Guía del usuario

AWS Recursos de etiquetado y editor de etiquetas

Version 1.0

AWS Recursos de etiquetado y editor de etiquetas: Guía del usuario

Table of Contents

¿Qué es Tag Editor?

El editor de etiquetas le permite gestionar las etiquetas de forma eficaz. Las etiquetas son pares de claves y valores que actúan como metadatos para organizar AWS los recursos. En la mayoría de AWS los recursos, tiene la opción de añadir etiquetas al crear el recurso. Algunos ejemplos de recursos son una instancia de Amazon Elastic Compute Cloud (AmazonEC2), un bucket de Amazon Simple Storage Service (Amazon S3) o una entrada secreta. AWS Secrets Manager

> **Important**
>
> No almacene información de identificación personal (PII) ni ningún otro tipo de información confidencial o sensible en las etiquetas. Utilizamos etiquetas para prestarle servicios de facturación y administración. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar recursos. Puede crear etiquetas para clasificar los recursos según su finalidad, propietario, entorno u otro criterio.

Cada etiqueta tiene dos partes:

- Una clave de etiqueta (por ejemplo, `CostCenter`, `Environment` o `Project`). Las claves de etiqueta distinguen entre mayúsculas y minúsculas.
- Un valor de etiqueta (por ejemplo, `111122223333` o `Production`). Al igual que las claves de etiqueta, los valores de etiqueta distinguen entre mayúsculas y minúsculas.

> **Note**
>
> Si bien las claves de etiquetas distinguen entre mayúsculas y minúsculas, IAM tiene validaciones adicionales de IAM recursos para evitar la aplicación de claves de etiquetas que solo difieren en mayúsculas y minúsculas. Recomendamos no utilizar llaves que solo difieran en la carcasa. En su lugar, puede utilizar las políticas de control de servicios (SCPs), que proporcionan un control central sobre el número máximo de permisos disponibles para los IAM usuarios y las IAM funciones de su organización.

Métodos de etiquetado de recursos

Hay tres formas de añadir etiquetas a los AWS recursos:

- Servicio de AWS APIoperación: las API operaciones de etiquetado apoyaron directamente un Servicio de AWS. Para descubrir qué funcionalidad de etiquetado Servicio de AWS proporciona cada una de ellas, consulte la documentación del servicio en el índice de AWS documentación.
- Consola Tag Editor: algunos servicios admiten el etiquetado con la consola Tag Editor.
- Etiquetado de grupos de recursos API: la mayoría de los servicios también admiten el etiquetado mediante. AWS Resource Groups Tagging API

> **Note**
>
> También puede usar AWS Service Catalog TagOptions Library para administrar fácilmente las etiquetas de los productos aprovisionados. A TagOptiones un par clave-valor administrado en Service Catalog. No es una AWS etiqueta, pero sirve como plantilla para crear una AWS etiqueta basada en. TagOption

Puede etiquetar los recursos de todos los servicios que generan costos en AWS. Para los siguientes servicios, AWS recomienda una alternativa más reciente Servicios de AWS que admita el etiquetado para adaptarse mejor a los casos de uso de los clientes.

Amazon Cloud Directory	Amazon CloudSearch	Amazon Cognito Sync
AWS Data Pipeline	Amazon Elastic Transcoder	Amazon Machine Learning
AWS OpsWorks Stacks	Amazon S3 Glacier Direct	Amazon SimpleDB
Gestor WorkSpaces de aplicaciones de Amazon	AWS DeepLens	

Más información

Esta página proporciona información general sobre los AWS recursos de etiquetado. Para obtener más información sobre el etiquetado de los recursos de un AWS servicio en particular, consulte su documentación. Las siguientes son también fuentes de información útiles sobre el etiquetado:

- Para obtener información sobre el etiquetado AWS Resource Groups Tagging API, consulte la Guía de API referencia sobre el etiquetado de Resource Groups.
- Para obtener información sobre la funcionalidad de etiquetado que Servicio de AWS proporciona cada uno de ellos, consulte la documentación del servicio en el índice de AWS documentación.
- Para obtener información sobre el uso de etiquetas en IAM las políticas para ayudar a controlar quién puede ver sus AWS recursos e interactuar con ellos, consulte Controlar el acceso a y para IAM los usuarios y roles mediante etiquetas en la Guía del IAM usuario.

Mejores prácticas y estrategias

En estas secciones se proporciona información sobre las mejores prácticas y estrategias a la hora de etiquetar AWS los recursos y utilizar el editor de etiquetas.

Mejores prácticas de etiquetado

Al crear una estrategia de etiquetado para AWS los recursos, siga las prácticas recomendadas:

- No añada información de identificación personal (PII) ni ningún otro tipo de información confidencial o delicada en las etiquetas. Muchos AWS servicios, incluida la facturación, pueden acceder a las etiquetas. Las etiquetas no se han diseñado para usarse con información privada o confidencial.
- Utilice un formato estandarizado que distinga mayúsculas de minúsculas para las etiquetas y aplíquelo de forma coherente a todos los tipos de recursos.
- Tenga en cuenta las directrices de etiquetas que admiten múltiples propósitos, como administrar el control de acceso a recursos, el seguimiento de costos, la automatización y la organización.
- Use herramientas automatizadas para ayudar a administrar las etiquetas de recursos. El editor de etiquetas y el etiquetado de Resource Groups API permiten el control programático de las etiquetas, lo que facilita la administración, la búsqueda y el filtrado automáticos de etiquetas y recursos.

- Es mejor usar demasiadas etiquetas que pocas etiquetas.
- Recuerde que es fácil cambiar las etiquetas para adaptarlas a los requisitos empresariales cambiantes, pero tenga en cuenta las consecuencias de los cambios futuros. Por ejemplo, cambiar las etiquetas de control de acceso significa que también debe actualizar las políticas que hacen referencia a esas etiquetas y controlar el acceso a los recursos.
- Puede hacer cumplir automáticamente los estándares de etiquetado que su organización decida adoptar mediante la creación e implementación de políticas de etiquetas con AWS Organizations. Las políticas de etiquetas permiten especificar reglas de etiquetado que definen los nombres de clave válidos y los valores válidos para cada clave. Puede elegir solo monitorear, lo cual le da la oportunidad de evaluar y limpiar las etiquetas existentes. Una vez que las etiquetas cumplan con los estándares que haya elegido, podrá activar su cumplimiento en las políticas de etiquetas para evitar que se creen etiquetas que no cumplan con los requisitos. Para obtener más información, consulte Políticas de etiquetas en la Guía del usuario de AWS Organizations .

Prácticas recomendadas para la nomenclatura de etiquetas

Estas son algunas prácticas recomendadas y convenciones de nomenclatura que le recomendamos utilizar con sus etiquetas.

Los nombres clave de las AWS etiquetas distinguen entre mayúsculas y minúsculas, así que asegúrese de que se utilizan de forma coherente. Por ejemplo, las claves de etiquetas `CostCenter` y `costcenter` son diferentes. Una clave de etiqueta podría estar configurada como etiqueta de asignación de costos para análisis e informes financieros, mientras la otra clave de etiqueta podría no estar configurada para el mismo uso.

Varias etiquetas están predefinidas AWS o creadas automáticamente por varios Servicios de AWS. Muchos de los nombres de las etiquetas AWS que se generan utilizan minúsculas, guiones para separar las palabras del nombre y prefijos seguidos de dos puntos para identificar el servicio de origen de la etiqueta. Por ejemplo, consulte lo siguiente:

- `aws:ec2spot:fleet-request-id`es una etiqueta que identifica la solicitud de instancia EC2 puntual de Amazon que lanzó la instancia.
- `aws:cloudformation:stack-name` es una etiqueta que identifica la pila de AWS CloudFormation que creó el recurso.
- `elasticbeanstalk:environment-name` es una etiqueta que identifica la aplicación que creó el recurso.

Considere la posibilidad de asignar un nombre a las etiquetas mediante las siguientes reglas:

- Usar todas las palabras en minúsculas.
- Usar guiones para separar las palabras.
- Usar un prefijo seguido de dos puntos para identificar el nombre de la organización o el nombre abreviado.

Por ejemplo, para el nombre de una empresa ficticia AnyCompany, puede definir etiquetas como las siguientes:

- `anycompany:cost-center` para identificar el código interno del centro de costos.
- `anycompany:environment-type` para identificar si el entorno es de desarrollo, prueba o producción.
- `anycompany:application-id` para identificar la aplicación para la que se creó el recurso.

El prefijo garantiza que las etiquetas sean claramente reconocibles tal como las define su organización y no por AWS una herramienta de terceros que pueda estar utilizando. Usar todas minúsculas con guiones para los separadores evita confusiones sobre cómo poner en mayúsculas el nombre de una etiqueta. Por ejemplo, `anycompany:project-id` es más fácil de recordar que `ANYCOMPANY:ProjectID`, `anycompany:projectID` o bien `Anycompany:ProjectId`.

Límites y requisitos de nomenclatura de etiquetas

Los siguientes requisitos básicos de nomenclatura y uso se aplican a las etiquetas:

- Cada recurso puede tener un máximo de 50 etiquetas creadas por el usuario.
- Las etiquetas creadas por el sistema que comienzan por `aws:` están reservadas para uso de AWS y no cuentan con este límite. No puede editar ni eliminar una etiqueta que comience con el prefijo `aws:`.
- Para cada recurso, cada clave de etiqueta debe ser única y solo puede tener un valor.
- La clave de la etiqueta debe tener un mínimo de 1 y un máximo de 128 caracteres Unicode en UTF-8.
- El valor de la etiqueta debe ser un mínimo de 0 y un máximo de 256 caracteres Unicode en UTF-8.
- Los caracteres permitidos pueden variar según el AWS servicio. Para obtener información sobre los caracteres que puedes usar para etiquetar recursos en un AWS servicio concreto,

consulta su documentación. En general, los caracteres permitidos son letras, números, espacios representables en UTF -8 y los siguientes caracteres: _.:/= + - @.

- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Como práctica recomendada, decida una estrategia de uso de mayúsculas y minúsculas en las etiquetas e implemente esa estrategia sistemáticamente en todos los tipos de recursos. Por ejemplo, decida si se va a utilizar `Costcenter`, `costcenter` o `CostCenter` y utilice la misma convención para todas las etiquetas. Procure no utilizar etiquetas similares con un tratamiento de mayúsculas y minúsculas incoherente.

