuyo nombre clave comience por `aws`.

```
tag:none -tag.key:aws*
```

Buscar recursos sin etiquetar

Para encontrar todos los recursos que tengan una etiqueta de cualquier tipo, puede usar el operador lógico NOT (-) con el filtro para casos especiales tag: none de la siguiente manera.

```
-tag:none
```

Buscar recursos a los que les falte una etiqueta específica

También en relación con ABAC, es posible que desee buscar todos los recursos que no tengan una etiqueta con una clave específica. En el siguiente ejemplo, se utiliza el operador lógico NOT - para proporcionar todos los recursos a los que les falta una etiqueta con el nombre de la clave `Department`.

```
-tag.key:Department
```

Buscar recursos que tengan valores de etiqueta no válidos

Por motivos de conformidad, es posible que desee buscar todos los recursos a los que les falten valores de etiqueta o que estén mal escritos en las etiquetas importantes. El siguiente ejemplo

proporciona todos los recursos que tengan una etiqueta con el nombre clave `environment`. Sin embargo, la consulta filtra cualquier recurso que tenga uno de los valores válidos `prod`, `integ` o `dev`. Los resultados que aparecen en esta consulta tienen algún otro valor que debe investigar y corregir.

> **Important**
>
> Las búsquedas del explorador de recursos no distinguen entre mayúsculas y minúsculas y no pueden distinguir entre nombres clave y valores que solo difieren por la forma en que se escriben en mayúscula. Por ejemplo, los valores del siguiente ejemplo coinciden con `PROD`, `prod`, `PrOd` o con cualquier variación. Sin embargo, algunas aplicaciones utilizan etiquetas que distinguen mayúsculas de minúsculas. Se recomienda estandarizar una estrategia de capitalización para su organización, por ejemplo, utilizando únicamente nombres y valores clave de etiquetas en minúscula. Un enfoque coherente puede ayudar a evitar la confusión que puede provocar tener etiquetas que solo se diferencien por la forma en que se escriben con mayúscula.

```
tag.key:environment -tag:environment=prod -tag:environment=integ -tag:environment=dev
```

Buscar recursos en un subconjunto de Regiones de AWS

Usa el operador comodín `'*'` para hacer coincidir todas las regiones de una zona determinada del mundo. El siguiente ejemplo devuelve todos los recursos que se encuentran en las regiones de Europa (UE).

```
region:eu-*
```

Buscar recursos globales

Utilice el valor `global` de casos especiales para el filtro `region:` para encontrar los recursos que se consideran globales y no están asociados a una región individual.

```
region:global
```

Busque recursos de un tipo determinado que estén ubicados en una región específica

Cuando se utilizan varios filtros, el explorador de recursos evalúa la expresión combinando los prefijos con los operadores lógicos implícitos AND. El ejemplo siguiente muestra que todos los recursos que se encuentran en la región Asia-Pacífico (Hong Kong) AND son instancias de Amazon EC2.

```
region:ap-east-1 resourcetype:ec2:instance
```

> **Note**
>
> Debido al AND implícito, solo puede utilizar correctamente un filtro para un atributo que pueda tener únicamente un valor asociado al recurso. Por ejemplo, un recurso solo puede formar parte de un Región de AWS. Por lo tanto, la consulta indica que no hay resultados.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Esta limitación no se aplica a los filtros de los atributos que pueden tener varios valores al mismo tiempo, como por ejemplo, `tag:`, `tag.key:` y `tag.value:`.

Buscar recursos que tengan un término de varias palabras

Escriba un término de varias palabras entre comillas dobles (") para obtener solo los resultados que contengan todo el término en el orden especificado. Sin comillas dobles, el explorador de recursos proporciona los recursos que coinciden con las palabras individuales que componen el término. Por ejemplo, en la siguiente consulta se utilizan comillas dobles para mostrar únicamente los recursos que coinciden con el término `"west wing"`. La consulta no coincide con los recursos de la región `us-west-2` Región de AWS (ni de ninguna otra región que incluya `west` en su código) ni con los recursos que coincidan con la palabra «ala» sin la palabra «oeste».

```
"west wing"
```

Buscar recursos que formen parte de una pila de CloudFormation específica

Cuando crea un recurso como parte de una pila AWS CloudFormation, todos se etiquetan automáticamente con el nombre de la pila. El siguiente ejemplo demuestra todos los recursos que se crearon como parte de la pila especificada.

```
tag:aws:cloudformation:stack-name=my-stack-name
```

Uso de la búsqueda unificada en la AWS Management Console

La AWS Management Console incluye una barra de búsqueda en la parte superior de cada página de la consola de AWS. Esta barra de búsqueda puede buscar la documentación y los temas del blog del Servicio de AWS, y llevarlo directamente a las páginas de la consola de servicio de AWS. También puede mostrar los recursos de su Cuenta de AWS, si activa la característica de búsqueda unificada mediante la activación de las funciones necesarias del explorador de recursos.

Con la búsqueda unificada, los usuarios pueden buscar recursos desde cualquier consola del Servicio de AWS sin tener que dirigirse primero a la consola Explorador de recursos de AWS.

> **Tip**
>
> Si desea utilizar la barra de búsqueda unificada para buscar recursos específicos, comience la consulta de búsqueda y escriba **`/Resources`**. Esto hace que los recursos de AWS ocupen una posición más alta en los resultados de la búsqueda que los resultados que no representan recursos.

Temas

> **Important**
>
> La búsqueda unificada inserta automáticamente un operador de caracteres comodín (*) al final de la primera palabra clave de la cadena. Esto significa que los resultados de la búsqueda unificada incluyen los recursos que coinciden con cualquier cadena que comienza con la palabra clave especificada.
> La búsqueda realizada mediante el cuadro de texto Consulta de la página de búsqueda de recursos de la consola del explorador de recursos no añade automáticamente un carácter comodín. Puede insertar un * manualmente después de cualquier término de la cadena de búsqueda.

Cómo comprobar que la búsqueda unificada se encuentra habilitada

Para ver si la búsqueda unificada se encuentra habilitada en su Cuenta de AWS, consulte la parte superior de la página Configuración. Allí, el explorador de recursos muestra el estado actual de cada requisito.. Los requisitos para la búsqueda unificada son los siguientes:

- Activar el explorador de recursos en al menos una Región de AWS. Solamente los recursos de las regiones con índices del explorador de recursos pueden aparecer en los resultados de búsqueda unificados.
- Crear un índice agregador en la región que elija. Las búsquedas realizadas en esta región arrojan los resultados de todas las regiones registradas en la cuenta.
- Crear una vista predeterminada en la región que contenga el índice agregador. Todos los usuarios que necesiten utilizar la búsqueda unificada de recursos deben tener permiso para usar esta vista predeterminada.
- Los usuarios deben tener una política de permisos AWS Identity and Access Management (IAM) asignada a su entidad principal de IAM que conceda permiso para realizar las acciones `resource-explorer-2:Get*`, `resource-explorer-2:List*`, `resource-explorer-2:Describe*`, `resource-explorer-2:Search`. Puede conceder estos permisos mediante el uso de sus propias políticas de IAM personalizadas. Estos permisos ya están incluidos como parte de las siguientes políticas gestionadas de AWS que están disponibles para su uso:
  - Acceso de solo lectura explorador de recursos de AWS
  - Acceso completo al explorador de recursos de AWS

Activar la búsqueda unificada

Para poder incluir los recursos de su cuenta en los resultados de la búsqueda unificada desde cualquier consola AWS, debe seguir los siguientes pasos:

1. Activar Explorador de recursos de AWS en una o más Regiones de AWS de su cuenta.
2. Registrar una región para incluir el índice agregador.
3. Crear una vista predeterminada en la región con el índice agregador.

Uso de AWS Chatbot para buscar recursos

Puede buscar y descubrir información sobre los Servicios de AWS y sus recursos de AWS haciendo preguntas en lenguaje AWS Chatbot natural. AWS Chatbot responde a las preguntas relacionadas con el servicio directamente en sus canales de chat con la documentación de AWS pertinente y extractos de artículos de soporte. AWS Chatbot utiliza Resource Explorer para buscar y encontrar respuestas a sus preguntas relacionadas con los recursos.

Para obtener más información, consulte ¿Qué es AWS Chatbot? en la Guía de administración de AWS Chatbot.

Preguntas sobre recursos de AWS

AWS Chatbot utiliza Resource Explorer para buscar y descubrir sus recursos. AWS Chatbot muestra los resultados de la búsqueda en una lista. Esta lista muestra los cinco recursos más coincidentes e incluye la posibilidad de filtrar aún más los resultados por tipo de recurso, Región de AWS y etiqueta.

Requisitos previos

Para hacer preguntas relacionadas con los recursos AWS Chatbot, debe hacer lo siguiente:

- Asegurarse de tener índices y vistas activos con al menos una vista predeterminada en su Región de AWS. Los índices y las vistas permiten a Resource Explorer catalogar y consultar sus recursos. Para obtener más información, consulte Términos y conceptos de Resource Explorer.
- Agrega la AWSResourceExplorerReadOnlyAccess política a tu rol de canal o a cada rol de usuario apropiado, según el esquema de permisos de tu canal.
- Comprueba que las políticas de protección de tu canal permiten AWSResourceExplorerReadOnlyAccess los permisos.

Preguntas frecuentes sobre los recursos

Puede hacer estas preguntas directamente desde sus canales de chat. Reemplace las palabras por texto rojo con su propia información.

```
@aws What services am I using in Region?

@aws What are the resources in my account with tags?
```

```
@aws What lambda functions do I have?
```

Seguridad en Explorador de recursos de AWS

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS 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 Servicios de AWS en Nube de AWS. Además, AWS 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 conformidad de . Para obtener información sobre los programas de conformidad que se aplican a Resource Explorer, consulte Servicios de AWS en el ámbito del programa de conformidad .
- Seguridad en la nube: su responsabilidad viene determinada por el Servicio de AWS 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 cuando se utiliza Explorador de recursos de AWS. Muestra cómo configurar Resource Explorer para satisfacer sus objetivos de seguridad y conformidad. También puede obtener información sobre cómo utilizar otros Servicios de AWS que le ayuden a monitorear y proteger los recursos de Resource Explorer.

Contenido

Administración de identidades y accesos en Explorador de recursos de AWS

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede estar autenticado (inició sesión) y autorizado (tiene permisos) para utilizar los recursos de Resource Explorer. IAM es un servicio de AWS que se puede utilizar sin cargo adicional.

Temas

Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que realice en Resource Explorer.

Usuario de servicio: si utiliza el servicio de Resource Explorer para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Resource Explorer para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Resource Explorer, consulte Solución de problemas de permisos Explorador de recursos de AWS.

Administrador de servicio: si está a cargo de los recursos de Resource Explorer en la empresa, probablemente tenga acceso completo a Resource Explorer. Su trabajo consiste en determinar a qué características y recursos de Resource Explorer deben acceder los usuarios del servicio. Luego,

debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Resource Explorer, consulte Cómo funciona Resource Explorer con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Resource Explorer. Para consultar ejemplos de políticas basadas en identidades de Resource Explorer que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidad de Explorador de recursos de AWS.

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como el Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad de AWS IAM Identity Center. Los usuarios (del Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la AWS Management Console o en el portal de acceso a AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre la firma de solicitudes, consulte Firma de solicitudes API de AWS en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS Single Sign-On y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Usuario raíz de cuenta de AWS

Cuando se crea una cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Usuarios y grupos

Un usuario de IAM es una identidad en su Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del Usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles

Un rol de IAM es una identidad de tu cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Consolecambiando de roles. Puede asumir un

rol llamando a una operación de AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del Usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del Usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. El IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede asociar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
  - Reenviar sesiones de acceso (FAS): cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos

para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un servicio de AWS en la Guía del usuario de IAM.
- Rol vinculado a servicios: un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del Usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de las políticas JSON en la Guía del Usuario de IAM.

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

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del usuario de la consola, AWS CLI o la API de AWS.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede vincular a una identidad, como un usuario, grupo o rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política en función de identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para obtener más información acerca de cómo elegir una política administrada o una política insertada, consulte Elección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM 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. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios de AWS.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas por AWS en una política basada en recursos.

Explorador de recursos de AWS no admite políticas basadas en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de política JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para Desarrolladores de Amazon Simple Storage Service.

Explorador de recursos de AWS no admite las ACL.