Estrategias habituales de etiquetado

Utilice las siguientes estrategias de etiquetado para ayudar a identificar y administrar recursos de AWS .

Contenido

Etiquetas para la organización de recursos

Las etiquetas son una buena forma de organizar AWS los recursos en. AWS Management Console Puede configurar etiquetas para que se muestren con recursos y puede buscar y filtrar por etiquetas. Con el AWS Resource Groups servicio, puede crear grupos de AWS recursos basados en una o más etiquetas o partes de etiquetas. También puede crear grupos en función de su aparición en una AWS CloudFormation pila. Con los grupos de recursos y el editor de etiquetas, puede consolidar y consultar datos de aplicaciones que consten de varios servicios, recursos y regiones en un solo lugar.

Etiquetas para la asignación de costos

AWS Cost Explorer y los informes de facturación detallados le permiten desglosar AWS los costos por etiqueta. Por lo general, se utilizan etiquetas empresariales como centro de costes o unidad de negocio, cliente o proyecto para asociar AWS los costes con las dimensiones tradicionales de

asignación de costes. Sin embargo, un informe de asignación de costos puede incluir cualquier etiqueta. Eso le permite asociar los costos con dimensiones técnicas o de seguridad, como aplicaciones, entornos o programas de conformidad específicos.

En el caso de algunos servicios, puede utilizar una `createdBy` etiqueta AWS generada por usted para asignar los costes, a fin de ayudar a contabilizar los recursos que, de otro modo, no estarían categorizados. La etiqueta `createdBy` solo está disponible para servicios y recursos de AWS compatibles. Su valor contiene datos asociados a eventos específicos API o de consola. Para obtener más información, consulte Etiquetas de asignación de costos generadas por AWS en la Guía del usuario de AWS Billing and Cost Management .

Etiquetas para la automatización

Las etiquetas específicas de recursos o servicios se utilizan a menudo para filtrar recursos durante las actividades de automatización. Las etiquetas de automatización se utilizan para incluir o excluir tareas automatizadas o para identificar versiones específicas de recursos para su archivado, actualización o eliminación. Por ejemplo, puede ejecutar los scripts automatizados `stop` o `start` que desactivan entornos de desarrollo durante horas no laborables para reducir costos. En este escenario, las etiquetas de instancia de Amazon Elastic Compute Cloud (AmazonEC2) son una forma sencilla de identificar las instancias para excluirse de esta acción. En el caso de los scripts que buscan y eliminan EBS instantáneas de Amazon obsoletas o continuas, las etiquetas de instantáneas pueden añadir una dimensión adicional a los criterios de búsqueda. out-of-date

Etiquetas para el control de acceso

IAMlas políticas admiten condiciones basadas en etiquetas, lo que te permite restringir IAM los permisos en función de etiquetas o valores de etiqueta específicos. Por ejemplo, los permisos de IAM usuario o rol pueden incluir condiciones para limitar las EC2 API llamadas a entornos específicos (como los de desarrollo, pruebas o producción) en función de sus etiquetas. Se puede utilizar la misma estrategia para limitar API las llamadas a redes específicas de Amazon Virtual Private Cloud (AmazonVPC). El soporte para IAM permisos a nivel de recursos basados en etiquetas es específico del servicio. Cuando utilice condiciones basadas en etiquetas para el control de acceso, asegúrese de definir y restringir quién puede modificar las etiquetas. Para obtener más información sobre el uso de etiquetas para controlar el API acceso a AWS los recursos, consulte los AWS servicios con los que funcionan IAM en la Guía del IAM usuario.

Control del etiquetado

Una estrategia de etiquetado eficaz utiliza etiquetas estandarizadas y las aplica de forma coherente y programática en todos los recursos. AWS Puede utilizar enfoques tanto reactivos como proactivos para controlar las etiquetas en su entorno. AWS

- La gobernanza reactiva sirve para encontrar recursos que no estén debidamente etiquetados mediante herramientas como Resource Groups API Reglas de AWS Config, Tagging y scripts personalizados. Para buscar recursos manualmente, puede usar el editor de etiquetas y los informes de facturación detallados.
- La gobernanza proactiva utiliza herramientas como Service Catalog AWS CloudFormation, políticas de etiquetas o permisos a IAM nivel de recursos para garantizar que las etiquetas estandarizadas se apliquen de forma coherente en la creación de los recursos. AWS Organizations

  Por ejemplo, puede usar la AWS CloudFormation `Resource Tags` propiedad para aplicar etiquetas a los tipos de recursos. En Service Catalog, puede agregar etiquetas de cartera y de productos que se combinen y se apliquen a un producto automáticamente cuando este se lance. Las formas más estrictas de gobierno proactivo incluyen tareas automatizadas. Por ejemplo, puede utilizar el etiquetado Resource Groups API para buscar las etiquetas de un AWS entorno o ejecutar scripts para poner en cuarentena o eliminar los recursos etiquetados de forma incorrecta.

Etiquetado de categorías

Las empresas que son más eficaces en el uso de etiquetas suelen crear agrupaciones de etiquetas relevantes para el negocio para organizar sus recursos en las dimensiones técnicas, de negocio y de seguridad. Las empresas que utilizan procesos automatizados para administrar su infraestructura también incluyen etiquetas adicionales específicas de automatización.

Etiquetas técnicas	Etiquetas para la automatización	Etiquetas comerciales	Etiquetas de seguridad
• Nombre: identifica recursos individuales. • ID de la aplicación: identifica los	• Fecha/Hora: identifica la fecha u hora en que se debe iniciar, parar, eliminar o rotar un recurso.	• Proyecto: identifica los proyectos que admite el recurso. • Propietario: identifica quién es	• Confidencialidad: un identificador para el nivel concreto de confidencialidad

Etiquetas técnicas	Etiquetas para la automatización	Etiquetas comerciales	Etiquetas de seguridad
recursos que están relacionados con una aplicación específica. • Rol de la aplicación: describe la función de un recurso determinado (como servidor web, agente de mensajes y base de datos). • Clúster: identifica granjas de recursos que comparten una configuración común y realizan una función específica para una aplicación. • Entorno: distingue entre recursos de desarrollo, prueba y producción. • Versión: ayuda a distinguir entre versiones de recursos o aplicaciones.	• Alta/Baja: indica si un recurso debe incluirse en una actividad automatizada, como iniciar, parar o cambiar el tamaño de instancias. • Seguridad: determine los requisitos, como el cifrado o la activación de los registros de VPC flujo de Amazon; identifique las tablas de enrutamiento o los grupos de seguridad que requieren un escrutinio adicional	responsable del recurso. • Centro de costos/unidad de negocio: identifica el centro de costos o la unidad de negocio asociados a un recurso, normalmente para la asignación y el seguimiento de costos. • Cliente: identifica un cliente específico o al que sirve un determinado grupo de recursos.	de los datos que admite un recurso. • Conformidad: un identificador para cargas de trabajo que deben cumplir requisitos específicos de conformidad.

Comience a usar el editor de etiquetas.

> **Important**
>
> No almacene información de identificación personal (PII) u otra información confidencial o sensible en las etiquetas. Utilizamos etiquetas para prestarle servicios de facturación y administración. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

Para añadir, editar o eliminar etiquetas de varios recursos a la vez, utilice el editor de etiquetas. Con el editor de etiquetas, busque los recursos que desee etiquetar y, a continuación, administre las etiquetas de los recursos que aparecen en los resultados de la búsqueda.

Para iniciar el editor de etiquetas

1. Inicie sesión en la AWS Management Console.
2. Lleve a cabo uno de los siguientes pasos:
   - Elija Servicios. A continuación, en Administración y gobernanza, seleccione Grupo de recursos y editor de etiquetas. En el panel de navegación de la izquierda, elija Editor de etiquetas.
   - Utilice el enlace directo: AWS Consola Tag Editor.

No todos los recursos admiten etiquetas. Para obtener información sobre los recursos compatibles con Tag Editor, consulte la columna de etiquetado del editor de etiquetas en Tipos de recursos compatibles en la AWS Resource Groups Guía del usuario. Si un tipo de recurso que quieres etiquetar no es compatible, deja AWS Para saberlo, selecciona Comentarios en la esquina inferior izquierda de la ventana de la consola.

Para obtener información acerca de los permisos y roles necesarios para etiquetar recursos, consulte Configuración de permisos.

Temas

Requisitos previos para trabajar con el editor de etiquetas

Antes de empezar a etiquetar tus recursos, asegúrate de tener una activa Cuenta de AWS con los recursos existentes y los derechos adecuados para etiquetar los recursos y crear grupos.

Temas

Inscríbase en una Cuenta de AWS

Si no tienes un Cuenta de AWS, complete los pasos siguientes para crear uno.

Para suscribirse a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
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 una Cuenta de AWS, un Usuario raíz de la cuenta de AWSse crea. El usuario root tiene acceso a todos Servicios de AWS y los recursos de la 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. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de suscribirse a una Cuenta de AWS, asegure su Usuario raíz de la cuenta de AWS, habilitar AWS IAM Identity Center y cree un usuario administrativo para no utilizar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

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

   Para obtener ayuda para iniciar sesión con un usuario root, consulte Iniciar sesión como usuario root en la AWS Sign-In Guía del usuario.
2. Activa la autenticación multifactorial (MFA) para tu usuario root.

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

Creación de un usuario con acceso administrativo

1. Habilite IAM Identity Center.

   Para obtener instrucciones, consulte Habilitar AWS IAM Identity Center en la AWS IAM Identity Center Guía del usuario.
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre el uso de 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 AWS IAM Identity Center Guía del usuario.

Iniciar sesión como usuario con acceso de administrador

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

  Para obtener ayuda para iniciar sesión con un usuario de IAM Identity Center, consulte Iniciar sesión en AWS acceda al portal en el AWS Sign-In Guía del 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 con privilegios mínimos.

Para obtener instrucciones, consulte Crear un conjunto de permisos en AWS IAM Identity Center Guía del usuario.

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para obtener instrucciones, consulte Añadir grupos en la AWS IAM Identity Center Guía del usuario.

Crear recursos de

Debe tener recursos en su Cuenta de AWS etiquetar. Para obtener más información sobre los tipos de recursos admitidos, consulte la columna Etiquetado del editor de etiquetas, en la sección Tipos de recursos admitidos, en AWS Resource Groups Guía del usuario.

Configuración de permisos

Para hacer pleno uso del editor de etiquetas, es posible que necesite más permisos para etiquetar recursos o para las claves de etiquetas y los valores de un recurso. Estos permisos se dividen en las categorías siguientes:

- Los permisos para los servicios individuales, para que pueda etiquetar los recursos de dichos servicios e incluirlos en los grupos de recursos.
- Los permisos necesarios para usar la consola del editor de etiquetas.

Si es administrador, puede proporcionar permisos a sus usuarios mediante la creación de políticas a través de AWS Identity and Access Management (IAM) servicio. Primero debe crear IAM roles, usuarios o grupos y, a continuación, aplicar las políticas con los permisos que necesitan. Para obtener información sobre cómo crear y adjuntar IAM políticas, consulte Trabajar con políticas.

Permisos para servicios individuales

> **Important**
>
> En esta sección se describen los permisos que se requieren si quieres etiquetar recursos de otros AWS consolas de servicio y APIs.

Para añadir etiquetas a un recurso, debe tener los permisos necesarios para el servicio al que pertenece el recurso. Por ejemplo, para etiquetar EC2 instancias de Amazon, debes tener permisos para las operaciones de etiquetado de ese servicioAPI, como Amazon EC2 CreateTagsoperación.

Permisos necesarios para utilizar la consola de Tag Editor

Para utilizar la consola de Tag Editor para enumerar y etiquetar recursos, se deben añadir los siguientes permisos a la declaración de política del usuario enIAM. Puede añadir cualquiera de los dos AWS políticas gestionadas que se mantienen y mantienen actualizadas mediante AWS, o puede crear y mantener su propia política personalizada.

Utilización AWS políticas gestionadas para los permisos del editor de etiquetas

El editor de etiquetas admite lo siguiente AWS políticas gestionadas que puede utilizar para proporcionar un conjunto predefinido de permisos a sus usuarios. Puede adjuntar estas políticas administradas a cualquier rol, usuario o grupo del mismo modo que lo haría con cualquier otra política que cree.

ResourceGroupsandTagEditorReadOnlyAccess

Esta política otorga al IAM rol o usuario asociado permiso para realizar operaciones de solo lectura en ambos casos AWS Resource Groups y Editor de etiquetas. Para leer las etiquetas de un recurso, también debe tener permisos para ese recurso mediante una política independiente. Obtenga más información en la siguiente nota importante.

ResourceGroupsandTagEditorFullAccess

Esta política otorga al IAM rol o usuario adjunto permiso para llamar a cualquier operación de Resource Groups y a las operaciones de etiquetas de lectura y escritura en Tag Editor. Para leer o escribir las etiquetas de un recurso, también debe tener permisos para ese recurso mediante una política independiente. Obtenga más información en la siguiente nota importante.

Important

Las dos políticas anteriores conceden permiso para llamar a las operaciones del editor de etiquetas y utilizar la consola del editor de etiquetas. Sin embargo, también debe tener los permisos no solo para invocar la operación, sino también los permisos adecuados para el recurso específico a cuyas etiquetas está intentando acceder. Para conceder ese acceso a las etiquetas, también debe asociar una de estas políticas:

- La AWS política gestionada ReadOnlyAccessconcede permisos a las operaciones de solo lectura para los recursos de cada servicio. AWS mantiene esta política actualizada automáticamente con las nuevas Servicios de AWS a medida que estén disponibles.
- Muchos servicios ofrecen servicios de solo lectura específicos AWS políticas gestionadas que puede utilizar para limitar el acceso únicamente a los recursos proporcionados por ese servicio. Por ejemplo, Amazon EC2 ofrece AmazonEC2ReadOnlyAccess.
- Puede crear su propia política que conceda acceso solo a las operaciones específicas de solo lectura para los pocos servicios y recursos a los que desea que accedan sus usuarios. Esta política utiliza una estrategia de lista de permitidos o una estrategia de lista de denegación.

  Una estrategia de lista de permitidos aprovecha el hecho de que el acceso está denegado de forma predeterminada hasta que se permita explícitamente en una política. Por lo tanto, puede utilizar una política como la del ejemplo siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to allow tagging>"
        }
    ]
}
```

  Como alternativa, puede utilizar una estrategia de lista de negación que permita el acceso a todos los recursos excepto a aquellos que bloquee explícitamente. Esto requiere una política independiente que se aplique a los usuarios relevantes y que permita el acceso. A continuación, el siguiente ejemplo de política deniega el acceso a los recursos específicos que figuran en el nombre del recurso de Amazon (ARN).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "tag:*" ],
```

```
            "Resource": "<ARNs of resources to disallow tagging>"
        }
    ]
}
```

Añadir los permisos del editor de etiquetas manualmente

- `tag:*` (Este permiso permite todas las acciones del editor de etiquetas. Si en su lugar desea restringir las acciones que están disponibles para un usuario, puede sustituir el asterisco por una acción específica o por una lista de acciones separadas por comas).
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`
- `resource-groups:SearchResources`
- `resource-groups:ListResourceTypes`

> **Note**
>
> El `resource-groups:SearchResources` permiso permite a Tag Editor enumerar los recursos al filtrar la búsqueda mediante claves o valores de etiqueta.
> El `resource-explorer:ListResources` permiso permite a Tag Editor enumerar los recursos cuando se buscan recursos sin definir las etiquetas de búsqueda.

Concesión de permisos para utilizar el editor de etiquetas

Para añadir una política de uso AWS Resource Groups y asigne un rol al Editor de etiquetas, haga lo siguiente.

1. Abre la IAMconsola en la página de roles.

2. Busque el rol al que desea conceder permisos del editor de etiquetas. Elija el nombre de la función para abrir la página Resumen de la función.
3. En la pestaña Permissions (Permisos), seleccione Add permissions (Añadir permisos).
4. Elija Adjuntar directamente políticas existentes.
5. Elija Crear política.
6. En la JSONpestaña, pegue la siguiente declaración de política.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:*",
        "resource-groups:SearchResources",
        "resource-groups:ListResourceTypes"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> Esta declaración de política de ejemplo concede permisos para realizar únicamente acciones del editor de etiquetas.

7. Elija Next: Tags (Siguiente: Etiquetas) y, a continuación, seleccione Next: Review (Siguiente: Revisar).
8. Escriba un nombre y la descripción de la nueva política. Por ejemplo, **`AWSTaggingAccess`**.
9. Elija Crear política.

Ahora que la política está guardadaIAM, puede adjuntarla a otros principios, como roles, grupos o usuarios. Para obtener más información sobre cómo agregar una política a un director, consulte Agregar y quitar permisos de IAM identidad en la Guía del IAM usuario.

Autorización y control de acceso basados en etiquetas

Servicios de AWS admiten lo siguiente:

- Políticas basadas en acciones: por ejemplo, puede crear una política que permita a los usuarios realizar `GetTagKeys` u operaciones `GetTagValues`, pero no el resto.
- Permisos a nivel de recursos en las políticas: muchos servicios permiten ARNsespecificar recursos individuales en la política.
- Autorización basada en etiquetas: muchos servicios admiten el uso de etiquetas de recursos en la condición de una política. Por ejemplo, puede crear una política que permita a los usuarios el acceso completo a un grupo que haya etiquetado. Para obtener más información, consulte ¿Para qué sirve ABAC AWS? en el AWS Identity and Access Management Guía del usuario.
- Credenciales temporales: los usuarios pueden asumir una función con una política que permita operaciones del editor de etiquetas.

El editor de etiquetas no utiliza ningún rol vinculado a servicios.

Para obtener más información sobre cómo se integra Tag Editor con AWS Identity and Access Management (IAM), consulte los siguientes temas en la AWS Identity and Access Management Guía del usuario:

- AWS servicios que funcionan con IAM
- Actions, resources, and condition keys for Tag Editor
- Controlar el acceso a AWS recursos mediante políticas

Búsqueda de recursos para etiquetar

Con el editor de etiquetas, puede crear una consulta para buscar recursos en uno o más Regiones de AWS que estén disponibles para etiquetar. Puede elegir hasta 20 tipos de recursos individuales o crear una consulta en All resource types (Todos los tipos de recurso). Su consulta puede incluir recursos que ya tengan etiquetas o que no las tengan. Para más información, consulte la columna Etiquetado del editor de etiquetas en Tipos de recursos admitidos en la Guía del usuario de AWS Resource Groups .

Después de buscar recursos para etiquetar, puede utilizar el editor de etiquetas para añadir, ver, editar o eliminar etiquetas.

Para buscar recursos para etiquetar

1. Abra la Consola del editor de etiquetas.
2. (Opcional) Elija la opción Regiones de AWS en la que desea buscar los recursos para etiquetarlos. Su región actual se usa de forma predeterminada. Para este procedimiento, elija us-east-1 y us-west-2.
3. Elija al menos un tipo de recurso de la lista desplegable Tipos de recurso. Puede añadir o editar etiquetas de hasta 20 tipos de recursos individuales a la vez o seleccionar All resource types (Todos los tipos de recursos). Para este procedimiento, elija AWS:: :Instance yEC2: :S3 AWS: :Bucket.
4. (Opcional) Introduzca una clave de etiqueta o un par de clave y valor de etiqueta en el campo Etiquetas para limitar los recursos de la Región de AWS actual a únicamente los etiquetados con sus valores especificados. Al introducir una clave de etiqueta, las claves de etiqueta coincidentes de la región actual aparecen en una lista. Puede elegir una clave de etiqueta de la lista. El editor de etiquetas completa de forma automática la clave de etiqueta a medida que introduce los caracteres suficientes para que coincida con una etiqueta existente. Elija Añadir o pulse Intro cuando haya terminado de definir la etiqueta. En este ejemplo, filtre los recursos que tienen una clave de etiqueta Etapa. El valor de la etiqueta es opcional, pero permite limitar aún más los resultados de la consulta. Para añadir más etiquetas, elija Añadir. Las consultas asignan un operador `AND` a las etiquetas, por lo que la consulta solo devuelve los recursos que coinciden tanto con el tipo de recurso especificado como con todas las etiquetas especificadas.