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política en función de identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del Usuario de IAM.
- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada rootlong. Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidad del

rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del Usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información sobre cómo AWS decide si permite o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Resource Explorer con IAM

Antes de utilizar IAM para administrar el acceso a Explorador de recursos de AWS, debe comprender qué características de IAM están disponibles para su uso con Resource Explorer. Para obtener una perspectiva general sobre cómo funciona Resource Explorer y otros Servicios de AWS con IAM, consulte los Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Temas

- Políticas basadas en identidades de Resource Explorer
- Autorización basada en etiquetas de Resource Explorer
- Roles de IAM en Resource Explorer

Como cualquier otroServicio de AWS, Resource Explorer requiere permisos para usar sus operaciones e interactuar con sus recursos. Para hacer una búsqueda, los usuarios deben tener permiso para recuperar los detalles de una vista y también para buscar mediante la vista. Para crear índices o vistas, o para modificarlos o modificar cualquier otra configuración de Resource Explorer, debe contar con permisos adicionales.

Asigne políticas de IAM basadas en la identidad que concedan esos permisos a las entidades principales de IAM correspondientes. Resource Explorer proporciona varias políticas administradas que predefinen conjuntos de permisos comunes. Puede asignarlos a sus entidades principales de IAM.

Políticas basadas en identidades de Resource Explorer

Con las políticas basadas en identidades de IAM, usted puede especificar las acciones permitidas o denegadas con respecto a recursos específicos, y las condiciones en las que se permiten o deniegan

dichas acciones. Resource Explorer admite acciones específicas, recursos y claves de condición. Para obtener más información acerca de los elementos que utiliza en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Acciones

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. 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 de políticas en Resource Explorer utilizan el prefijo de servicio `resource-explorer-2` antes de la acción. Por ejemplo, para conceder a alguien permiso para buscar mediante una vista, con la operación de `Search` de API de Resource Explorer, debe incluir la acción `resource-explorer-2:Search` en una política asignada a esa entidad principal. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Resource Explorer define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio. Estas se alinean con las operaciones de API de Resource Explorer.

Para especificar varias acciones en una única instrucción, sepárelas con comas como se muestra en el siguiente ejemplo.

```
"Action": [
      "resource-explorer-2:action1",
      "resource-explorer-2:action2"
]
```

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

```
"Action": "resource-explorer-2:Describe*"
```

Para ver una lista de las acciones de Resource Explorer, consulte Acciones definidas por Explorador de recursos de AWS en la Referencia de autorizaciones de servicio de AWS.

Recursos

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

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el 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": "*"
```

Vista

El tipo de recurso principal de Resource Explorer es la vista.

La vista de Resource Explorer tiene el siguiente formato ARN.

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${unique-id}
```

El formato ARN de Resource Explorer se muestra en el ejemplo a continuación.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-Search-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> El ARN de una vista incluye un identificador único al final para garantizar que cada vista sea única. Esto ayuda a garantizar que una política de IAM que permitió el acceso a una vista anterior eliminada no se pueda utilizar para conceder accidentalmente el acceso a una nueva vista que, por casualidad, tenga el mismo nombre que la vista anterior. Cada nueva vista recibe un ID nuevo y único al final para garantizar que los ARN nunca se reutilicen.

Para obtener más información acerca del formato de los ARN, consulte Nombres de recursos de Amazon (ARN).

Utilice las políticas de IAM basadas en identidades asignadas a las entidades principales de IAM y especifique la vista como `Resource`. De este modo, podrá conceder el acceso de búsqueda a través de una vista a un conjunto de entidades principales y el acceso a través de una vista completamente diferente a un conjunto diferente de entidades principales.

Por ejemplo, para conceder permiso a una vista única denominada `ProductionResourcesView` en una instrucción de política de IAM, primero obtenga el nombre de recurso de Amazon (ARN) de la vista. Puede utilizar la página Vistas de la consola para ver los detalles de una vista o invocar la operación `ListViews` para recuperar el ARN completo de la vista que desee. A continuación, inclúyala en una instrucción de política, como la que se muestra en el siguiente ejemplo, que concede permiso para modificar la definición de una sola vista.

```
"Effect": "Allow",
"Action": "UpdateView",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
ProductionResourcesView/<unique-id>"
```

Para permitir las acciones en todas las vistas que pertenezcan a una cuenta determinada, utilice el carácter comodín (*) en la parte correspondiente del ARN. En el siguiente ejemplo, se concede permiso de búsqueda a todas las vistas en una Región de AWS y cuenta específica.

```
"Effect": "Allow",
"Action": "Search",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*"
```

Algunas acciones de Resource Explorer, como `CreateView`, no se realizan en un recurso específico porque, como en el ejemplo siguiente, el recurso aún no existe. En dichos casos, debe utilizar el carácter comodín (*) para todo el ARN del recurso.

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "*"
```

Si especifica una ruta que termina en un carácter comodín, puede restringir la operación `CreateView` a la creación de vistas con solo la ruta aprobada. El siguiente ejemplo de política muestra cómo permitir que la entidad principal cree vistas solo en la ruta`view/ProductionViews/`.

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/ProductionViews/*""
```

Índice

Otro tipo de recurso que puede utilizar para controlar el acceso a la funcionalidad de Resource Explorer es el índice.

La forma principal en la que puede interactuar con el índice es activar Resource Explorer en una Región de AWS mediante la creación de un índice en esa región. Después de eso, casi todo lo demás se hace interactuando con la vista.

Algo que puede hacer con el índice es controlar quién puede crear vistas en cada región.

> **Note**
>
> Tras crear una vista, IAM autoriza todas las demás acciones de visualización únicamente para el ARN de la vista y no para el índice.

El índice tiene un ARN que se puede referenciar en una política de permisos. El ARN de un índice de Resource Explorer tiene el siguiente formato.

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${unique-id}
```

El siguiente ejemplo muestra el ARN de un índice de Resource Explorer.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd22222222
```

Algunas acciones de Resource Explorer comprueban la autenticación con varios tipos de recursos. Por ejemplo, la operación CreateView sirve de autorización tanto para el ARN del índice como para el ARN de la vista, tal como será después de que Resource Explorer la cree. Para concederles a los administradores el permiso de administrar el servicio Resource Explorer, puede usar `"Resource": "*"` para autorizar acciones para cualquier recurso, índice o vista.

Como alternativa, puede restringir a una entidad principal para que solo pueda trabajar con recursos específicos de Resource Explorer. Por ejemplo, para limitar las acciones solo a los recursos de

Resource Explorer en una región específica, puede incluir una plantilla de ARN que coincida tanto con el índice como con la vista, pero que se aplique solo a una región. En el siguiente ejemplo, el ARN coincide con ambos índices o vistas solo en la región `us-west-2` de la cuenta específica. Especifique la región en el tercer campo del ARN, pero utilice un carácter comodín (*) en el último campo para que coincida con cualquier tipo de recurso.

```
"Resource": "arn:aws:resource-explorer-2:us-west-2:123456789012:*
```

Para obtener más información, consulte Acciones definidas por Explorador de recursos de AWS en la Referencia de autorizaciones de servicio de AWS. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recursos, consulte Acciones definidas por Explorador de recursos de AWS.

Claves de condición

Resource Explorer no proporciona ninguna clave de condición específica del servicio, pero sí admite el uso de algunas claves de condición globales. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

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

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación lógica `OR`. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para obtener más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Para ver una lista de las claves de condición que puede usar con Resource Explorer, consulte las Claves de condición para Explorador de recursos de AWS en la Referencia de autorización de servicio de AWS. Para obtener más información sobre las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Explorador de recursos de AWS.

Ejemplos

Para ver ejemplos de políticas basadas en identidades de Resource Explorer, consulte Ejemplos de políticas basadas en identidad de Explorador de recursos de AWS.

Autorización basada en etiquetas de Resource Explorer

Puede adjuntar etiquetas a los recursos de Resource Explorer o transferirlas en una solicitud a Resource Explorer. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `resource-explorer-2:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`. Para obtener más información acerca de cómo etiquetar los recursos de Resource Explorer, consulte Agregar etiquetas a vistas. Para utilizar la autorización basada en etiquetas en Resource Explorer, consulteUso de una autorización basada en etiquetas para controlar el acceso a sus vistas.

Roles de IAM en Resource Explorer

Un rol de IAM es una entidad principal dentro de su Cuenta de AWS que dispone de permisos específicos.

Uso de credenciales temporales con Resource Explorer

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen mediante una llamada a operaciones de la API de AWS Security Token Service (AWS STS), como AssumeRole o GetFederationToken.

Resource Explorer admite el uso de credenciales temporales

Roles vinculados a servicios

Los roles vinculados a servicios permiten a los Servicios de AWS obtener acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Resource Explorer utiliza roles vinculados a servicios para realizar su trabajo. Para obtener información detallada sobre los roles vinculados a servicios de Resource Explorer, consulte Uso de roles vinculados a servicios para Resource Explorer.

Ejemplos de políticas basadas en identidad de Explorador de recursos de AWS

De forma predeterminada, las entidades principales de AWS Identity and Access Management (IAM), como los roles, los grupos y los usuarios, no tienen permiso para crear ni modificar los recursos de Resource Explorer. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Un administrador de IAM debe crear políticas de IAM que concedan permiso a las entidades principales para realizar determinadas operaciones de API en los recursos especificados que necesiten. Después, el administrador debe asignar esas políticas a las entidades principales de IAM que necesiten esos permisos.

Para proporcionar acceso, agregue permisos a sus usuarios, grupos o roles:

- Usuarios y grupos de AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Create a permission set (Creación de un conjunto de permisos) en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda asumir. Siga las instrucciones de Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones de Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

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

Temas

- Prácticas recomendadas relativas a políticas
- Uso de la consola de Resource Explorer
- Otorgar acceso a una vista basada en etiquetas
- Otorgar acceso para crear una vista basada en etiquetas
- Permitir a las entidades principales consultar sus propios permisos

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Resource Explorer de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidad:

- Comience con las políticas administradas por AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en la Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, 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. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía de usuario de IAM.
- Use condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar 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 utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política JSON de IAM: condición en la Guía del usuario de IAM.
- Use el Analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el Analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas

recomendadas de IAM. IAM Access Analyzer proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para obtener más información, consulte la política de validación del Analizador de acceso de IAM en la Guía de usuario de IAM.

- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de MFA a sus políticas. Para obtener más información, consulte Configuración de acceso a una API protegida por MFA en la Guía de usuario de IAM.

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

Uso de la consola de Resource Explorer

Para que las entidades principales puedan realizar búsquedas en la consola de Explorador de recursos de AWS, deben tener un conjunto mínimo de permisos. Si usted no crea una política basada en identidad con los permisos mínimos necesarios, la consola de Resource Explorer no funcionará del modo esperado para las entidades principales de la cuenta.

Puede usar la política administrada de AWS llamada `AWSResourceExplorerReadOnlyAccess` para permitir el uso de la consola de Resource Explorer para realizar búsquedas con cualquier vista de la cuenta. Para conceder permisos de búsqueda con una sola vista, consulte Otorgar acceso a las vistas de Resource Explorer para la búsqueda y los ejemplos de las dos secciones siguientes.

No es necesario conceder permisos mínimos para la consola a las entidades principales que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, puede optar por conceder acceso solo a las acciones que coincidan con las operaciones de la API que deben realizar las entidades principales.

Otorgar acceso a una vista basada en etiquetas

En este ejemplo, usted desea conceder acceso a una vista de Resource Explorer en su Cuenta de AWS a las entidades principales de la cuenta. Para hacerlo, asigne políticas de IAM basadas en la identidad a las entidades principales que desee poder buscar en Resource Explorer. El siguiente ejemplo de política de IAM permite el acceso a cualquier solicitud en la que la etiqueta del `Search-Group` adjunta a la entidad principal que realiza la llamada coincida exactamente con el valor de la misma etiqueta adjunta a la vista que se usó en la solicitud.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:*:*:view/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Search-Group": "${aws:PrincipalTag/
Search-Group}"}
            }
        }
    ]
}
```

También puede asignar esta política a las entidades principales de IAM en su cuenta. Si una entidad principal con la etiqueta `Search-Group=A` intenta realizar una búsqueda mediante una vista de Resource Explorer, la vista también debe tener la etiqueta `Search-Group=A`. Si no es así, se le denegará el acceso a la entidad principal. La clave de la etiqueta de condición `Search-Group` coincide con los nombres de las claves de condición `Search-group` y `search-group` porque no distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condition en la Guía del usuario de IAM.

> **Important**
>
> Para ver sus recursos en los resultados de búsqueda unificados en la AWS Management Console, las entidades principales deben tener los permisos de `GetView` y `Search` para la vista predeterminada en Región de AWS que contiene el índice agregador. La forma más sencilla de conceder esos permisos es dejar el permiso basado en recursos predeterminado que estaba adjunto a la vista al activar Resource Explorer mediante la instalación rápida o avanzada.
>
> En este caso, podría considerar configurar la vista predeterminada para filtrar los recursos confidenciales y, a continuación, configurar vistas adicionales a las que conceder acceso basado en etiquetas, como se describe en el ejemplo anterior.

Otorgar acceso para crear una vista basada en etiquetas

En este ejemplo, le sugerimos permitir que solo las entidades principales que estén etiquetadas de la misma manera que el índice puedan crear vistas en la Región de AWS que contiene el índice. Para hacerlo, cree permisos basados en la identidad para permitir que las entidades principales realicen búsquedas con las vistas.

Ahora ya puede conceder permisos para crear una vista. Puede añadir las instrucciones de este ejemplo a la misma política de permisos que utiliza para conceder permisos `Search` a las entidades principales correspondientes. Las acciones se permiten o deniegan en función de las etiquetas adjuntas a las entidades principales que realizan la llamada a las operaciones y al índice a los que se va a asociar la vista. En el siguiente ejemplo, la política de IAM deniega cualquier solicitud para crear una vista cuando el valor de la etiqueta `Allow-Create-View` adjunta a la entidad principal del intermediario no coincide exactamente con el valor de la misma etiqueta adjunta al índice de la región en la que se crea la vista.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "resource-explorer-2:CreateView",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {"aws:ResourceTag/Allow-Create-View":
 "${aws:PrincipalTag/Allow-Create-View}"}
            }
        }
    ]
}
```

Permitir a las entidades principales consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se adjuntan a la identidad de sus usuarios. Esta política incluye permisos para llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de 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": "*"
        }
    ]
}
```

Ejemplos de políticas de control de servicios para AWS Organizations y Resource Explorer

Explorador de recursos de AWS admite políticas de control de servicios (SCP). Las SCP son políticas que se asocian a elementos de una organización para administrar los permisos dentro de esa organización. Un SCP se aplica a todos los miembros Cuentas de AWS de una organización que estén bajo el elemento al que se asocie el SCP. Las políticas de control de servicios (SCP) permiten un control centralizado de los máximos permisos disponibles para todas las cuentas de la organización. Pueden ayudarlo a garantizar que se Cuentas de AWS mantenga dentro de las pautas de control de acceso de su organización. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .

Requisitos previos

Para usar políticas de control de servicios, primero debe hacer lo siguiente:

- Habilitar todas las características en la organización. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations .
- Habilite las SCP para utilizar en su organización. Para obtener más información, consulte Activación y desactivación de los tipos de políticas en la Guía del usuario de AWS Organizations .
- Cree las SCP que sean necesarias. Para obtener más información sobre cómo crear SCP, consulte Crear y actualizar SCP en la Guía del usuario de AWS Organizations .

Ejemplo de políticas de control de servicios

En el siguiente ejemplo, se muestra cómo puede utilizar el control de acceso basado en atributos (ABAC) para controlar el acceso a las operaciones administrativas de Resource Explorer. Este ejemplo de política deniega el acceso a todas las operaciones de Resource Explorer, a excepción de los dos permisos necesarios para realizar búsquedas, `resource-explorer-2:Search` y `resource-explorer-2:GetView`, a menos que la entidad principal de IAM que realiza la solicitud reciba la etiqueta `ResourceExplorerAdmin=TRUE`. Para obtener una explicación más completa sobre el uso de ABAC con Resource Explorer, consulte Uso de una autorización basada en etiquetas para controlar el acceso a sus vistas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
```

```
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView""
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
          "StringNotEqualsIgnoreCase": {"aws:PrincipalTag/ResourceExplorerAdmin":
 "TRUE"}
      }
   ]
}
```

AWS políticas gestionadas para Explorador de recursos de AWS

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Políticas AWS administradas generales que incluyen permisos de Resource Explorer

- AdministratorAccess— Otorga acceso completo a los recursos Servicios de AWS y a los mismos.

- ReadOnlyAcceso: otorga acceso de solo lectura a los recursos Servicios de AWS y recursos.
- ViewOnlyAcceso: otorga permisos para ver los recursos y los metadatos básicos de. Servicios de AWS

> **Note**
>
> Los permisos de `Get*` de Resource Explorer incluidos en la política de `ViewOnlyAccess` funcionan igual que los permisos `List`, aunque solo devuelven un valor único ya que una región solo puede contener un índice y una vista predeterminada.

AWS políticas administradas para Resource Explorer

- AWSResourceExplorerFullAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy

AWS política gestionada: AWSResourceExplorerFullAccess

Puede asignar la política de `AWSResourceExplorerFullAccess` a las identidades de IAM.

Esta política otorga permisos que permiten un control administrativo total del servicio de Resource Explorer. Puede realizar todas las tareas relacionadas con la activación y la administración de Resource Explorer en las Regiones de AWS en su cuenta.

Detalles de los permisos

Esta política incluye permisos que permiten realizar todas las acciones del Explorador de recursos, como activar y desactivar el Explorador de recursos Regiones de AWS, crear o eliminar un índice agregador para la cuenta, crear, actualizar y eliminar vistas y realizar búsquedas. Esta política también incluye permisos que no forman parte de Resource Explorer:

- `ec2:DescribeRegions`: permite a Resource Explorer acceder a información detallada sobre las regiones de su cuenta.
- `ram:ListResources`: permite a Resource Explorer enumerar los recursos compartidos de los que forman parte los recursos.
- `ram:GetResourceShares`: permite a Resource Explorer identificar detalles sobre los recursos compartidos que le pertenecen o que se comparten con usted.

- `iam:CreateServiceLinkedRole`: permite a Resource Explorer crear el rol vinculado al servicio necesario al activar Resource Explorer mediante la creación del primer índice.
- `organizations:DescribeOrganization`: permite a Resource Explorer acceder a información sobre su organización.

Para ver la versión más reciente de esta política AWS administrada, consulte la Guía *AWSResourceExplorerFullAccess* de referencia de políticas AWS administradas.

AWS política gestionada: AWSResourceExplorerReadOnlyAccess

Puede asignar la política de `AWSResourceExplorerReadOnlyAccess` a las identidades de IAM.

Esta política concede permisos de solo lectura que brindan a los usuarios acceso a búsqueda básica para divulgar sus recursos.

Detalles de los permisos

Esta política incluye permisos que les permiten a los usuarios utilizar las operaciones de `Get*`, `List*` y `Search` de Resource Explorer para ver información sobre los componentes y los ajustes de configuración de Resource Explorer, pero no permite que los usuarios los cambien. Los usuarios también pueden realizar búsquedas. Esta política también incluye dos permisos que no forman parte de Resource Explorer:

- `ec2:DescribeRegions`: permite a Resource Explorer acceder a información detallada sobre las regiones de su cuenta.
- `ram:ListResources`: permite a Resource Explorer enumerar los recursos compartidos de los que forman parte los recursos.
- `ram:GetResourceShares`: permite a Resource Explorer identificar detalles sobre los recursos compartidos que le pertenecen o que se comparten con usted.
- `organizations:DescribeOrganization`: permite a Resource Explorer acceder a información sobre su organización.

Para ver la versión más reciente de esta política AWS gestionada, consulte `AWSResourceExplorerReadOnlyAccess` la Guía de referencia de políticas AWS gestionadas.

AWS política gestionada: AWSResourceExplorerServiceRolePolicy

No puede adjuntar `AWSResourceExplorerServiceRolePolicy` a ninguna entidad IAM usted mismo. Esta política puede estar adjunta solamente a un rol vinculado a servicios que permita a Resource Explorer realizar acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios para Resource Explorer.

Esta política concede los permisos necesarios para que Resource Explorer recupere información sobre sus recursos. El explorador de recursos rellena los índices que mantiene en cada uno de los Región de AWS que registre.

Para ver la versión más reciente de esta política AWS administrada, consulte `AWSResourceExplorerServiceRolePolicy` en la consola de IAM.

AWS política gestionada: AWSResourceExplorerOrganizationsAccess

Puede asignar `AWSResourceExplorerOrganizationsAccess` a sus identidades de IAM.

Esta política otorga permisos administrativos al Explorador de recursos y otorga permisos de solo lectura a otros Servicios de AWS para respaldar este acceso. El AWS Organizations administrador necesita estos permisos para configurar y administrar la búsqueda de varias cuentas en la consola.

Detalles de los permisos

Esta política incluye permisos que les permiten a los administradores configurar la búsqueda de varias cuentas para la organización:

- `ec2:DescribeRegions`: permite a Resource Explorer acceder a información detallada sobre las regiones de su cuenta.
- `ram:ListResources`: permite a Resource Explorer enumerar los recursos compartidos de los que forman parte los recursos.
- `ram:GetResourceShares`: permite que Resource Explorer identifique detalles sobre los recursos compartidos que le pertenecen o que se comparten con usted.
- `organizations:ListAccounts`: permite a Resource Explorer identificar las cuentas dentro de una organización.
- `organizations:ListRoots`: permite a Resource Explorer identificar las cuentas raíz dentro de una organización.
- `organizations:ListOrganizationalUnitsForParent`: permite a Resource Explorer identificar las unidades organizativas (UO) de una unidad organizativa principal o raíz.

- `organizations:ListAccountsForParent`: permite a Resource Explorer identificar las cuentas de una organización que se encuentran contenidas en la raíz de destino especificada o en una UO.
- `organizations:ListDelegatedAdministrators`— Permite que Resource Explorer identifique las AWS cuentas designadas como administradores delegados en esta organización.
- `organizations:ListAWSServiceAccessForOrganization`— Permite a Resource Explorer identificar una lista de las Servicios de AWS que están habilitadas para integrarse con su organización.
- `organizations:DescribeOrganization`: permite a Resource Explorer recuperar información sobre la organización a la que pertenece la cuenta del usuario.
- `organizations:EnableAWSServiceAccess`— Permite que Resource Explorer habilite la integración de un Servicio de AWS (el servicio especificado por`ServicePrincipal`) con AWS Organizations.
- `organizations:DisableAWSServiceAccess`— Permite que Resource Explorer deshabilite la integración de un Servicio de AWS (el servicio especificado por ServicePrincipal) con AWS Organizations.
- `organizations:RegisterDelegatedAdministrator`— Permite que Resource Explorer habilite la cuenta de miembro especificada para administrar las funciones de la organización del AWS servicio especificado.
- `organizations:DeregisterDelegatedAdministrator`— Permite a Resource Explorer eliminar al miembro especificado Cuenta de AWS como administrador delegado del miembro especificado Servicio de AWS.
- `iam:GetRole`: permite a Resource Explorer recuperar información sobre el rol especificado, incluidos la ruta del rol, GUID, ARN y la política de confianza del rol que concede permiso para asumirlo.
- `iam:CreateServiceLinkedRole`: permite a Resource Explorer crear el rol vinculado al servicio necesario al activar Resource Explorer mediante la creación del primer índice.

Para ver la versión más reciente de esta política AWS gestionada, consulte `AWSResourceExplorerOrganizationsAccess` en la consola de IAM.

Resource Explorer actualiza las políticas AWS administradas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas para Resource Explorer desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas

automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Resource Explorer.

Cambio	Descripción	Fecha
AWSResourceExplorerServiceRolePolicy- Se actualizaron los permisos de las políticas para ver otros tipos de recursos	Resource Explorer agregó permisos a la política de roles vinculados al servicio AWSResourceExplorerServiceRolePolicy que permiten a Resource Explorer ver otros tipos de recursos: • apprunner:ListVpcConnectors • backup:ListReportPlans • emr-serverless:ListApplications • events:ListEventBuses • geo:ListPlaceIndexes • geo:ListTrackers • greengrass:ListComponents • greengrass:ListComponentVersions • iot:ListRoleAliases • iottwinmaker:ListComponentTypes • iottwinmaker:ListEntities	12 de diciembre de 2023

Cambio	Descripción	Fecha
	• iottwinmaker:ListScenes • kafka:ListConfigurations • kms:ListKeys • kinesisanalytics:ListApplications • lex:ListBots • lex:ListBotAliases • mediapackage-vod:ListPackagingConfigurations • mediapackage-vod:ListPackagingGroups • mq:ListBrokers • personalize:ListDatasetGroups • personalize:ListDatasets • personalize:ListSchemas • route53:ListHealthChecks • route53:ListHostedZones • secretsmanager:ListSecrets	

Cambio	Descripción	Fecha
Nueva política administrada por	Resource Explorer agregó la siguiente política AWS administrada: • AWSResourceExplorerOrganizationsAccess	14 de noviembre de 2023
Actualización de la políticas administradas	Resource Explorer actualizó las siguientes políticas AWS administradas para permitir la búsqueda en varias cuentas: • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess	14 de noviembre de 2023

Cambio	Descripción	Fecha
AWSResourceExplorerServiceRolePolicy— Política actualizada para admitir la búsqueda de múltiples cuentas con Organizations	Resource Explorer agregó permisos a la política de roles vinculados al servicio AWSResourceExplorerServiceRolePolicy que permite que Resource Explorer admita la búsqueda en varias cuentas con Organizations: • `organizations:ListAWSServiceAccessForOrganization` • `organizations:DescribeAccount` • `organizations:DescribeOrganization` • `organizations:ListAccounts` • `organizations:ListDelegatedAdministrators`	14 de noviembre de 2023