> **Note**
>
> La consola del editor de etiquetas no admite actualmente los caracteres comodín.

Para buscar recursos con varios valores para una clave de etiqueta, añada otra etiqueta con la misma clave a la consulta, pero especifique un valor distinto. Los resultados incluyen todos los recursos etiquetados con la misma clave de etiqueta y que tienen cualquiera de los valores seleccionados. La búsqueda distingue entre mayúsculas y minúsculas.

Deje las casillasEtiquetas vacías para buscar todos los recursos del tipo especificado en la Regiones de AWS seleccionada. Esta consulta devuelve los recursos que tienen alguna etiqueta e incluye los que no las tengan. Para eliminar una etiqueta de una consulta, seleccione X en el rótulo de la etiqueta.

Para buscar recursos que tengan una etiqueta, pero con un valor vacío, elija (valor vacío).

> **Note**
>
> Antes de que pueda buscar recursos con las etiquetas especificadas, estas se deben haber aplicado a al menos un recurso del tipo especificado en la Región de AWS actual.

5. Cuando su consulta esté lista, seleccione Search resources (Buscar recursos). Los recursos se muestran como una tabla en el área Resultados de la búsqueda de recursos.

   Para filtrar un gran número de recursos, introduzca cualquier texto de filtro, como una parte del nombre de un recurso, en Filter resources (Filtrar recursos).

   > **Note**
   >
   > Puede usar subcadenas para filtrar sus resultados.

6. (Opcional) Para configurar las columnas que Tag Editor muestra en los resultados de la búsqueda de recursos, selecciona el icono con forma de engranaje de preferencias en los resultados de la búsqueda de recursos.

En la página Preferences (Preferencias), seleccione el número de filas que desea que se muestren en sus resultados de búsqueda. Si desea ver todo el texto de la tabla, active la casilla Ajustar líneas.

Active las columnas que desea que el editor de etiquetas muestre en sus resultados. Puede mostrar una columna para cada etiqueta que aparezca en sus resultados de búsqueda o un subconjunto seleccionado de sus resultados de búsqueda. Puede hacerlo en cualquier momento después de encontrar recursos que etiquetar. Para activar una columna, seleccione el icono de interruptor situado junto a la etiqueta y cámbiela de desactivada a activada .

Cuando haya terminado de configurar las columnas visibles y el número de filas que se muestran, seleccione Confirm (Confirmar).

Vea y edite las etiquetas existentes de un recurso seleccionado

El editor de etiquetas le muestra las etiquetas que hay en los recursos seleccionados y que se encuentran en los resultados de la consulta de Buscar recursos para etiquetar.

Si habilitó alguna columna Etiquetas como se describe en la sección anterior, puede ver el valor actual de esa etiqueta para cada recurso en los resultados de la búsqueda.

> **Note**
>
> En este tema se explica cómo editar la etiqueta de un recurso individual. También puede editar en bloque las etiquetas de varios recursos seleccionados al mismo tiempo. Para obtener más información, consulte Administración de etiquetas con el editor de etiquetas.

Para editar las etiquetas en línea en la tabla de resultados de búsqueda

1. Seleccione el valor de la etiqueta del recurso que desea editar.

   > **Note**
   >
   > - Si el recurso elegido no tiene actualmente una etiqueta con la clave elegida, el valor se muestra como (no etiquetado).

- Si el recurso elegido tiene una etiqueta con la clave elegida pero sin valor, el valor se muestra como “–”.

2. Puede introducir un valor nuevo o elegir uno de los valores que ya están presentes en otros recursos con esta etiqueta. También puede eliminar la etiqueta de este recurso si elige Eliminar etiqueta.

Para ver todas las etiquetas de un recurso individual

1. En los resultados de la consulta de Buscar recursos para etiquetar, seleccione un número en la columna Etiquetas de cualquier recurso del que desea ver las etiquetas existentes. Los recursos con una raya en la columna Tags (Etiquetas) no tienen etiquetas existentes.
2. Ver etiquetas existentes en Resource tags (Etiquetas de recursos). También puede abrir esta ventana seleccionando Gestionar etiquetas de recursos seleccionados, cuando esté cambiando o eliminando etiquetas de la página Gestionar etiquetas.

> **Note**
>
> Si no ve la etiqueta que ha aplicado recientemente a un recurso, intente actualizar la ventana del navegador.

Exportar resultados al archivo .csv

Puede exportar los resultados de una consulta de Buscar recursos para etiquetar a un archivo de valores separados por comas (.csv). El archivo.csv incluye los nombres de los recursos, los servicios, la regiónIDs, el recurso, el número total de etiquetas y una columna para cada clave de etiqueta única de la colección. El archivo .csv puede ayudarle a desarrollar una estrategia de etiquetado para los recursos de su organización o a determinar si hay superposiciones o inconsistencias en el etiquetado de los recursos.

1. En los resultados de la consulta Buscar recursos para etiquetar, selecciona Exportar recursos a CSV.
2. Cuando su navegador se lo solicite, elija abrir el archivo .csv o guárdelo en una ubicación adecuada.

Administración de etiquetas con el editor de etiquetas

Después de buscar recursos que desea etiquetar, puede añadir, eliminar y editar las etiquetas para todos o algunos de los resultados de la búsqueda. El editor de etiquetas muestra las etiquetas que se asocian a los recursos. También muestra si esas etiquetas se agregaron en el Editor de etiquetas, mediante la consola de servicio del recurso o medianteAPI.

Important

No almacene información de identificación personal (PII) u otra información confidencial o sensible en las etiquetas. Utilizamos etiquetas para prestarle servicios de facturación y administración. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

Otras formas de administración de etiquetas

En este tema se tratan los recursos de etiquetado mediante el editor de etiquetas en el AWS Management Console. Sin embargo, también puedes gestionar las etiquetas de tu AWS recursos mediante las siguientes herramientas:

- Puede escribir o programar comandos en el intérprete de comandos mediante los `resourcegroupstaggingapi`comandos de AWS Command Line Interface (AWS CLI).
- Puede crear y ejecutar PowerShell scripts mediante el AWS Resource Groups Etiquetado API en el AWS Tools for PowerShell Core.
- Puede crear y ejecutar programas con cualquiera de los disponibles AWS SDKsmediante el etiquetado de grupos de recursos APIs, como el etiquetado para APIs Python o el etiquetado APIs para Java.

Al añadir, eliminar o editar las etiquetas existentes, solo las estará cambiando en aquellos recursos que ha seleccionado los resultados de la consulta de Buscar recursos para etiquetar. Puede seleccionar hasta 500 recursos en los que se vaya a administrar las etiquetas.

Añadir etiquetas a recursos seleccionados

Puede utilizar el editor de etiquetas para añadir las etiquetas a los recursos seleccionados que se encuentran en los resultados de la consulta de Buscar recursos para etiquetar.

> **Note**
>
> Este tema describe cómo editar de forma masiva las etiquetas de varios recursos. También puede editar los valores de las etiquetas de un recurso individual. Para obtener más información, consulte Vea y edite las etiquetas existentes de un recurso seleccionado.

1. Abra la consola del editor de etiquetas y envíe una consulta que devuelva varios recursos que desee etiquetar.
2. En la tabla de los resultados de la consulta de Buscar recursos para etiquetar, seleccione las casillas de verificación que se encuentran junto a los recursos a los que desea añadir las etiquetas. Escriba una cadena de texto en Filtrar recursos en la parte superior de la tabla para filtrar en función de una parte del nombre del recurso, el ID, las claves de etiquetas o los valores de etiqueta. En la columna Etiquetas, tenga en cuenta que los recursos que se encuentran en los resultados ya tiene etiquetas aplicadas.
3. Seleccione la casilla de verificación de uno o más recursos y, a continuación, elija Administrar las etiquetas de los recursos seleccionados.
4. En la página Manage tags (Administrar etiquetas) puede ver las etiquetas de los recursos que ha seleccionado. Aunque su consulta original obtenga más recursos, solo está añadiendo etiquetas a aquellos recursos que ha seleccionado en el paso 1. Seleccione Agregar etiqueta.
5. Introduzca una clave de etiqueta y un valor de etiqueta opcional. Para este procedimiento, agregará la clave de etiqueta **`Team`** y el valor de la etiqueta **`Development`**.

   > **Note**
   >
   > Un recurso puede tener un máximo de 50 etiquetas aplicadas por el usuario. Es posible que no puedas añadir nuevas etiquetas a un recurso si te acercas a las 50 etiquetas aplicadas por los usuarios. AWS las etiquetas generadas no se aplican al límite de 50 etiquetas. Las claves de etiqueta también tienen que ser únicas en los recursos seleccionados. No puede añadir una etiqueta nueva con una clave que coincida con una clave de etiqueta que ya existe en los recursos seleccionados.

6. Una vez que haya terminado la adición de etiquetas, seleccione Revisar y aplicar cambios.
7. Si acepta los cambios, seleccione Aplicar cambios a todos los seleccionados.
8. En función del número de recursos que seleccione, la aplicación de etiquetas nuevas puede tardar unos minutos. No salga de la página ni abra una página diferente en la misma pestaña del navegador. Si los cambios se han llevado a cabo correctamente, se muestra un banner verde que informa que se han realizado correctamente en la parte superior de la página. Espere a que aparezca un banner que indique si la operación se ha realizado correctamente o no.

   Si los cambios de etiquetas a algunos o todos los recursos no se han llevado a cabo correctamente, consulte Solución de problemas de cambios de etiquetas. Después de resolver los cambios de etiquetas que no se hayan realizado correctamente (como permisos insuficientes), puede volver a intentar los cambios de las etiquetas en los recursos en los que los cambios de etiquetas fallaron. Para obtener más información, consulte the section called “Volver a intentar los cambios de etiquetas erróneos”.