Cambio	Descripción	Fecha
AWSResourceExplorerServiceRolePolicy— Política actualizada para admitir tipos de recursos adicionales	Resource Explorer agregó permisos a la política de roles vinculados al servicio de AWSResourceExplorerServiceRolePolicy que permiten al servicio indexar los siguientes tipos de recursos: • accessanalyzer:analyzer • acmpca:certificateauthority • amplify:app • amplify:backendenvironment • amplify:branch • amplify:domainassociation • amplifyuibuilder:component • amplifyuibuilder:theme • appintegrations:eventintegration • apprunner:service • appstream:appblock • appstream:application • appstream:fleet • appstream:imagebuilder • appstream:stack • appsync:graphqlapi • aps:rulegroupsnamespace • aps:workspace • apigateway:restapi • apigateway:deployment	17 de octubre de 2023

Cambio	Descripción	Fecha
	• athena:datacatalog • athena:workgroup • autoscaling:autoscalinggroup • backup:backupplan • batch:computeenvironment • batch:jobqueue • batch:schedulingpolicy • cloudformation:stack • cloudformation:stackset • cloudfront:fieldlevelencryptionconfig • cloudfront:fieldlevelencryptionprofile • cloudfront:originaccesscontrol • cloudtrail:trail • codeartifact:domain • codeartifact:repository • codecommit:repository • codeguruprofiler:profilinggroup • codestarconnections:connection • databrew:dataset • databrew:recipe • databrew:ruleset • detective:graph • directoryservices:directory • ec2:carriergateway	

Cambio	Descripción	Fecha
	• ec2:verifiedaccessendpoint • ec2:verifiedaccessgroup • ec2:verifiedaccessinstance • ec2:verifiedaccesstrustprovider • ecr:repository • elasticache:cachesecuritygroup • elasticfilesystem:accesspoint • events:rule • evidently:experiment • evidently:feature • evidently:launch • evidently:project • finspace:environment • firehose:deliverystream • faultinjectionsimulator:experimenttemplate • forecast:datasetgroup • forecast:dataset • frauddetector:detector • frauddetector:entitytype • frauddetector:eventtype • frauddetector:label • frauddetector:outcome • frauddetector:variable • gamelift:alias • globalaccelerator:accelerator	

Cambio	Descripción	Fecha
	• globalaccelerator:endpointgroup • globalaccelerator:listener • glue:database • glue:job • glue:table • glue:trigger • greengrass:group • healthlake:fhirdatastore • iam:virtualmfadevice • imagebuilder:componentbuildversion • imagebuilder:component • imagebuilder:containerrecipe • imagebuilder:distributionconfiguration • imagebuilder:imagebuildversion • imagebuilder:imagepipeline • imagebuilder:imagerecipe • imagebuilder:image • imagebuilder:infrastructureconfiguration • iot:authorizer • iot:jobtemplate • iot:mitigationaction • iot:provisioningtemplate • iot:securityprofile • iot:thing	

Cambio	Descripción	Fecha
	• iot:topicruledestination • iotanalytics:channel • iotanalytics:dataset • iotanalytics:datastore • iotanalytics:pipeline • iotevents:alarmmodel • iotevents:detectormodel • iotevents:input • iotsitewise:assetmodel • iotsitewise:asset • iotsitewise:gateway • iottwinmaker:workspace • ivs:channel • ivs:streamkey • kafka:cluster • kinesisvideo:stream • lambda:alias • lambda:layerversion • lambda:layer • lookoutmetrics:alert • lookoutvision:project • mediapackage:channel • mediapackage:origi nendpoint • mediatailor:playbackconfigu ration • memorydb:acl • memorydb:cluster • memorydb:parametergroup	

Cambio	Descripción	Fecha
	• memorydb:user • mobiletargeting:app • mobiletargeting:segment • mobiletargeting:template • networkfirewall:firewallpolicy • networkfirewall:firewall • networkmanager:glo balnetwork • networkmanager:device • networkmanager:link • networkmanager:attachment • networkmanager:cor enetwork • panorama:package • qldb:journalkinesisstreamsf orledger • qldb:ledger • rds:bluegreendeployment • refactorspaces:application • refactorspaces:environment • refactorspaces:route • refactorspaces:service • rekognition:project • resiliencehub:app • resiliencehub:resiliencypol icy • resourcegroups:group • route53:recoverygroup • route53:resourceset • route53:firewalldomain	

Cambio	Descripción	Fecha
	• route53:firewallrulegroup • route53:resolverendpoint • route53:resolverrule • sagemaker:model • sagemaker:notebook instance • signer:signingprofile • ssmincidents:responseplan • ssm:inventoryentry • ssm:resourcedatasync • states:activity • timestream:database • wisdom:assistant • wisdom:assistantassociation • wisdom:knowledgebase	

Cambio	Descripción	Fecha
AWSResourceExplorerServiceRolePolicy— Política actualizada para admitir tipos de recursos adicionales	Resource Explorer agregó permisos a la política de roles vinculados al servicio de AWSResourceExplorerServiceRolePolicy que permiten al servicio indexar los siguientes tipos de recursos: • codebuild:project • codepipeline:pipeline • cognito:identitypool • cognito:userpool • ecr:repository • efs:filesystem • elasticbeanstalk:application • elasticbeanstalk:applicationversion • elasticbeanstalk:environment • iot:policy • iot:topicrule • stepfunctions:statemachine • s3:bucket	1 de agosto de 2023

Cambio	Descripción	Fecha
AWSResourceExplorerServiceRolePolicy— Política actualizada para admitir tipos de recursos adicionales	Resource Explorer agregó permisos a la política de roles vinculados al servicio de `AWSResourceExplorerServiceRolePolicy` que permiten al servicio indexar los siguientes tipos de recursos: • elasticache:cluster • elasticache:globalreplicationgroup • elasticache:parametergroup • elasticache:replicationgroup • elasticache:reserved-instance • elasticache:snapshot • elasticache:subnetgroup • elasticache:user • elasticache:usergroup • lambda:code-signing-config • lambda:event-source-mapping • sqs:queue	7 de marzo de 2023

Cambio	Descripción	Fecha
Nuevas políticas administradas	Resource Explorer agregó las siguientes políticas AWS administradas: • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess • AWSResourceExplorerServiceRolePolicy	7 de noviembre de 2022
Resource Explorer comenzó hacer seguimiento de los cambios	Resource Explorer comenzó a realizar un seguimiento de los cambios de sus políticas AWS administradas.	7 de noviembre de 2022

Uso de roles vinculados a servicios para Resource Explorer

Explorador de recursos de AWS utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Resource Explorer. Los roles vinculados a servicios están predefinidos por Resource Explorer e incluyen todos los permisos que el servicio requiere para llamar a otros Servicios de AWS en su nombre.

Un rol vinculado a un servicio simplifica la configuración de Resource Explorer porque ya no tendrá que agregar manualmente los permisos necesarios. Resource Explorer define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos; dicha política de permisos no se puede asignar a ninguna otra entidad de IAM.

Para obtener más información sobre otros servicios que admiten los roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM. Allí, busque los servicios para los que se indique Sí en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de roles vinculados a servicios para Resource Explorer

Resource Explorer usa el rol vinculado a servicios denominado `AWSServiceRoleForResourceExplorer`. Este rol otorga permisos al servicio Resource Explorer para ver los recursos y eventos AWS CloudTrail que usted tiene en su Cuenta de AWS en su nombre e indexar esos recursos para facilitar las búsquedas.

El rol vinculado a un servicio de `AWSServiceRoleForResourceExplorer` confía solo en el servicio con la siguiente entidad principal para que asuma el rol:

- `resource-explorer-2.amazonaws.com`

La política de permisos de roles denominada AWSResourceExplorerServiceRolePolicy permite el acceso de solo lectura a Resource Explorer para recuperar los nombres y las propiedades de los recursos admitidos para AWS. Para ver los servicios y recursos que Resource Explorer admite, consulte Tipos de recursos que puede buscar con Resource Explorer. Para ver la lista completa de todas las acciones que puede realizar este rol, puede ver la política de `AWSResourceExplorerServiceRolePolicy` en la consola de IAM.

Una entidad principal es una entidad de IAM, como un usuario, un grupo o un rol. Si deja que Resource Explorer cree el rol vinculado al servicio por usted al crear el índice en la primera región de la cuenta, entonces la entidad principal que realice la tarea solo necesitará los permisos necesarios para crear el índice de Resource Explorer. Para crear el rol vinculado al servicio de forma manual mediante IAM, la entidad principal que realice la tarea debe tener permiso para crear un rol vinculado al servicio. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio para Resource Explorer

No necesita crear manualmente un rol vinculado a servicios. Cuando activas el Explorador de recursos en la AWS Management Console cuenta o ejecutas CreateIndexla primera Región de AWS función de tu cuenta mediante la API AWS CLI o una AWS API, el Explorador de recursos crea automáticamente el rol vinculado al servicio.

Si elimina este rol vinculado a un servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando estés RegisterResourceExploreren la primera región de tu cuenta, Resource Explorer volverá a crear el rol vinculado al servicio para ti.

Edición de un rol vinculado a un servicio para Resource Explorer

Resource Explorer no le permite modificar el rol vinculado al servicio de `AWSServiceRoleForResourceExplorer`. 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 Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Cómo eliminar un rol vinculado a un servicio para Resource Explorer

Puede utilizar la consola de IAM, la AWS CLI o la API de AWS para eliminar manualmente el rol vinculado al servicio. Para ello, primero debe eliminar los índices de Resource Explorer de cada Región de AWS de su cuenta y, a continuación, puede eliminar manualmente el rol vinculado a los servicios.

> **Note**
>
> Si el servicio de Resource Explorer está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría arrojar un error. En ese caso, asegúrese de eliminar todos los índices de todas las regiones, espere unos minutos e intente nuevamente completar la operación.

Cómo eliminar manualmente el rol vinculado a servicios mediante IAM

Puede usar la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado al servicio `AWSServiceRoleForResourceExplorer`. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a servicios de Resource Explorer

Resource Explorer admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte los puntos de conexión de Servicio de AWS en la Referencia general de Amazon Web Services.

Solución de problemas de permisos Explorador de recursos de AWS

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Resource Explorer y AWS Identity and Access Management (IAM).

Temas

- No tengo autorización para realizar una acción en Resource Explorer
- Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de Resource Explorer

No tengo autorización para realizar una acción en Resource Explorer

Si la AWS Management Console le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es quien le proporcionó las credenciales que utilizó para intentar esta operación.