Editar las etiquetas de los recursos seleccionados

Puede utilizar el editor de etiquetas para cambiar los valores de las etiquetas existentes en los recursos seleccionados que se encuentran en los resultados de la consulta de Buscar recursos para etiquetar. Al editar una etiqueta se cambia el valor de la etiqueta en todos los recursos seleccionados que tienen la misma clave de etiqueta. No se puede cambiar el nombre de una clave de etiqueta, pero puede eliminar una etiqueta y crear otra con un nombre nuevo para sustituir la clave de etiqueta original. Esta operación elimina todas las etiquetas con esa clave en los recursos seleccionados.

> **Important**
>
> No almacene información de identificación personal (PII) u otra información confidencial o sensible en las etiquetas. Utilizamos etiquetas para prestarle servicios de facturación y administración. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

1. En los resultados de la consulta de Buscar recursos para etiquetar, seleccione las casillas de verificación que se encuentran junto a los recursos a los que desea cambiar las etiquetas existentes. Escriba una cadena de texto en Filtrar recursos para filtrar en función de una parte del nombre del recurso o el ID. En la columna Etiquetas, tenga en cuenta que los recursos que se encuentran en los resultados ya tiene etiquetas aplicadas.

2. Seleccione Administrar las etiquetas de los recursos seleccionados.
3. En la página Administrar etiquetas, en Editar las etiquetas de los recursos seleccionados, vea las etiquetas del recurso que ha seleccionado. Aunque su consulta original podría haber obtenido más recursos, solo está cambiando las etiquetas para aquellos recursos que ha seleccionado en el paso 1.
4. Cambiar, añadir o eliminar valores de etiqueta. Las etiquetas existentes deben tener una clave de etiqueta, pero los valores de etiqueta son opcionales.

   En este procedimiento, cambiamos el valor de la etiqueta **`Team`** a **`QA`**.

   Si los recursos de su selección tienen valores diferentes para la misma clave, Los recursos seleccionados tienen valores de etiqueta diferentes se muestra en el campo Valor de etiqueta. En este caso, al colocar el cursor en la casilla se abre una lista desplegable con todos los valores disponibles para esta clave de etiqueta en los recursos seleccionados.

   Si los recursos de su selección tienen el valor de etiqueta que desea, el valor de etiqueta aparece resaltado cuando lo escribe. Por ejemplo, si los recursos de su selección ya tienen el valor de etiqueta **`QA`**, el valor aparece resaltado cuando escribe **`Q`**. Los valores de la lista desplegable ayudan a mantener la coherencia de los valores de etiqueta en los recursos. El valor de la etiqueta se cambia en todos los recursos seleccionados. En este ejemplo, el valor de la etiqueta cambia a **`QA`** en todos los recursos seleccionados que tenían una clave de etiqueta **`Team`**. En los recursos seleccionados que no tienen la etiqueta **`Team`**, se añade la etiqueta **`Team`** con el valor **`QA`**.
5. Una vez que haya terminado el cambio de etiquetas, seleccione Revisar y aplicar cambios.
6. Si acepta los cambios, seleccione Aplicar cambios a todos los seleccionados.
7. En función del número de recursos que ha seleccionado, la edición de etiquetas nuevas puede tardar unos minutos. No salga de la página ni abra una página diferente en la misma pestaña del navegador. Si los cambios se han llevado a cabo correctamente, se muestra un banner verde que informa que se han realizado correctamente en la parte superior de la página. Espere a que aparezca un banner que indique si la operación se ha realizado correctamente o no.

   Si los cambios de etiquetas a algunos o todos los recursos no se han llevado a cabo correctamente, consulte Solución de problemas de cambios de etiquetas. Después de resolver las causas principales de que no se hayan realizado correctamente los cambios de etiquetas (como permisos insuficientes), puede volver a intentar los cambios de etiquetas en los recursos en los que los cambios de etiquetas fallaron. Para obtener más información, consulte the section called “Volver a intentar los cambios de etiquetas erróneos”.

Eliminar etiquetas de los recursos seleccionados

Puede utilizar el editor de etiquetas para eliminar las etiquetas de los recursos seleccionados que se encuentran en los resultados de la consulta de Buscar recursos para etiquetar. Al eliminar una etiqueta, se elimina la etiqueta de todos los recursos seleccionados que tengan la etiqueta. Dado que no puede editar las claves de etiqueta, puede eliminar las etiquetas y sustituirlas por nuevas etiquetas si necesita editar una clave de etiqueta. Esta operación elimina todas las etiquetas con esa clave en los recursos seleccionados.

1. En los resultados de la consulta de Buscar recursos para etiquetar, seleccione las casillas de verificación que se encuentran junto a los recursos de los que desea eliminar las etiquetas. Escriba una cadena de texto en Filtrar recursos para filtrar en función de una parte del nombre del recurso o el ID.
2. Seleccione Administrar las etiquetas de los recursos seleccionados.
3. En la página Administrar etiquetas, en Editar las etiquetas de los recursos seleccionados, vea las etiquetas de los recursos que ha seleccionado. Aunque su consulta original podría haberle obtenido más recursos, solo está cambiando etiquetas de aquellos recursos que ha seleccionado en el paso 1.
4. Seleccione la opción Eliminar etiqueta situada junto a cualquiera de las etiquetas que desea eliminar. En este procedimiento, eliminaremos la etiqueta de **`Team`**.

   > **Note**
   >
   > Al seleccionar Eliminar etiqueta, se elimina una etiqueta de todos los recursos seleccionados que tengan la etiqueta.

5. Seleccione Revisar y aplicar cambios.
6. En la página de confirmación, seleccione Aplicar cambios a todos los seleccionados.
7. En función del número de recursos que ha seleccionado, la eliminación de las etiquetas nuevas puede tardar unos minutos. No salga de la página ni abra una página diferente en la misma pestaña del navegador. Si los cambios se han llevado a cabo correctamente, se muestra un banner verde que informa que se han realizado correctamente en la parte superior de la página. Espere a que aparezca un banner que indique si la operación se ha realizado correctamente o no.

   Si los cambios de etiquetas a algunos o todos los recursos no se han llevado a cabo correctamente, consulte Solución de problemas de cambios de etiquetas. Después de resolver

las causas principales de que no se hayan realizado correctamente los cambios de etiquetas (como permisos insuficientes), puede volver a intentar los cambios de etiquetas en los recursos en los que los cambios de etiquetas fallaron. Para obtener más información, consulte the section called “Volver a intentar los cambios de etiquetas erróneos”.

Uso de etiquetas en las políticas de IAM permisos

AWS Identity and Access Management (IAM) es la Servicio de AWS que se utiliza para crear y administrar las políticas de permisos que determinan quién puede acceder a sus AWS recursos. Cada intento de acceder a un AWS servicio o leer o escribir un AWS recurso está controlado por una IAM política.

Estas políticas le permiten proporcionar acceso detallado a los recursos. Una de las características que puede utilizar para ajustar este acceso es el elemento `Condition` de la política. Este elemento le permite especificar las condiciones que debe cumplir la solicitud para determinar si la solicitud puede continuar. Entre las cosas que puede comprobar con el elemento `Condition` se encuentran las siguientes:

- Las etiquetas asociadas al usuario o rol que realiza la solicitud.
- Etiquetas adjuntas al recurso objeto de la solicitud.

Etiquetas de control de acceso basado en atributos

Las etiquetas pueden ser una parte importante de su estrategia de control de AWS acceso. Para obtener información sobre el uso de etiquetas como atributos en una estrategia de control de acceso basada en atributos (ABAC), consulte Controlar el acceso a AWS los recursos mediante etiquetas y Controlar el acceso a y para IAM los usuarios y las funciones mediante etiquetas, ambas en la Guía del IAMusuario.

Hay un tutorial completo que muestra cómo conceder acceso a diferentes proyectos y grupos mediante etiquetas en el IAMtutorial: Definir los permisos de acceso a los AWS recursos en función de las etiquetas de la Guía del AWS Identity and Access Management usuario.

Si utilizas un proveedor de identidad (IdP) SAML basado en el inicio de sesión único, puedes adjuntar etiquetas a los roles asumidos que proporcionan acceso a tus usuarios. Para obtener más información, consulte el IAMtutorial: Uso de etiquetas de SAML sesión ABAC en la Guía del AWS Identity and Access Management usuario.

Claves de condición relacionadas con etiquetas

En la siguiente tabla se describen las claves de condición que puede utilizar en una política de IAM permisos para controlar el acceso en función de las etiquetas. Estas claves de condición le permiten hacer lo siguiente:

- Comparar las etiquetas de la entidad principal que realiza la operación.
- Comparar las etiquetas proporcionadas con la operación como parámetro.
- Comparar las etiquetas asociadas a un recurso al que accedería la operación.

Para obtener más detalles sobre una clave de condición y cómo utilizarla, consulte la página enlazada en la columna Nombre de clave de condición.

Nombre de clave de condición	Descripción
aws:PrincipalTag	Compara la etiqueta adjunta al principal (IAMrol o usuario) que realiza la solicitud con la etiqueta que se especifica en la política.
aws:RequestTag	Compara el par clave-valor de etiqueta que se transfirió en la solicitud como un parámetro con el par de etiquetas clave-valor especificado en la política.
aws:ResourceTag	Compara el par clave-valor que se adjunta al recurso con el par clave-val or de la etiqueta que se especifica en la política.
aws:TagKeys	Compara solo las claves de etiqueta de la solicitud con las claves que se especifican en la política.