En el siguiente ejemplo, el error se produce cuando alguien asume el rol de IAM `MyExampleRole` e intenta utilizar la consola para ver detalles sobre una vista, pero no tiene permisos `resource-explorer-2:GetView`.

```
User: arn:aws:iam::123456789012:role/MyExampleRole is not authorized to perform:
 resource-explorer-2:GetView on resource: arn:aws:resource-explorer-2:us-
east-1:123456789012:view/EC2-Only-View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

En este caso, la persona que utilice el rol deberá pedirle al administrador que actualice las políticas de permisos del rol para permitir el acceso a la vista mediante la acción `resource-explorer-2:GetView`.

Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de Resource Explorer

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 admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Resource Explorer admite estas funciones, consulte Cómo funciona Resource Explorer con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.

- Para obtener información acerca de cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una identidad federada, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Protección de los datos en Explorador de recursos de AWS

El modelo de responsabilidad compartida, y de AWS se aplica a la protección de datos de Explorador de recursos de AWS. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la 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 las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Para proteger los datos, recomendamos proteger las credenciales de Cuenta de AWS y configurar cuentas de usuario 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 autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. reSe recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los 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 módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Recomendamos firmemente nunca ingresar 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 las situaciones en las que debe trabajar con Resource Explorer o con otros Servicios de AWS a través de la consola, la API, la AWS CLI o los AWS SDK. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Cifrado en reposo

Los datos que almacena Resource Explorer incluyen la lista indexada de los recursos y los ARN asociados que utiliza el cliente y las vistas para acceder a ellos.

Estos datos se cifran cuando están en reposo mediante claves de cifrado simétricas de AWS Key Management Service (AWS KMS) que implementan Advanced Encryption Standard (AES) en el modo de contador Galois (GCM) con claves de 256 bits (AES-256-GCM).

Cifrado en tránsito

Las solicitudes de los clientes y todos los datos asociados se cifran en tránsito mediante Transport Later Security (TLS) 1.2 o una versión posterior. Todos los puntos de conexión de Resource Explorer son compatibles con HTTPS para cifrar datos en tránsito. Para obtener una lista completa de los puntos de conexión del servicio de Resource Explorer, consulte Puntos de conexión de Explorador de recursos de AWS y las cuotas en la Referencia general de AWS.

Validación de conformidad en Explorador de recursos de AWS

Para saber si un Servicio de AWS se encuentra dentro del ámbito de aplicación de los programas de cumplimiento específicos, consulte los Servicios de AWS en el ámbito del programa de cumplimiento. Para obtener información general, consulte los Programas de cumplimiento deAWS.

Puede descargar los informes de auditoría de terceros mediante AWS Artifact. Para obtener más información, consulte la Descarga de informes en AWS Artifact en la Guía del usuario de AWS Artifact.

Su responsabilidad de conformidad al usar Resource Explorer se encuentra determinada por la confidencialidad de los datos, los objetivos de cumplimiento de su empresa y las leyes y regulaciones aplicables. AWS brinda los siguientes recursos para ayudarlo con los requisitos de conformidad:

- Security and Compliance Quick Start Guides (Guías de inicio rápido de seguridad y conformidad) (Guías de inicio rápido de seguridad y conformidad): Estas guías de implementación analizan las consideraciones en materia de arquitectura y proporcionan los pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services (Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones compatibles con HIPAA.

  > **Note**
  >
  > No todos los Servicios de AWS son compatibles con HIPAA. Para obtener más información, consulte la Referencia de servicios aptos para HIPAA.

- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este servicio de AWS proporciona una vista integral de su estado de seguridad en AWS que lo ayuda a verificar si cumple con los estándares y las buenas prácticas de seguridad de la industria.

Resiliencia en Explorador de recursos de AWS

La infraestructura global se AWS construye en torno a las Regiones de AWS y a las zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja demora. Mediante 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 Regiones de AWS y las zonas de disponibilidad, consulte la Infraestructura global de AWS.

Seguridad de la infraestructura en Explorador de recursos de AWS

Como se trata de un servicio administrado, Explorador de recursos de AWS está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas de AWS para acceder a Resource Explorer a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) tales como DHE (Ephemeral Diffie-Hellman) o 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 estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Para obtener más información sobre procedimientos de seguridad de red global de AWS, consulte el documento técnico Amazon Web Services: Información general sobre procesos de seguridad.

Monitoreo de Explorador de recursos de AWS

El monitoreo es una parte importante para mantener la fiabilidad, la disponibilidad y el rendimiento de Explorador de recursos de AWS y de sus otras soluciones de AWS. AWS ofrece las siguientes herramientas de supervisión para vigilar Resource Explorer, informar cuando algo no funciona bien y tomar medidas de forma automática cuando corresponda:

- AWS CloudTrail captura las llamadas a la API y otros eventos relacionados que realiza la Cuenta de AWS o se realizan en nombre de esta. Además, entrega los archivos de registros a un bucket de Amazon S3 especificado. 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 Registro de llamadas a la API de Explorador de recursos de AWS mediante AWS CloudTrail y la Guía del usuario de AWS CloudTrail.

Registro de llamadas a la API de Explorador de recursos de AWS mediante AWS CloudTrail

Explorador de recursos de AWS está integrado con AWS CloudTrail, un servicio que proporciona un registro de las acciones que lleva a cabo un usuario, un rol o un Servicio de AWS en Resource Explorer. CloudTrail captura todas las llamadas a la API de Resource Explorer como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Resource Explorer y las llamadas desde el código a las operaciones de la API de Resource Explorer.

Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos para Resource Explorer. Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que usted especifique. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Mediante la información que recopila CloudTrail, puede determinar la solicitud que se hizo a Resource Explorer, la dirección IP desde la que se hizo dicha solicitud, quién la hizo y cuándo, además de información adicional.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información de Resource Explorer en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando la crea. Cuando se produce una actividad en Resource Explorer, dicha actividad se registra en un evento de CloudTrail junto con los demás

eventos de Servicio de AWS en el Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la Cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

> **Important**
>
> Para encontrar todos los eventos de Resource Explorer, busque Event source = resource-explorer-2.amazonaws.com

Para mantener un registro continuo de los eventos en su Cuenta de AWS, incluidos los eventos de Resource Explorer, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar 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. También es posible configurar otros Servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS CloudTrail:

- Creación de una traza para su Cuenta de AWS
- Integraciones de servicios de AWS con registros de CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recepción de archivos de registro de CloudTrail de varias regiones
- Recepción de archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las acciones de Resource Explorer y estas se documentan en la Referencia de la API de Explorador de recursos de AWS. Por ejemplo, las llamadas a las acciones `CreateIndex`, `DeleteIndex` y `UpdateIndex` generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información que lo ayuda a determinar quién generó la solicitud.

- Credenciales raíz de Cuenta de AWS
- Credenciales de seguridad temporales de un rol de AWS Identity and Access Management (IAM) o de un usuario federado.

- Credenciales de seguridad a largo plazo de un usuario de IAM.
- Otro servicio de AWS.

> **Important**
>
> Por motivos de seguridad, todos los valores `Tags`, `Filters` y `QueryString` se eliminan de las entradas del registro de CloudTrail.

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

Comprensión de las entradas de archivos de registro de Resource Explorer

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que usted especifique. Los archivos de registro de CloudTrail pueden contener una o varias entradas de registro. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

Temas

- CreateIndex
- DeleteIndex
- UpdateIndexType
- Búsqueda
- CreateView
- DeleteView
- DisassociateDefaultView

CreateIndex

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

```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-166EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-166EXAMPLE",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:13:59Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-index",
    "requestParameters": {
        "ClientToken": "792ee665-58af-423c-bfdb-d7c9aEXAMPLE"
    },
    "responseElements": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "State": "CREATING",
        "CreatedAt": "2022-08-23T19:13:59.775Z"
    },
    "requestID": "a193afe9-17ff-4f30-ae0a-73bb0EXAMPLE",
    "eventID": "2ec50598-4de6-474d-bd0e-f5c00EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
```

```
    "eventCategory": "Management"
}
```

DeleteIndex

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

> **Note**
>
> Esta acción también elimina de forma asíncrona todas las vistas de la cuenta en esa región, lo que genera un evento `DeleteView` para cada vista eliminada.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:My-Role-Name",
        "arn": "arn:aws:sts::123456789012:assumed-role/My-Admin-Role/My-Delegated-
Role",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/My-Admin-Role",
                "accountId": "123456789012",
                "userName": "My-Admin-Role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T18:33:06Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:04:06Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteIndex",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-index",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "State": "DELETING",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "requestID": "d7d80bd2-cd2d-47fb-88d6-5133aEXAMPLE",
    "eventID": "675eab39-c514-4d32-989d-0ea98EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


UpdateIndexType

En el ejemplo siguiente, se muestra una entrada de registro de CloudTrail para ilustrar la acción `UpdateIndexType` para promover un índice de tipo `LOCAL` a `AGGREGATOR`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
```

```
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:21:18Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "UpdateIndexType",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.update-index-type",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "Type": "AGGREGATOR"
    },
    "responseElements": {
        "Type": "AGGREGATOR",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "LastUpdatedAt": "2022-08-23T19:21:17.924Z",
        "State": "UPDATING"
    },
    "requestID": "a145309d-df14-4c2e-a9f6-8ed45EXAMPLE",
    "eventID": "ed33ab96-f5c6-4a77-a69a-8585aEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


Búsqueda

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

> **Note**
>
> Por motivos de seguridad, todas las referencias a parámetros de `Tag`, `Filters` y `QueryString` están eliminadas en las entradas del registro de seguimiento de CloudTrail.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-03T16:50:11Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "Search",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.search",
    "requestParameters": {
        "QueryString": "***"
    },
    "responseElements": null,
    "requestID": "22320db5-b194-446f-b9f4-e603bEXAMPLE",
```

```
    "eventID": "addb3bca-0c41-46bf-a5e6-42299EXAMPLE",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


CreateView

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


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-01-20T21:54:48Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
```

```
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-view",
    "requestParameters": {
        "ViewName": "CTTagsTest",
        "Tags": "***"
    },
    "responseElements": {
        "View": {
            "Filters": "***",
            "IncludedProperties": [],
            "LastUpdatedAt": "2023-01-20T21:54:48.079Z",
            "Owner": "123456789012",
            "Scope": "arn:aws:iam::123456789012:root",
            "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    },
    "requestID": "b22d8ced-4905-42c4-b1aa-ef713EXAMPLE",
    "eventID": "f62e339f-1070-41a8-a6ec-12491EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


DeleteView

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail que ilustra el evento que puede producirse cuando la acción `DeleteView` se inicia automáticamente debido a una operación `DeleteIndex` en la misma Región de AWS.

> **Note**
>
> Si la vista eliminada es la vista predeterminada de la región, esta acción también disocia de forma asíncrona la vista como la predeterminada. Esto produce un evento `DisassociateDefaultView`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-09-16T19:33:27Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "cd174d1e-0a24-4b47-8b67-d024aEXAMPLE",
    "readOnly": false,
    "resources": [{
        "accountId": "334026708824",
        "type": "AWS::ResourceExplorer2::View",
        "ARN": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }],
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

DisassociateDefaultView

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail que ilustra el evento que puede producirse cuando la acción `DisassociateDefaultView` se inicia automáticamente debido a una operación `DeleteView` en la vista predeterminada actual.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "resource-explorer-2.amazonaws.com"
    },
    "eventTime": "2022-09-16T19:33:26Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DisassociateDefaultView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.disassociate-default-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "d8016cb1-5c23-4ea4-bda2-70b03EXAMPLE",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Cómo crear recursos de Resource Explorer con CloudFormation

Explorador de recursos de AWS es un servicio integrado con AWS CloudFormation que lo ayuda a modelar y configurar los recursos de AWS. De este modo, puede dedicar menos tiempo a crear y administrar los recursos y la infraestructura. Puede crear una plantilla que describa todos los recursos de AWS que desee, y CloudFormation aprovisiona y configura esos recursos por usted. Algunos ejemplos de recursos son: los índices, las vistas o la asignación de una vista predeterminada para la Región de AWS.

Cuando utiliza CloudFormation, puede volver a utilizar la plantilla para configurar los recursos de Resource Explorer de forma coherente y reiterada. Solo tiene que describir los recursos una vez y, luego, proporcionar los mismos recursos una y otra vez en varias cuentas y regiones de Cuentas de AWS.

Utilizar AWS CloudFormation para implementar Resource Explorer en AWS Organizations

Puede usar los StackSets de AWS CloudFormation para implementar Resource Explorer en todas las cuentas de su organización. Cuando agrega o crea cuentas de miembros en su organización, StackSets puede configurar automáticamente los índices de cada Región de AWS, incluido un índice agregador donde lo especifique, para cada nueva cuenta de miembro. Para obtener instrucciones, consulte Implementar el explorador de recursos en las cuentas de una organización.

Plantillas de Resource Explorer y CloudFormation

Para aprovisionar y configurar los recursos de Resource Explorer y sus servicios relacionados debe entender las plantillas de AWS CloudFormation. Las plantillas son archivos de texto con formato de tipo JSON o YAML. Estas plantillas describen los recursos que desea proporcionar en sus pilas de CloudFormation. Si no está familiarizado con JSON o YAML, puede utilizar AWS CloudFormation Designer que lo ayudará a comenzar a utilizar las plantillas de CloudFormation. Para obtener más información, consulte ¿Qué es Designer AWS CloudFormation ? en la Guía del usuario de AWS CloudFormation.

Resource Explorer admite la creación de los siguientes tipos de recursos en CloudFormation:

- Índice: crea un índice en una región y activa Resource Explorer en esa región. Puede especificar que el índice sea local o el índice agregador para la Cuenta de AWS. Para obtener más

información, consulte Activar el explorador de recursos en una Región de AWS para indexar sus recursos y Activación de la búsqueda entre regiones mediante la creación de un índice agregador.

- Vista: crea una vista que determina qué resultados pueden aparecer cuando el usuario realiza una búsqueda. Cada operación de búsqueda debe especificar una vista. Debe conceder a los usuarios permiso para utilizar las vistas a las que quiere que accedan. Para obtener más información, consulte Cómo administrar las vistas de Resource Explorer para proporcionar acceso a la búsqueda.

  > **Note**
  >
  > Para poder crear una vista en una región, primero, debe crear un índice en esa misma región. Si crea un índice y una vista como parte de la misma pila, utilice el atributo `DependsOn` en la vista, como se muestra en la siguiente plantilla de ejemplo, para asegurarse de que el índice se cree primero.

- DefaultViewAssociation: asigna la vista especificada como la predeterminada en su región. Cuando un usuario no especifica de forma explícita la vista que se va a utilizar en una operación de búsqueda, Resource Explorer intenta utilizar la vista predeterminada asociada a la región en la que el usuario realiza la búsqueda. Para obtener más información, consulte Establecer una vista predeterminada en un Región de AWS

El siguiente ejemplo ilustra cómo crear un índice y una vista en la misma región y cómo configurar la vista para que sea la predeterminada de la región.

YAML