Ejemplos de IAM políticas que utilizan etiquetas

Example Ejemplo 1: obligar a los usuarios a adjuntar una etiqueta específica al crear un recurso

El siguiente ejemplo de política de IAM permisos muestra cómo obligar al usuario que crea o modifica las etiquetas de una IAM política a incluir una etiqueta con la clave`0wner`. Además, la política requiere que el valor de la etiqueta `0wner` se establezca en el mismo valor que la etiqueta actualmente adjunta a la entidad principal de seguridad de llamada. Para que esta estrategia

funcione, todas las entidades principales deben tener una etiqueta `0wner` adjunta y se debe impedir que los usuarios modifiquen esa etiqueta. Si se intenta crear o modificar una política sin incluir la etiqueta `0wner`, la política no coincide y la operación no está permitida.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagCustomerManagedPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:TagPolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:policy/*",
            "Condition": {
                "StringEquals": {"aws:RequestTag/Owner": "${aws:PrincipalTag/Owner}"}
            }
        }
    ]
}
```

Example Ejemplo 2: usar etiquetas para limitar el acceso a un recurso a su “propietario”

El siguiente ejemplo de política de IAM permisos permite al usuario detener una EC2 instancia de Amazon en ejecución solo si el principal que realiza la llamada está etiquetado con el mismo valor de `project` etiqueta que la instancia.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances"
      ],
      "Resource": [
        "arn:aws:iam::123456789012:instance/*"
      ],
      "Condition": {
        "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/project}"}
```

```
      }
    }
  ]
}
```

Este ejemplo es un ejemplo de control de acceso basado en atributos () ABAC. Para obtener más información y ejemplos adicionales sobre el uso de IAM políticas para implementar una estrategia de control de acceso basada en etiquetas, consulte los siguientes temas de la Guía del AWS Identity and Access Management usuario:

- Controlar el acceso a AWS los recursos mediante etiquetas
- Controlar el acceso a y para IAM los usuarios y roles mediante etiquetas
- IAMtutorial: Defina los permisos de acceso a AWS los recursos en función de las etiquetas: muestra cómo conceder acceso a diferentes proyectos y grupos mediante varias etiquetas.

AWS Organizations políticas de etiquetas

Una política de etiquetas es un tipo de política que se crea en AWS Organizations. Puede utilizar las políticas de etiquetas para ayudar a estandarizar las etiquetas en todos los recursos de las cuentas de su organización. Para utilizar las políticas de etiquetas, te recomendamos que sigas los flujos de trabajo que se describen en la sección Introducción a las políticas de etiquetas de la AWS Organizations Guía del usuario. Como se menciona en esa página, los flujos de trabajo recomendados incluyen buscar y corregir etiquetas que no cumplan con los requisitos. Para ejecutar estas tareas, se utiliza la consola del editor de etiquetas.

Requisitos previos y permisos

Antes de poder evaluar el cumplimiento de las políticas de etiquetas en el editor de etiquetas, debe cumplir los requisitos y establecer los permisos necesarios.

Temas

Requisitos previos para evaluar el cumplimiento de las políticas de etiquetas

La evaluación del cumplimiento de las políticas de etiquetas requiere lo siguiente:

- Primero debe activar la función en AWS Organizations, y crear y adjuntar políticas de etiquetas. Para obtener más información, consulte las siguientes páginas del AWS Organizations Guía del usuario:
  - Requisitos previos y permisos para administrar las políticas de etiquetas
  - Habilitación de las políticas de etiquetas
  - Introducción a las políticas de etiquetas
- Para encontrar etiquetas no conformes en los recursos de una cuenta, necesita credenciales de inicio de sesión para esa cuenta y los permisos enumerados en Permisos para evaluar el cumplimiento de una cuenta.

- Para evaluar el cumplimiento en toda la organización, necesita credenciales de inicio de sesión para la cuenta de gestión de la organización y los permisos enumerados en Permisos para evaluar el cumplimiento en toda la organización . Puede solicitar el informe de conformidad únicamente en el Región de AWS Este de EE. UU. (Virginia del Norte).

Permisos para evaluar el cumplimiento de una cuenta

Para encontrar etiquetas no conformes en los recursos de una cuenta se requieren los permisos siguientes:

- `organizations:DescribeEffectivePolicy`: para obtener el contenido de la política de etiquetas vigente para la cuenta.
- `tag:GetResources`: para obtener una lista de los recursos que no cumplen con la política de etiquetas adjunta.
- `tag:TagResources`: para agregar o actualizar etiquetas. También necesita permisos específicos del servicio para crear etiquetas. Por ejemplo, para etiquetar recursos en Amazon Elastic Compute Cloud (AmazonEC2), necesitas permisos para`ec2:CreateTags`.
- `tag:UnTagResources`: para eliminar una etiqueta. También necesita permisos específicos del servicio para eliminar etiquetas. Por ejemplo, para eliminar la etiqueta de los recursos en AmazonEC2, necesitas permisos para`ec2:DeleteTags`.

El siguiente ejemplo AWS Identity and Access Management La política (IAM) proporciona permisos para evaluar el cumplimiento de las etiquetas de una cuenta.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:GetResources",
                "tag:TagResources",
                "tag:UnTagResources"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Para obtener más información sobre IAM las políticas y los permisos, consulta la Guía del IAM usuario.

Permisos para evaluar el cumplimiento en toda la organización

Para evaluar el cumplimiento de las políticas de etiquetas en toda la organización, se requieren los permisos siguientes:

- `organizations:DescribeEffectivePolicy`: para obtener el contenido de la política de etiquetas adjunta a la organización, unidad organizativa (OU) o cuenta.
- `tag:GetComplianceSummary`: para obtener un resumen de los recursos no conformes en todas las cuentas de la organización.
- `tag:StartReportCreation`: para exportar los resultados de la evaluación de conformidad más reciente a un archivo. El cumplimiento en toda la organización se evalúa cada 48 horas.
- `tag:DescribeReportCreation`: para comprobar el estado de la creación de informes.
- `s3:ListAllMyBuckets`— Para facilitar el acceso al informe de cumplimiento de toda la organización.
- `s3:GetBucketAcl`— Inspeccionar la lista de control de acceso (ACL) del bucket de Amazon S3 que recibe el informe de conformidad.
- `s3:GetObject`— Para recuperar el informe de conformidad del bucket de Amazon S3 propiedad del servicio.
- `s3:PutObject`— Colocar el informe de conformidad en el bucket de Amazon S3 especificado.

El siguiente ejemplo de IAM política proporciona permisos para evaluar el cumplimiento en toda la organización. Sustituya cada uno *`placeholder`* con tu propia información:

- *`bucket_name`* — El nombre de su bucket de Amazon S3
- *`organization_id`* — El ID de su organización

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:StartReportCreation",
                "tag:DescribeReportCreation",
                "tag:GetComplianceSummary",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GetBucketAclForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GetObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::*/tag-policy-compliance-reports/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "PutObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                },
                "StringLike": {
                    "s3:x-amz-copy-source": "*/tag-policy-compliance-reports/*"
```

```
                }
            }
        }
    ]
}
```

Para obtener más información sobre IAM las políticas y los permisos, consulte la Guía del IAM usuario.

Política de bucket de Amazon S3 para el almacenamiento de informes

Para crear un informe de conformidad para toda la organización, la identidad que utilices para llamar `StartReportCreation` API debe tener acceso a un depósito de Amazon Simple Storage Service (Amazon S3) en la región EE.UU. Este (Norte de Virginia) para almacenar el informe. Tag Policies utiliza las credenciales de la identidad que realiza la llamada para enviar el informe de conformidad al segmento especificado.

Si el bucket y la identidad que se utiliza para llamar `StartReportCreation` API pertenecen a la misma cuenta, no se necesitan políticas de bucket adicionales de Amazon S3 para este caso de uso.

Si la cuenta asociada a la identidad utilizada para llamar a la cuenta `StartReportCreation` API es diferente de la cuenta propietaria del bucket de Amazon S3, se debe adjuntar al bucket la siguiente política de bucket. Sustituya cada una *`placeholder`* con tu propia información:

- *`bucket_name`* — El nombre de su bucket de Amazon S3
- *`organization_id`* — El ID de su organización
- *`identidad_ ARN`* — La ARN de la IAM identidad utilizada para llamar a la `StartReportCreation` API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccountTagPolicyACL",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name"
```

```
        },
        {
            "Sid": "CrossAccountTagPolicyBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/*"
        }
    ]
}
```

Evaluación del cumplimiento de una cuenta

Puede evaluar la conformidad de una cuenta de su organización con su política de etiquetas efectiva.

> **Important**
>
> Los recursos no etiquetados no aparecen como no conformes en los resultados. Para buscar recursos sin etiquetar en tu cuenta, utilízalos Explorador de recursos de AWS con una consulta que utilice**`tag:none`**. Para obtener más información, consulte Búsqueda de recursos para etiquetar en la Guía del usuario de Explorador de recursos de AWS .

La política de etiquetas en vigor especifica las reglas de etiquetado que se aplican a una cuenta. La política de etiquetas en vigor es la suma de cualquier política de etiquetas que herede la cuenta, además de cualquier política de etiquetas asociada directamente a la cuenta. Cuando se asocia una política de etiquetas a la raíz de la organización, esta se aplica a todas las cuentas de la organización. Al adjuntar una política de etiquetas a una unidad organizativa (OU), se aplica a todas las cuentas OUs que pertenezcan a la OU.

> **Note**
>
> Si aún no ha creado políticas de etiquetas, consulte Introducción a las políticas de etiquetas en la Guía del usuario de AWS Organizations .

Para encontrar etiquetas que no estén en conformidad con los siguientes permisos:

- `organizations:DescribeEffectivePolicy`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`

Para evaluar el cumplimiento por parte de una cuenta de su política de etiquetas vigente (consola)

1. Mientras está conectado a la cuenta cuyo cumplimiento desea comprobar, abra la Consola de políticas de etiquetas.
2. La sección Política de etiquetas vigente muestra cuándo se actualizó por última vez la política y las claves de etiquetas definidas. Puede ampliar una clave de etiqueta para ver información sobre sus valores, tratamiento de casos y si los valores se aplican a tipos de recursos específicos.

   > **Note**
   >
   > Si ha iniciado sesión en la cuenta de administración, debe elegir una cuenta para ver su política vigente y ver la información de cumplimiento.

3. En la sección Recursos con etiquetas no conformes, especifica en qué etiquetas buscar Región de AWS las que no cumplen los requisitos. Si lo desea, también puede buscar por tipo de recurso. Seleccione Buscar recursos.

   Los resultados en tiempo real se muestran en la sección Resultados de búsqueda. Para cambiar el número de resultados devueltos por página o las columnas que se van a mostrar, seleccione el icono de configuración.
4. En los resultados de búsqueda, seleccione un recurso con etiquetas no conformes.
5. En el cuadro de diálogo que enumera las etiquetas del recurso, seleccione el hipervínculo para abrir el Servicio de AWS donde se creó el recurso. Desde esa consola, corrija la etiqueta no conforme.

   > **Tip**
   >
   > Si no tiene la certeza de qué etiquetas no cumplen la normativa, vaya a la sección Política de etiquetas en vigor para la cuenta en la consola Políticas de etiquetas. Puede expandir una clave de etiqueta para ver sus reglas de etiquetado.

6. Repita el proceso de búsqueda y corrección de etiquetas hasta que los recursos de la cuenta que le interesen cumplan los requisitos de cada región.

Para buscar etiquetas que no cumplan con los requisitos (AWS CLI, AWS API)

Utilice los siguientes comandos y operaciones para encontrar etiquetas no conformes:

- AWS Command Line Interface (AWS CLI):
  - aws resourcegroupstaggingapi get-resources
  - aws resourcegroupstaggingapi tag-resources
  - aws resourcegroupstaggingapi untag-resources

  Para ver el procedimiento completo de uso de las políticas de etiquetas en el AWS CLI, consulte Uso de políticas de etiquetas AWS CLI en la Guía del AWS Organizations usuario.
- AWS Resource Groups Tagging API:
  - GetResources
  - TagResources
  - UntagResources

Siguientes pasos

Le recomendamos que repita el proceso de detección y corrección de los problemas de cumplimiento. Continúe hasta que los recursos de la cuenta que le interesan cumplan con la política de etiquetas vigente en cada región.

La detección y corrección de etiquetas no conformes es un proceso iterativo por múltiples razones, entre ellas las siguientes:

- El uso de las políticas de etiquetas por parte de su organización puede evolucionar con el tiempo.
- A la hora de crear recursos, se necesita tiempo para que se produzcan cambios en la organización.
- El cumplimiento puede cambiar cada vez que se crea un nuevo recurso o cuando se asignan nuevas etiquetas a un recurso.
- La política de etiquetas en vigor de una cuenta se actualiza cada vez que una política de etiquetas se adjunta o se separa de ella. La política de etiquetas vigente también se actualiza cada vez que se producen cambios para etiquetar las políticas que hereda la cuenta.

Si ha iniciado sesión como cuenta de administración de la organización, también puede generar un informe. Este informe muestra información sobre los recursos etiquetados en las cuentas de su organización. Para obtener más información, consulte Evalúe el cumplimiento en toda la organización.

Evalúe el cumplimiento en toda la organización

Puede evaluar el cumplimiento por parte de su organización de su política de etiquetado en vigor. Puede generar un informe que muestra todos los recursos etiquetados en las cuentas de la organización y si cada recurso cumple con la política de etiquetas efectiva.

> **Important**
>
> Los recursos no etiquetados no aparecen como no conformes en los resultados. Para buscar recursos sin etiquetar en tu cuenta, usa Explorador de recursos de AWS con una consulta que utilice**`tag:none`**. Para obtener más información, consulte Buscar recursos sin etiquetar en el Explorador de recursos de AWS Guía del usuario.

Puede generar el informe desde la cuenta de administración de su organización en el `us-east-1` Región de AWS únicamente. La cuenta que genera el informe debe tener acceso a un bucket de Amazon S3 en la región Este de EE. UU. (Norte de Virginia). El bucket debe tener una política de bucket asociada como se muestra en Amazon S3 bucket policy for storing report.

Para generar un informe de conformidad de toda la organización, debe contar con los permisos siguientes:

- `organizations:DescribeEffectivePolicy`
- `tag:GetComplianceSummary`
- `tag:StartReportCreation`
- `tag:DescribeReportCreation`
- `s3:ListAllMyBuckets`
- `s3:GetBucketAcl`
- `s3:GetObject`
- `s3:PutObject`

Para ver un ejemplo IAM de política que muestre estos permisos, consulta los permisos para evaluar el cumplimiento en toda la organización.

Generación de un informe de conformidad de toda la organización (consola)

1. Abra la Consola de políticas de etiquetas.
2. Seleccione la pestaña Raíz de esta organización y, en la parte inferior de la página, seleccione Generar informe.
3. En la pantalla Generar informe, especifique dónde almacenar el informe.
4. Elija Comenzar exportación.

Cuando el informe esté completo, puede descargarlo de la sección Informe de no conformidad de la pestaña Raíz de la organización.

Notas

El cumplimiento en toda la organización se evalúa cada 48 horas. Se obtiene el siguiente resultado:

- Los cambios de los recursos o una política de etiquetas pueden tardar hasta 48 horas en mostrarse en el informe de conformidad de toda la organización. Por ejemplo, supongamos que tiene una política de etiquetas que define una etiqueta estandarizada nueva para un tipo de recurso. Los recursos de ese tipo que no tienen esta etiqueta pueden mostrarse como conformes en el informe durante un máximo de 48 horas.
- Si bien puede generar el informe en cualquier momento, los resultados del informe no se actualizan hasta que se complete la siguiente evaluación.
- La NoncompliantKeyscolumna muestra las claves de etiquetas del recurso que no cumplen con la política de etiquetas vigente.
- En la KeysWithNonCompliantValuescolumna se enumeran las claves definidas en la política vigente que se encuentran en el recurso con un tratamiento incorrecto de mayúsculas y minúsculas o con valores no conformes.
- Si cierra un Cuenta de AWS que era miembro de la organización, puede seguir apareciendo en el informe de conformidad con las etiquetas durante un máximo de 90 días.

Para generar un informe de conformidad para toda la organización (AWS CLI, AWS API)

Use los siguientes comandos y operaciones para generar un informe de conformidad para toda la organización, comprobar su estado y ver el informe:

- AWS Command Line Interface AWS CLI):
  - aws resourcegroupstaggingapi start-report-creation
  - aws resourcegroupstaggingapi describe-report-creation
  - aws resourcegroupstaggingapi get-compliance-summary

  Para ver el procedimiento completo de uso de las políticas de etiquetas en el AWS CLI, consulte Uso de políticas de etiquetas en la AWS CLI en la AWS Organizations Guía del usuario.
- AWS API:
  - StartReportCreation
  - DescribeReportCreation
  - GetComplianceSummary

Supervise los cambios en las etiquetas con flujos de trabajo sin servidor y Amazon EventBridge

Amazon EventBridge admite cambios en las etiquetas de AWS los recursos. Con este EventBridge tipo, puedes crear EventBridge reglas que coincidan con los cambios en las etiquetas y dirigir los eventos a uno o más objetivos. Por ejemplo, un objetivo puede ser una AWS Lambda función para invocar flujos de trabajo automatizados. En este tema se proporciona un tutorial sobre el uso de Lambda para crear una solución rentable sin servidor que procese de forma segura los cambios de etiquetas en sus recursos. AWS

Los cambios en las etiquetas generan eventos EventBridge

EventBridge ofrece un flujo casi en tiempo real de los eventos del sistema que describen los cambios en AWS los recursos. Muchos AWS recursos admiten etiquetas, que son atributos personalizados y definidos por el usuario para organizar y categorizar AWS los recursos con facilidad. Los casos de uso más frecuentes de las etiquetas son la asignación de costos, la categorización, el control de acceso, la seguridad y la automatización.

Con él EventBridge, puede supervisar los cambios en las etiquetas y realizar un seguimiento del estado de las etiquetas en AWS los recursos. Anteriormente, para lograr una funcionalidad similar, podías haber sondeado APIs y orquestado varias llamadas de forma continua. Ahora, cualquier cambio en una etiqueta, incluido el servicio individualAPIs, el editor de etiquetas y el etiquetado, API iniciará el cambio de etiqueta en el evento del recurso. El siguiente ejemplo muestra un EventBridge evento típico provocado por un cambio de etiqueta. Muestra las claves de etiqueta nuevas, actualizadas o eliminadas y sus valores asociados.