```
Description: >-
  Sample CFN Stack setting up Resource Explorer with an aggregator index and a default
 view
Resources:
  SampleIndex:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
  SampleView:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
```

```
      ViewName: mySampleView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
    DependsOn: SampleIndex
  SampleDefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref SampleView
```

JSON

```
{
    "Description": "Sample CFN Stack setting up Resource Explorer with an aggregator
 index and a default view ",
    "Resources": {
        "SampleIndex": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer Sample Stack"
                }
            }
        },
        "SampleView": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "mySampleView",
                "IncludedProperties": [
                    {
                        "Name": "tags"
                    }
                ],
                "Tags": {
                    "Purpose": "ResourceExplorer Sample CFN Stack"
                }
            },
            "DependsOn": "SampleIndex"
        },
        "SampleDefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
```

```
            "Properties": {
                "ViewArn": {
                    "Ref": "SampleView"
                }
            }
        }
    }
}
```

Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para los índices y vistas de Resource Explorer, consulte la referencia del tipo de recurso de ResourceExplorer2 en la guía del usuario de AWS CloudFormation.

Obtener más información sobre AWS CloudFormation

Para obtener más información acerca de CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- Guía del usuario de AWS CloudFormation
- Guía del usuario de la interfaz de la línea de comandos de AWS CloudFormation

Solución de problemas de Resource Explorer

Si surgen problemas a la hora de trabajar con Resource Explorer, consulte los temas de esta sección. Consulte también Solución de problemas de permisos Explorador de recursos de AWS en la sección de seguridad de esta guía.

Temas

Problemas generales

Temas

He recibido un enlace a Resource Explorer, pero cuando lo abro, la consola solo muestra un error.

Algunas herramientas de terceros producen enlaces a direcciones de URL en Resource Explorer. En algunos casos, esas direcciones de URL no incluyen el parámetro que dirige la consola a una Región de AWS específica. Si abre un enlace de este tipo, no se indicará a la consola de Resource Explorer qué región usar y, de forma predeterminada, usará la última región en la que el usuario inició sesión. Si el usuario no tiene permisos para acceder a Resource Explorer en esa región, la consola intentará utilizar la región Este de EE. UU. (Norte de Virginia) (`us-east-1`) o bien Oeste de EE. UU. (Oregón) (`us-west-2`) si la consola no puede acceder a `us-east-1`.

Si el usuario no tiene permiso para acceder al índice de cualquiera de esas regiones, la consola de Resource Explorer mostrará un error.

Para evitar este problema, asegúrese de que todos los usuarios tengan los siguientes permisos:

- `ListIndexes`: ningún recurso específico; use `*`.

- `GetIndex` para el ARN de cada índice creado en la cuenta. Para evitar tener que rehacer las políticas de permisos si eliminó y volvió a crear un índice, le recomendamos que utilice `*`.

La política mínima para lograr esto sería similar a la de este ejemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetIndex",
                "resource-explorer-2:ListIndexes",
            ],
            "Resource": "*"
        }
    ]
}
```

Como alternativa, puede considerar la posibilidad de adjuntar el permiso administrado de `AWSAWSResourceExplorerReadOnlyAccess` a todos los usuarios que necesiten usar Resource Explorer. Esto otorga los permisos obligatorios, además de los permisos necesarios para ver las vistas disponibles en la región y realizar búsquedas con esas vistas.

¿Por qué la búsqueda unificada en la consola produce errores de “acceso denegado” en mis registros de CloudTrail?

La búsqueda unificada en el AWS Management Console permite a las entidades principales buscar desde cualquier página de la AWS Management Console. Los resultados pueden incluir recursos de la cuenta de la entidad principal si Resource Explorer está activado y configurado para admitir la búsqueda unificada. Siempre que empiece a escribir en la barra de búsqueda unificada, la búsqueda unificada intentará notificar a la operación `resource-explorer-2:ListIndexes` para comprobar si puede incluir recursos de la cuenta del usuario en los resultados.

La búsqueda unificada utiliza los permisos del usuario que ha iniciado sesión en ese instante para realizar esta comprobación. Si ese usuario no tiene el permiso para informar a `resource-explorer-2:ListIndexes` otorgado en una política de permisos adjunta AWS Identity and Access Management (IAM), se produce un error en la comprobación. Ese error se añade como una entrada de `Access denied` en los registros de CloudTrail.

Esta entrada de registro de CloudTrail incluye las siguientes características:

- Origen del evento: `resource-explorer-2.amazonaws.com`
- Nombre del evento: `ListIndexes`
- Código de error: `403` (Acceso denegado)

Las siguientes políticas administradas de AWS deben incluir permisos para informar a `resource-explorer-2:ListIndexes`. Si asigna alguna de estas políticas a la entidad principal o a cualquier otra política que incluya este permiso, no se producirá este error:

- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerFullAccess
- ReadOnlyAccess
- ViewOnlyAccess

Solución de problemas de instalación y configuración de Resource Explorer

Esta información le ayudará a diagnosticar y solucionar los problemas que puedan surgir cuando instale o configure Explorador de recursos de AWS por primera vez.

Temas

Aparece un mensaje de "acceso denegado" al realizar una solicitud a Resource Explorer

- Compruebe que tiene permisos para llevar a cabo la acción y el recurso que ha solicitado. Un administrador puede conceder permisos asignando una política de permisos AWS Identity and Access Management (IAM) a su entidad principal de IAM, como un rol, un grupo o un usuario.

  Para proporcionar acceso, agregue permisos a sus usuarios, grupos o roles:

- Usuarios y grupos de AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Create a permission set (Creación de un conjunto de permisos) en la AWS IAM Identity Center Guía del usuario de.

- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda asumir. Siga las instrucciones de Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones de Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

  La política debe permitir el `Action` solicitado en el `Resource` al que desee acceder.

  Si las instrucciones de la política que conceden esos permisos incluyen alguna condición, como la hora del día o restricciones de direcciones IP, también debe cumplir esos requisitos cuando envíe la solicitud. Para obtener más información sobre cómo consultar o modificar políticas de una entidad principal de IAM, consulte Administrar políticas de IAM en la Guía del usuario de IAM.

- Si va a firmar las solicitudes a la API manualmente (sin usar los SDK de AWS) compruebe que haya firmado la solicitud correctamente.

Aparece un mensaje de "acceso denegado" al realizar una solicitud con credenciales de seguridad temporales

- Compruebe que la entidad principal de IAM que está utilizando para realizar la solicitud tenga los permisos adecuados. Los permisos de credenciales de seguridad temporales se obtienen de una entidad principal definida en IAM, y, por lo tanto, están limitados a los concedidos a la entidad principal. Para obtener más información sobre cómo se determinan los permisos de las credenciales de seguridad temporales, consulte Controlar los permisos para credenciales de seguridad temporales en la Guía del usuario de IAM.
- Compruebe que las solicitudes se han firmado correctamente y que la solicitud tiene el formato correcto. Para obtener más información, consulte la documentación del conjunto de herramientas

del SDK seleccionado o Uso de credenciales de seguridad temporales con recursos de AWS en la Guía del usuario de IAM.

- Compruebe que sus credenciales de seguridad temporales no hayan caducado. Para obtener más información, consulte la Solicitud de credenciales de seguridad temporales en la Guía del usuario de IAM.

Solución de problemas de búsqueda de Resource Explorer

Utilice la información que se indica aquí para diagnosticar y solucionar los errores comunes que puedan surgir al buscar recursos mediante Resource Explorer.

Temas

¿Por qué faltan algunos recursos en los resultados de búsqueda de Resource Explorer?

En la siguiente lista se indican los motivos por los que es posible que algunos recursos no aparezcan en los resultados de la búsqueda de la forma esperada:

La indexación inicial no está completa

> Tras activar Resource Explorer por primera vez en una Región de AWS, la indexación y la replicación en el índice del agregador pueden tardar hasta 36 horas en completarse. Intente buscar más tarde.

El recurso es nuevo

> Resource Explorer puede tardar unos minutos en descubrir un recurso nuevo y añadirlo al índice local. Intente nuevamente en unos minutos.

La información sobre un recurso nuevo en una región aún no se ha propagado al índice del agregador

Los detalles sobre un nuevo recurso descubierto en una región pueden tardar algún tiempo en indexarse en su propia región y, a continuación, replicarse en el índice agregador de la cuenta. El nuevo recurso solo puede aparecer en los resultados de búsquedas entre regiones una vez completada la replicación. Intente buscar más tarde.

La región con el recurso no tiene activado Resource Explorer

El administrador determina en qué Regiones de AWS puede operar Resource Explorer. La página de Configuración muestra qué regiones tienen activado Resource Explorer y contienen un índice. Si la región con su recurso no está activada, pida al administrador que active Resource Explorer en esa región.

El recurso existe en una región diferente y la región buscada no contiene el índice del agregador

Puede buscar recursos en todas las regiones de la cuenta solo usando una vista de la región que contenga el índice agregador. Las búsquedas en cualquier otra región muestran recursos únicamente de la región en la que se realiza la búsqueda.

Los filtros de la vista excluyen ese recurso

Cada vista puede incluir filtros en la configuración que restringen los resultados que se pueden incluir en los resultados de búsqueda realizados con esa vista. Asegúrese de que el recurso que busca coincide con los filtros de la vista que utiliza para realizar la búsqueda. Para obtener más información sobre los filtros, consulte. Filtros Para obtener más información acerca de las visualizaciones, consulte Acerca de las vistas del explorador de recursos.

Resource Explorer no admite este tipo de recurso

Resource Explorer no admite ciertos tipos de recurso. Para más información, consulte Tipos de recursos que puede buscar con Resource Explorer.

Los índices o las vistas no están configurados en la región de la consola

Si los índices o las vistas no están configurados en las regiones esperadas por la consola que consume el widget, no verá los resultados esperados. Para obtener más información, consulte Activación de la búsqueda entre regiones mediante la creación de un índice agregador y Acerca de las vistas del explorador de recursos.

Sus vistas no incluyen etiquetas

El widget Resource Explorer requiere etiquetas. Si tus vistas no incluyen etiquetas, los recursos no se incluirán en los resultados. Para más información, consulte Agregar etiquetas a vistas.

La búsqueda utiliza una sintaxis de consulta de búsqueda incorrecta

La búsqueda en Resource Explorer es exclusiva de este servicio. Sin la sintaxis correcta, no encontrará los recursos que espera. Para más información, consulte Búsqueda de referencia de sintaxis de consulta en Resource Explorer.

Ha etiquetado sus recursos recientemente

Tras etiquetar un recurso, transcurren 30 segundos antes de que el recurso aparezca en los resultados de la búsqueda.

El tipo de recurso no admite filtros de etiquetas

Si el tipo de recurso no admite los filtros de etiquetas, no se mostrarán en el widget del explorador de recursos. Los tipos de recursos que no admiten filtros de etiquetas son:

- `cloudfront:cache-policy`
- `cloudfront:origin-access-identity`
- `cloudfront:function`
- `cloudfront:origin-request-policy`
- `cloudfront:realtime-log-config`
- `cloudfront:response-headers-policy`
- `cloudwatch:dashboard`
- `docdb:globalcluster`
- `elasticache:globalreplicationgroup`
- `iam:group`
- `lambda:code-signing-config`
- `lambda:event-source-mapping`
- `ssm:windowtarget`
- `ssm:windowtask`
- `rds:auto-backup`
- `rds:global-cluster`
- `s3:accesspoint`

¿Por qué mis recursos no aparecen en los resultados de búsqueda unificados de la consola?

Los resultados de búsqueda unificados están disponibles en la barra de búsqueda situada en la parte superior de cada página de la AWS Management Console. Sin embargo, la búsqueda solo puede devolver recursos que coincidan con la consulta en los resultados de la búsqueda una vez que se hayan completado las siguientes opciones de configuración:

- Debe haber un índice del agregador en una de las regiones de la cuenta.
- Debe haber una vista predeterminada en la región que contenga el índice del agregador.
- Todas las entidades principales (roles de IAM y usuarios) deben tener permiso para buscar con esa vista predeterminada.

¿Por qué la búsqueda unificada en la consola y en Resource Explorer a veces arroja resultados diferentes?

Los resultados de búsqueda unificados están disponibles en la barra de búsqueda situada en la parte superior de cada página de la AWS Management Console. Cuando se utiliza la búsqueda unificada, el proceso de búsqueda unificada inserta automáticamente un carácter comodín (*) al final del primer término que se ingrese en la cadena de consulta. El carácter comodín no está visible en el cuadro de búsqueda unificada, pero sí afecta a los resultados.

> **Important**
>
> La búsqueda unificada inserta automáticamente un operador de caracteres comodín (*) al final de la primera palabra clave de la cadena. Esto significa que los resultados de la búsqueda unificada incluyen recursos que coinciden con cualquier cadena que comience por la palabra clave especificada.
> La búsqueda realizada mediante el cuadro de texto Consulta de la página de Búsqueda de recursos de la consola de Resource Explorer no añade automáticamente un carácter comodín. Puede insertar manualmente un * después de cualquier término de la cadena de búsqueda.

¿Qué permisos necesito para poder buscar recursos?

Para realizar una búsqueda, debe tener permiso para realizar las siguientes dos operaciones en una vista que se encuentre en la región en la que lleva a cabo la operación:

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

Para hacerlo, puede añadir una instrucción similar a la del siguiente ejemplo a una política asignada a su entidad principal de IAM.

```
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-
View-Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
```

Puede sustituir el número de recurso de Amazon (ARN) de una vista específica por un ARN que incluya un comodín (*) para conceder permiso a todas las vistas que coincidan.

Si no especifica una vista en la solicitud, Resource Explorer utilizará automáticamente la vista predeterminada para la región en la que realizó la solicitud. Si no tiene permisos para usar la vista predeterminada, hable con su administrador.

> **Note**
>
> Incluso si ve un recurso en los resultados de una consulta de búsqueda de Resource Explorer, necesita permisos sobre el propio recurso para poder interactuar con él.

Tipos de recursos que puede buscar con Resource Explorer

Temas

En las siguientes tablas se enumeran los tipos de recursos que se admiten para realizar búsquedas en Explorador de recursos de AWS.

> **Notas**
>
> - Algunos tipos de recursos se identifican mediante cadenas de Nombres de recursos de Amazon (ARN) que comparten un formato común con otro tipo de recurso. Cuando esto ocurre, Resource Explorer puede reportar esos recursos como el otro tipo de recurso. Para obtener una lista de los tipos de recursos afectados por este problema, consulte Tipos de recursos que aparecen como otros tipos.
> - En este momento, las etiquetas adjuntas a los recursos AWS Identity and Access Management (de IAM), como los roles o los usuarios, no se pueden usar para realizar búsquedas.
> - Si tiene acceso cifrado a algunos de sus recursos, Resource Explorer no podrá detectarlos. No verá estos recursos en los resultados de la búsqueda.

Tipos de recursos y servicios admitidos

Compatible Servicios de AWS

- Amazon API Gateway
- AWS App Runner
- Amazon AppStream 2.0
- AWS AppSync
- Amazon Athena

- AWS Backup
- AWS Batch
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- Amazon, CloudWatch evidentemente
- Amazon CloudWatch Logs
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- Amazon CodeGuru Profiler
- AWS CodePipeline
- AWS CodeConnections
- Amazon Cognito
- Amazon Connect
- Amazon Connect Wisdom
- Amazon Detective
- Amazon DynamoDB
- Generador de Imágenes de EC2
- Amazon ECR Public
- AWS Elastic Beanstalk
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- AWS Elemental MediaPackage
- AWS Elemental MediaTailor

- Amazon EMR sin servidor
- Amazon EventBridge
- AWS Fault Injection Service
- Amazon Forecast
- Amazon Fraud Detector
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS Identity and Access Management
- Amazon Interactive Video Service
- AWS IoT
- AWS IoT Analytics
- AWS IoT Events
- AWS IoT Greengrass Version 1
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- Amazon Kinesis
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- Amazon Location Service
- Amazon Lookout for Metrics
- Amazon Lookout for Vision
- Amazon Managed Service para Apache Flink
- Amazon Managed Service para Prometheus
- Servicio administrado por Amazon para Prometheus
- Transmisión gestionadada de Amazon para Apache Kafka

- AWS Migration Hub Refactor Spaces
- AWS Network Firewall
- AWS Network Manager
- OpenSearch Servicio Amazon
- AWS Panorama
- Amazon Personalize
- AWS Private Certificate Authority
- Amazon QLDB
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (Amazon RDS)
- AWS Resilience Hub
- AWS Resource Groups
- Explorador de recursos de AWS
- Amazon Route 53
- Preparación para la recuperación de Amazon Route 53
- Amazon Route 53 Resolver
- Amazon SageMaker
- AWS Secrets Manager
- AWS Service Catalog
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager
- Acceso verificado de AWS
- AWS Wavelength

Amazon API Gateway

- `apigateway:restapis`

AWS App Runner

- apprunner:vpcconnector

Amazon AppStream 2.0

- appstream:appblock
- appstream:application
- appstream:fleet
- appstream:stack

AWS AppSync

- appsync:apis

Amazon Athena

- athena:datacatalog
- athena:workgroup

AWS Backup

- backup:backupplan

AWS Batch

- batch:computeenvironment
- batch:jobqueue
- batch:schedulingpolicy

AWS CloudFormation

- cloudformation:stack

- cloudformation:stackset

Amazon CloudFront

- cloudfront:cache-policy
- cloudfront:distribution
- cloudfront:function
- cloudfront:fieldlevelencryptionconfig
- cloudfront:fieldlevelencryptionprofile
- cloudfront:origin-access-identity
- cloudfront:originaccesscontrol
- cloudfront:origin-request-policy
- cloudfront:realtime-log-config
- cloudfront:response-headers-policy

AWS CloudTrail

- cloudtrail:trail

Amazon CloudWatch

- cloudwatch:alarm
- cloudwatch:dashboard
- cloudwatch:insight-rule
- cloudwatch:metric-stream
- evidently:project

Amazon, CloudWatch evidentemente

- evidently:project/experiment
- evidently:project/feature
- evidently:project/launch

Amazon CloudWatch Logs

- `logs:destination`
- `logs:log-group`

AWS CodeArtifact

- `codeartifact:domain`
- `codeartifact:repository`

AWS CodeBuild

- `codebuild:project`

AWS CodeCommit

- `codecommit:repository`

Amazon CodeGuru Profiler

- `codeguru-profiler:profilingGroup`

AWS CodePipeline

- `codepipeline:pipeline`

AWS CodeConnections

- `codestarconnections:connect`

Amazon Cognito

- `cognito:identitypool`

- cognito:userpool

Amazon Connect

- appintegrations:eventintegration

Amazon Connect Wisdom

- wisdom:assistant
- wisdom:association
- wisdom:knowledge-base

Amazon Detective

- detective:graph

Amazon DynamoDB

- dynamodb:table

Generador de Imágenes de EC2

- imagebuilder:component
- imagebuilder:containerrecipe
- imagebuilder:distributionconfiguration
- imagebuilder:image
- imagebuilder:imagepipeline
- imagebuilder:imagerecipe
- imagebuilder:infrastructureconfiguration

Amazon ECR Public

- ecrpublic:repository

AWS Elastic Beanstalk

- elasticbeanstalk:application
- elasticbeanstalk:applicationversion
- elasticbeanstalk:configurationtemplate
- elasticbeanstalk:environment

Amazon ElastiCache

- elasticache:cluster
- elasticache:globalreplicationgroup
- elasticache:parametergroup
- elasticache:replicationgroup
- elasticache:reserved-instance
- elasticache:snapshot
- elasticache:subnetgroup
- elasticache:user
- elasticache:usergroup

Amazon Elastic Compute Cloud (Amazon EC2)

- ec2:capacity-reservation
- ec2:capacity-reservation-fleet
- ec2:client-vpn-endpoint
- ec2:customer-gateway
- ec2:dedicated-host
- ec2:dhcp-options
- ec2:egress-only-internet-gateway
- ec2:elastic-gpu
- ec2:elastic-ip

- ec2:fleet
- ec2:fpga-image
- ec2:host-reservation
- ec2:image
- ec2:instance
- ec2:instance-event-window
- ec2:internet-gateway
- ec2:ipam
- ec2:ipam-pool
- ec2:ipam-scope
- ec2:ipv4pool-ec2
- ec2:key-pair
- ec2:launch-template
- ec2:natgateway
- ec2:network-acl
- ec2:network-insights-access-scope
- ec2:network-insights-access-scope-analysis
- ec2:network-insights-analysis
- ec2:network-insights-path
- ec2:network-interface
- ec2:placement-group
- ec2:prefix-list
- ec2:reserved-instances
- ec2:route-table
- ec2:security-group
- ec2:security-group-rule
- ec2:snapshot
- ec2:spot-fleet-request
- ec2:spot-instances-request

- ec2:subnet
- ec2:subnet-cidr-reservation
- ec2:traffic-mirror-filter
- ec2:traffic-mirror-filter-rule
- ec2:traffic-mirror-session
- ec2:traffic-mirror-target
- ec2:transit-gateway
- ec2:transit-gateway-attachment
- ec2:transit-gateway-connect-peer
- ec2:transit-gateway-multicast-domain
- ec2:transit-gateway-policy-table
- ec2:transit-gateway-route-table
- ec2:transitgatewayroutetableannouncement
- ec2:volume
- ec2:vpc
- ec2:vpc-endpoint
- ec2:vpc-flow-log
- ec2:vpc-peering-connection
- ec2:vpn-connection
- ec2:vpn-gateway

Amazon Elastic Container Registry

- ecr:repository

Amazon Elastic Container Service

- ecs:cluster
- ecs:container-instance
- ecs:service

- ecs:task
- ecs:task-definition
- ecs:task-set

Amazon Elastic File System

- efs:filesystem
- efs:accesspoint

Elastic Load Balancing

- elasticloadbalancing:listener
- elasticloadbalancing:listener-rule
- elasticloadbalancing:listener-rule/app
- elasticloadbalancing:listener/app
- elasticloadbalancing:listener/net
- elasticloadbalancing:loadbalancer
- elasticloadbalancing:loadbalancer/app
- elasticloadbalancing:loadbalancer/net
- elasticloadbalancing:targetgroup

AWS Elemental MediaPackage

- mediapackage:channel
- mediapackage:originendpoint
- mediapackage-vod:packaging-configurations
- mediapackage-vod:packaging-groups

AWS Elemental MediaTailor

- mediatailor:playbackConfiguration

Amazon EMR sin servidor

- emr-serverless:applications

Amazon EventBridge

- events:event-bus
- events:rule

AWS Fault Injection Service

- fis:experimenttemplate

Amazon Forecast

- forcast:dataset
- forcast:dataset-group

Amazon Fraud Detector

- frauddetector:detector
- frauddetector:entity-type
- frauddetector:event-type
- frauddetector:label
- frauddetector:outcome
- frauddetector:variable

Amazon GameLift

- gamelift:alias

AWS Global Accelerator

- globalaccelerator:accelerator
- globalaccelerator:accelerator/listener
- globalaccelerator:accelerator/listener/endpoint-group

AWS Glue

- glue:database
- glue:job
- glue:table
- glue:trigger

AWS Glue DataBrew

- databrew:dataset
- databrew:recipe
- databrew:ruleset

AWS Identity and Access Management

- iam:group
- iam:instance-profile
- iam:oidc-provider
- iam:policy
- iam:role
- iam:saml-provider
- iam:server-certificate
- iam:user
- iam:virtualmfadevice

Amazon Interactive Video Service

- ivs:channel
- ivs:streamkey

AWS IoT

- iot:authorizer
- iot:jobtemplate
- iot:mitigationaction
- iot:policy
- iot:provisioningtemplate
- iot:rolealias
- iot:securityprofile
- iot:thing
- iot:topicrule

AWS IoT Analytics

- iotanalytics:channel
- iotanalytics:dataset
- iotanalytics:datastore
- iotanalytics:pipeline

AWS IoT Events

- iotevents:alarmModel
- iotevents:detectorModel
- iotevents:input

AWS IoT Greengrass Version 1

- greengrass:components
- greengrass:groups

AWS IoT SiteWise

- iotsitewise:asset
- iotsitewise:assetmodel
- iotsitewise:gateway

AWS IoT TwinMaker

- iottwinmaker:workspace
- iottwinmaker:workspace/component-type
- iottwinmaker:workspace/entity

AWS Key Management Service

- kms:key

Amazon Kinesis

- kinesis:stream

Amazon Data Firehose

- kinesisfirehose:deliverystream

Amazon Kinesis Video Streams

- kinesisvideo:stream

AWS Lambda

- `lambda:code-signing-config`
- `lambda:event-source-mapping`
- `lambda:function`

Amazon Lex

- `lex:bot`

Amazon Location Service

- `geo:place-index`
- `geo:tracker`

Amazon Lookout for Metrics

- `lookoutmetrics:Alert`

Amazon Lookout for Vision

- `lookoutvision:project`

Amazon Managed Service para Apache Flink

- `kinesisanalytics:application`

Amazon Managed Service para Prometheus

- `aps:rulegroupsnamespace`
- `aps:workspace`

Servicio administrado por Amazon para Prometheus

- memorydb:cluster
- memorydb:parametergroup
- memorydb:user

Transmisión gestionadada de Amazon para Apache Kafka

- kafka:cluster
- kafka:configuration

AWS Migration Hub Refactor Spaces

- refactor-spaces:environment
- refactor-spaces:environment/application
- refactor-spaces:environment/application/route
- refactor-spaces:environment/application/service

AWS Network Firewall

- network-firewall:firewall-policy

AWS Network Manager

- networkmanager:core-network
- networkmanager:device
- networkmanager:global-network
- networkmanager:link

OpenSearch Servicio Amazon

- es:domain

AWS Panorama

- panorama:package

Amazon Personalize

- personalize:dataset
- personalize:dataset-group
- personalize:schema

AWS Private Certificate Authority

- acmpca:certificateauthority

Amazon QLDB

- qldb:ledger
- qldb:stream

Amazon Redshift

- redshift:cluster
- redshift:eventsubscription
- redshift:parametergroup
- redshift:snapshot
- redshift:snapshotcopygrant
- redshift:snapshotschedule
- redshift:subnetgroup
- redshift:usagelimit

Amazon Rekognition

- rekognition:project

Amazon Relational Database Service (Amazon RDS)

- rds:auto-backup
- rds:cev
- rds:cluster
- rds:cluster-endpoint
- rds:cluster-pg
- rds:cluster-snapshot
- rds:db
- rds:db-proxy
- rds:db-proxy-endpoint
- rds:deployment
- rds:es
- rds:global-cluster
- rds:og
- rds:pg
- rds:ri
- rds:secgrp
- rds:snapshot
- rds:subgrp

AWS Resilience Hub

- resiliencehub:resiliencypolicy

AWS Resource Groups

- resourcegroups:group

Explorador de recursos de AWS

- resource-explorer-2:index

- resource-explorer-2:view

Amazon Route 53

- route53:healthcheck
- route53:hostedzone

Preparación para la recuperación de Amazon Route 53

- route53-recover-readiness:recovery-group
- route53-recover-readiness:resource-set

Amazon Route 53 Resolver

- route53resolver:firewalldomainlist
- route53resolver:firewallrulegroup
- route53resolver:resolverendpoint
- route53resolver:resolverrule

Amazon SageMaker

- sagemaker:model
- sagemaker:notebookinstance

AWS Secrets Manager

- secretsmanager:secret

AWS Service Catalog

- servicecatalog:applications
- servicecatalog:attribute-groups

Amazon Simple Notification Service

- sns:topic

Amazon Simple Queue Service

- sqs:queue

Amazon Simple Storage Service (Amazon S3)

- s3:accesspoint
- s3:bucket
- s3:storage-lens

AWS Step Functions

- states:statemachine
- stepfunctions:activity

AWS Systems Manager

- ssm:association
- ssm:automation-execution
- ssm:document
- ssm:maintenancewindow
- ssm:managed-instance
- ssm:parameter
- ssm:patchbaseline
- ssm:resourcedatasync
- ssm:windowtarget
- ssm:windowtask

Acceso verificado de AWS

- `ec2:verifiedaccessendpoint`
- `ec2:verifiedaccessgroup`
- `ec2:verifiedaccessinstance`
- `ec2:verifiedaccesstrustprovider`

AWS Wavelength

- `ec2:carriergateway`

Acceso mediante programación a la lista de tipos de recursos admitidos

Para acceder a la lista de tipos de recursos compatibles desde el código, puedes invocar la ListSupportedResourceTypesoperación desde cualquier AWS SDK.

Por ejemplo, puedes ejecutar el comando list-supported-resource-types AWS Command Line Interface (AWS CLI), como se muestra en el siguiente ejemplo.

```
$ aws resource-explorer-2 list-supported-resource-types
{
    "ResourceTypes": [
        {
            "ResourceType": "acm-pca:certificate-authority",
            "Service": "acm-pca"
        },
        {
            "ResourceType": "airflow:environment",
            "Service": "airflow"
        },
        {
            "ResourceType": "amplify:branches",
            "Service": "amplify"
        },
... truncated for brevity ...
```

Tipos de recursos que aparecen como otros tipos

Algunos tipos de recursos se identifican mediante cadenas de Nombres de recursos de Amazon (ARN) que comparten un formato común con otro tipo de recurso. Cuando esto ocurre, Resource Explorer puede reportar esos recursos como el otro tipo de recurso. Esto afecta a los tipos de recursos de la siguiente tabla.

Tipo de recurso real	Se informa como tipo de recurso
`ec2:securitygroupegress` `ec2:securitygroupingress`	`ec2:security-group-rule`
`elasticloadbalancingv2:loadbalancer`	`elasticloadbalancing:loadbalancer`

`docdb:dbcluster`
`neptune:dbcluster`
`rds:dbcluster`
	`rds:cluster`

`docdb:dbclusterparametergroup`
`neptune:dbclusterparametergroup`
`rds:dbclusterparametergroup`
	`rds:cluster-pg`

`docdb:clustersnapshot`
`neptune:dbclustersnapshot`
`rds:clustersnapshot`
	`rds:cluster-snapshot`

`docdb:dbinstance`
`neptune:dbinstance`
`rds:dbinstance`
	`rds:db`

`docdb:eventsubscription`	`rds:es`

Tipo de recurso real	Se informa como tipo de recurso

`neptune:eventsubscription`
 	
`rds:eventsubscription`	

`docdb:globalcluster`
 	
`rds:globalcluster`
	`rds:global-cluster`

`neptune:dbparametergroup`
 	
`rds:dbparametergroup`
	`rds:pg`

`docdb:dbsubnetgroup`
 	
`neptune:dbsubnetgroup`
 	
`rds:dbsubnetgroup`
	`rds:subgrp`

Cuotas para Resource Explorer

Su Cuenta de AWS tiene cuotas predeterminadas para cada Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región. Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para ver todas las cuotas de Explorador de recursos de AWS, abra la consola de Service Quotas. En el panel de navegación, elija Servicios de AWS y seleccione el Resource Explorer.

Para solicitar un aumento de cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas. Si la cuota aún no se encuentra disponible en Service Quotas, utilice el formulario de aumento del límite.

Las siguientes cuotas son las predeterminadas para Resource Explorer.

Cuotas de valor máximo	Valor predeterminado
Número de vistas en una Región de AWS	10

Límites de velocidad para las operaciones	Valor predeterminado
Máximo de operaciones de búsqueda por segundo	5
Máximo de operaciones que no son de búsqueda por segundo	3
Máximo de operaciones de búsqueda en la región de agregador por mes	10 000
Máximo de operaciones de búsqueda en las regiones locales por mes	500

Explorador de recursos de AWS Utilización con un AWS SDK

AWS Los kits de desarrollo de software (SDK) están disponibles para muchos lenguajes de programación populares. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en su lenguaje preferido.

Documentación de SDK	Ejemplos de código
AWS SDK for C++	AWS SDK for C++ ejemplos de código
AWS CLI	AWS CLI ejemplos de código
AWS SDK for Go	AWS SDK for Go ejemplos de código
AWS SDK for Java	AWS SDK for Java ejemplos de código
AWS SDK for JavaScript	AWS SDK for JavaScript ejemplos de código
AWS SDK para Kotlin	AWS SDK para Kotlin ejemplos de código
AWS SDK for .NET	AWS SDK for .NET ejemplos de código
AWS SDK for PHP	AWS SDK for PHP ejemplos de código
AWS Tools for PowerShell	Herramientas para ejemplos PowerShell de código
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) ejemplos de código
AWS SDK for Ruby	AWS SDK for Ruby ejemplos de código
AWS SDK para Rust	AWS SDK para Rust ejemplos de código
AWS SDK para SAP ABAP	AWS SDK para SAP ABAP ejemplos de código
AWS SDK para Swift	AWS SDK para Swift ejemplos de código

Ejemplo de disponibilidad

¿No encuentra lo que necesita? Solicite un ejemplo de código a través del enlace de Enviar comentarios que se encuentra al final de esta página.

Historial de documentos de la Guía del usuario de Resource Explorer

En la siguiente tabla se describen las versiones de la documentación de Explorador de recursos de AWS. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Adición de compatibilidad con los nuevos tipos de recursos	Resource Explorer agregó soporte para 65 nuevos recursos AWS Key Management Service, Servicios de AWS entre los que se incluyen Amazon Route 53 y Amazon Fraud Detector.	20 de febrero de 2024
Políticas administrada actualizada	Resource Explorer agregó soporte para ver tipos de recursos adicionales. La política `AWSResourceExplorerServiceRolePolicy` AWS administrada se ha actualizado para permitir a Resource Explorer acceder a otros tipos de recursos.	12 de diciembre de 2023
Adición de un nuevo filtro de búsqueda	Resource Explorer ahora admite la búsqueda de recursos por aplicación.	16 de noviembre de 2023
Adición de compatibilidad con el tipo de recurso	Resource Explorer agregó soporte para 86 nuevos recursos de Servicios de	15 de noviembre de 2023

	AWS AWS CloudForm ation Inclusive AWS Glue, y Amazon SageMaker.	
Resource Explorer admite la búsqueda multicuenta	Ahora puede utilizar Resource Explorer para buscar y descubrir recursos en las Cuentas de AWS dentro de su organización o unidad organizativa. Para obtener más información, consulte Activar la búsqueda multicuenta.	14 de noviembre de 2023
Políticas administradas nuevas y actualizadas	Resource Explorer agregó soporte para AWS Organizations. Se han agregado y actualizado las políticas administradas de AWS para permitir que Resource Explorer acceda a su organización, estructura organizativa, cuentas y administradores delegados.	14 de noviembre de 2023
Se agregó compatibilidad con los nuevos tipos de recursos	Resource Explorer agregó soporte para AWS Organizations. Se han actualizado las políticas administradas de AWS para permitir que Resource Explorer acceda a su organización, estructura organizativa, cuentas y administradores delegados.	14 de noviembre de 2023

Se agregó compatibilidad con los nuevos tipos de recursos	Resource Explorer ahora admite 12 nuevos tipos de recursos de servicios como Amazon Cognito, AWS Elastic Beanstalk y Amazon Elastic File System.	18 de octubre de 2023
Se agregó compatibilidad con los nuevos tipos de recursos	Resource Explorer agregó soporte para 164 recursos. Se actualizaron las políticas administradas de AWS que permiten a Resource Explorer acceder a los recursos indexados para incluir esos nuevos tipos de recursos.	17 de octubre de 2023
Resource Explorer ya se encuentra disponible en algunas regiones en las que se permite la suscripción	Los clientes de BAH y CGK ahora pueden optar por usar Resource Explorer.	5 de octubre de 2023
Adición de compatibilidad con los nuevos tipos de recursos	Resource Explorer agregó compatibilidad con los siguientes recursos Servicios de AWS: AWS CodeBuild AWS CodePipeline, Amazon Cognito, Amazon Elastic Container Registry AWS Elastic Beanstalk, Amazon Elastic File System y AWS IoT. AWS Step Functions Se actualizaron las políticas administradas de AWS que permiten a Resource Explorer acceder a los recursos indexados para incluir esos nuevos tipos de recursos.	1 de agosto de 2023

Resource Explorer ahora permite exportar los resultados de la búsqueda a un CSV	Ahora puede exportar los resultados de la búsqueda en la página de Búsqueda de recursos a un archivo con formato CSV.	4 de abril de 2023
Úselo AWS Chatbot para buscar y descubrir sus recursos AWS	Ahora puede utilizarlos AWS Chatbot para buscar sus recursos mediante preguntas en lenguaje natural. Para obtener más información, consulte Uso de AWS Chatbot para buscar recursos .	30 de marzo de 2023
Se agregó compatibilidad con los nuevos tipos de recursos	Resource Explorer agregó soporte para recursos de los siguientes Servicios de AWS: Amazon ElastiCache y Amazon Simple Queue Service (Amazon SQS). AWS Lambda Se actualizaron las políticas administradas de AWS que permiten a Resource Explorer acceder a los recursos indexados para incluir esos nuevos tipos de recursos.	7 de marzo de 2023
Actualizaciones de las prácticas recomendadas de IAM	Guía actualizada para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte las Prácticas recomendadas de seguridad en IAM.	6 de diciembre de 2022

Nuevas políticas administradas AWS	Resource Explorer agrega AWSResourceExplorerFullAccess y AWSResourceExplorerServiceRolePolicy administra políticas. AWSResourceExplorerReadOnlyAccess	7 de noviembre de 2022
Versión inicial	Versión inicial de la Guía del usuario de Resource Explorer	7 de noviembre de 2022

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.