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
```

```
  "detail": {
    "changed-tag-keys": [
      "a-new-key",
      "an-updated-key",
      "a-deleted-key"
    ],
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added",
      "an-updated-key": "tag-value-was-just-changed",
      "an-unchanged-key": "tag-value-still-the-same"
    },
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
  }
}
```

Todos los EventBridge eventos tienen los mismos campos de nivel superior:

- version: de forma predeterminada, este valor está definido en `0` (cero) en todos los eventos.
- id: se genera un valor único para cada evento. Esto puede resultar útil a la hora de realizar un seguimiento de los eventos mientras se desplazan a destinos a través de reglas y se procesan.
- detail-type: identifica, en combinación con `source`, los campos y los valores que aparecen en detalle.
- source: identifica el servicio que fue la fuente del evento. La fuente de los cambios en las etiquetas es `aws.tag`.
- time: la hora del evento.
- region: identifica la Región de AWS en la que se originó el evento.
- resources: esta JSON matriz contiene los nombres de recursos de Amazon (ARNs) que identifican los recursos involucrados en el evento. Este es el recurso en el que las etiquetas han cambiado.
- detalle: JSON objeto cuyo contenido es diferente en función del tipo de evento. Para el cambio de etiqueta en un recurso, se incluyen los siguientes campos detallados:
  - changed-tag-keys— Las claves de etiqueta que han cambiado a causa de este evento.
  - service: el servicio al que pertenece el recurso. En este ejemplo, el servicio es `ec2` AmazonEC2.
  - resource-type: el tipo de recurso del servicio. En este ejemplo, se trata de una EC2 instancia de Amazon.

- version: la versión del conjunto de etiquetas. La versión comienza en 1 y aumenta cuando se cambian las etiquetas. Puede usar la versión para verificar el orden de los eventos de cambio de etiquetas.
- tags: las etiquetas asociadas al recurso después del cambio.

Para obtener más información, consulta los patrones de EventBridge eventos de Amazon en la Guía del EventBridge usuario de Amazon.

Al usarlo EventBridge, puede crear reglas que coincidan con patrones de eventos específicos en función de los diferentes campos. En el tutorial se muestra cómo hacerlo. Además, mostramos cómo se puede detener automáticamente una EC2 instancia de Amazon si no se adjunta una etiqueta específica a la instancia. Usamos los EventBridge campos para crear un patrón que coincida con los eventos de etiqueta de la instancia que lanza una función Lambda.

Lambda y sin servidor

AWS Lambda sigue el paradigma sin servidor para ejecutar código en la nube. Solo se ejecuta el código cuando es necesario, sin pensar en los servidores. Solo se paga por el tiempo exacto de computación que se usa. Aunque se llame sin servidor, no significa que no haya ninguno. En este contexto, sin servidor significa que no tiene que aprovisionar, configurar ni administrar los servidores que se utilizan para ejecutar el código. AWS hace todo eso por ti, para que puedas centrarte en tu código. Para obtener más información acerca de Lambda, consulte la Descripción general del producto AWS Lambda.

Tutorial: Detener automáticamente EC2 las instancias de Amazon a las que les faltan las etiquetas obligatorias

Como tu grupo de AWS recursos y Cuentas de AWS si administra y crece, puede usar etiquetas para facilitar la categorización de sus recursos. Las etiquetas se suelen utilizar para casos de uso críticos, como la asignación de costos y la seguridad. Para gestionarlos de forma eficaz AWS los recursos, sus recursos deben estar etiquetados de forma coherente. A menudo, cuando se aprovisiona un recurso, recibe todas las etiquetas apropiadas. Sin embargo, un proceso posterior puede provocar un cambio de etiqueta que provoque una desviación de la política de etiquetas corporativa. Al monitorear los cambios en las etiquetas, puede detectar la desviación de etiquetas y responder de inmediato. Esto le da más confianza en que los procesos que dependen de que sus recursos estén debidamente categorizados producirán los resultados deseados.

En el siguiente ejemplo, se muestra cómo supervisar los cambios de etiquetas en EC2 las instancias de Amazon para comprobar que una instancia específica sigue teniendo las etiquetas necesarias. Si las etiquetas de la instancia cambian y la instancia ya no tiene las etiquetas necesarias, se invoca una función de Lambda para cerrar la instancia automáticamente. ¿Para qué hacerlo? Garantiza que todos los recursos estén etiquetados de acuerdo con la política de etiquetas de su empresa, para poder asignar los costes de forma eficaz o para poder confiar en la seguridad basada en el control de acceso basado en atributos () ABAC.

> **Important**
>
> Le recomendamos encarecidamente que realice este tutorial en una cuenta que no sea de producción, de forma que no pueda cerrar instancias importantes sin darse cuenta.
> El código de ejemplo de este tutorial limita intencionadamente el impacto de este escenario solo a las instancias de una lista de instancias. IDs Debe actualizar la lista con la instancia IDs que desee cerrar para la prueba. Esto ayuda a garantizar que no puedas cerrar accidentalmente todas las instancias de una región de tu Cuenta de AWS.
> Tras realizar las pruebas, asegúrese de que todas las instancias estén etiquetadas de acuerdo con la estrategia de etiquetado de su empresa. A continuación, puedes eliminar el código que limita la función solo a la instancia IDs de la lista.

En este ejemplo se utiliza JavaScript y la versión 16.x de Node.js. El ejemplo usa el ejemplo Cuenta de AWS El identificador 123456789012 y el Región de AWS EE. UU. Este (Virginia del Norte) (). `us-east-1` Sustitúyalos por el ID y la región de su cuenta de prueba.

> **Note**
>
> Si la consola usa una región diferente como predeterminada, asegúrese de cambiar la región que está usando en este tutorial cada vez que cambie de consola. Una causa frecuente de que este tutorial no funcione es tener la instancia y la función en dos regiones diferentes.

Si utiliza una región diferente de `us-east-1`, asegúrese de cambiar todas las referencias de los siguientes ejemplos de código a la región que elija.

Temas

Paso 1. Creación de la función de Lambda

Para crear la función de Lambda

1. Abra el icono AWS Lambda consola de administración.
2. Elija Crear función, y, a continuación, Autor desde cero.
3. En Function name (Nombre de función), escriba **`AutoEC2Termination`**.
4. En Tiempo de ejecución, elija Node.js 16.x.
5. Mantenga el resto de campos con sus valores predeterminados y seleccione Crear función.
6. En la pestaña Código de la página de detalles de `AutoEC2Termination`, abra el archivo index.js para ver su código.
   - Si hay abierta una pestaña con index.js, puede seleccionar el cuadro de edición de esa pestaña para editar su código.
   - Si una pestaña con el archivo index.js no está abierta, haga clic con el botón secundario en el archivo index.js situado en la EC2Terminator carpeta Auto del panel de navegación. A continuación, elija Abrir.
7. En la pestaña index.js, pegue el siguiente código en el cuadro del editor y sustituya todo lo que ya esté presente.

   Reemplace el valor `RegionToMonitor` por la región en la que desea ejecutar esta función.

```
// Set the following line to specify which Region's instances you want to monitor
// Only instances in this Region are succesfully stopped on a match

const RegionToMonitor = "us-east-1"

// Specify the instance ARNs to check.
// This limits the function for safety to avoid the tutorial shutting down all
 instances in account
// The first ARN is a "dummy" that matches the test event you create in Step 3.
```

```
// Replace the second ARN with one that matches a real instance that you want to
 monitor and that you can
// safely stop

const InstanceList = [
    "i-0000000aaaaaaaaaa",
    "i-05db4466d02744f07"
];

// The tag key name and value that marks a "valid" instance. Instances in the
 previous list that
// do NOT have the following tag key and value are stopped by this function

const ValidKeyName = "valid-key";
const ValidKeyValue = "valid-value";

// Load and configure the AWS SDK
const AWS = require('aws-sdk');
// Set the AWS Region
AWS.config.update({region: RegionToMonitor});
// Create EC2 service object.
const ec2 = new AWS.EC2({apiVersion: '2016-11-15'});

exports.handler = (event, context, callback) => {

  // Retrieve the details of the reported event.
  var detail = event.detail;
  var tags = detail["tags"];
  var service = detail["service"];
  var resourceType = detail["resource-type"];
  var resource = event.resources[0];
  var resourceSplit = resource.split("/");
  var instanceId = resourceSplit[resourceSplit.length - 1];

  // If this event is not for an EC2 resource, then do nothing.
  if (!(service === "ec2")) {
    console.log("Event not for correct service -- no action (", service, ")" );
    return;
  }

  // If this event is not about an instance, then do nothing.
  if (!(resourceType === "instance")) {
    console.log("Event not for correct resource type -- no action (", resourceType,
 ")" );
```

```
    return;
 }

 // CAUTION - Removing the following 'if' statement causes the function to run
against
 //           every EC2 instance in the specified Region in the calling Cuenta de
AWS.
 //           If you do this and an instance is not tagged with the approved tag
key
 //           and value, this function stops that instance.

 // If this event is not for the ARN of an instance in our include list, then do
nothing.
 if (InstanceList.indexOf(instanceId)<0) {
    console.log("Event not for one of the monitored instances -- no action (",
resource, ")");
    return;
 }

 console.log("Tags changed on monitored EC2 instance (",instanceId,")");

 // Check attached tags for expected tag key and value pair
 if ( tags.hasOwnProperty(ValidKeyName) && tags[ValidKeyName] == "valid-value"){
    // Required tags ARE present
    console.log("The instance has the required tag key and value -- no action");
    callback(null, "no action");
    return;
 }

 // Required tags NOT present
 console.log("This instance is missing the required tag key or value -- attempting
to stop the instance");

 var params = {
    InstanceIds: [instanceId],
    DryRun: true
 };

 // call EC2 to stop the selected instances
 ec2.stopInstances(params, function(err, data) {
    if (err && err.code === 'DryRunOperation') {
      // dryrun succeeded, so proceed with "real" stop operation
      params.DryRun = false;
      ec2.stopInstances(params, function(err, data) {
```

```
        if (err) {
          console.log("Failed to stop instance");
          callback(err, "fail");
        } else if (data) {
          console.log("Successfully stopped instance", data.StoppingInstances);
          callback(null, "Success");
        }
      });
    } else {
      console.log("Dryrun attempt failed");
      callback(err);
    }
  });
};
```

8. Seleccione Implementar para guardar los cambios y activar la nueva versión de la función.

Esta función Lambda comprueba las etiquetas de una EC2 instancia de Amazon, según lo informado por el evento de cambio de etiqueta en. EventBridge En este ejemplo, si a la instancia del evento le falta la clave de etiqueta requerida `valid-key` o si esa etiqueta no tiene el valor `valid-value`, la función intenta detener la instancia. Puede cambiar esta comprobación lógica o los requisitos de etiqueta para sus casos de uso específicos.

Mantenga abierta la ventana de la consola Lambda en su navegador.

Paso 2. Configure los permisos necesarios IAM

Antes de que la función pueda ejecutarse correctamente, debes concederle el permiso para detener una EC2 instancia. La AWS función proporcionada lambda_basic_executionno tiene ese permiso. En este tutorial, modificará la política de IAM permisos predeterminada que se adjunta al rol de ejecución de la función denominado`AutoEC2Termination-role-`*`uniqueid`*. El permiso adicional mínimo requerido para este tutorial es `ec2:StopInstances`.

Para obtener más información sobre la creación de IAM políticas EC2 específicas de Amazon, consulte AmazonEC2: permite iniciar o detener una EC2 instancia y modificar un grupo de seguridad, mediante programación y en la consola, en la Guía del IAMusuario.

Para crear una política de IAM permisos y adjuntarla a la función de ejecución de la función Lambda

1. En otra pestaña o ventana del navegador, abra la página Roles de la IAM consola.

2. Comience a escribir el nombre del rol **`AutoEC2Termination`** y, cuando aparezca en la lista, selecciónelo.
3. En la página de Resumen del rol, seleccione la pestaña Permisos y elija el nombre de la política que ya está adjunta.
4. En la página de Resumen de la política, elija Editar política.
5. En la pestaña Editor visual, elija Agregar permisos adicionales.
6. En Service (Servicio), seleccione EC2.
7. En Acciones, elija StopInstances. Puede escribir **`Stop`** en la barra de búsqueda y, a continuación, elegir `StopInstances` cuándo aparezca.
8. En Recursos, seleccione Todos los recursos, seleccione Revisar política y, a continuación, seleccione Guardar cambios.

   De esta forma se crea automáticamente una nueva versión de la directiva y se establece esa versión como predeterminada.

   La política final debe ser similar al ejemplo siguiente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:StopInstances",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-east-1:123456789012:*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
```

```
            "Resource": "arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/
AutoEC2Termination:*"
        }
    ]
}
```

Paso 3. Realice una prueba preliminar de la función de Lambda

En este paso, envía un evento de prueba a su función. La funcionalidad de la prueba de Lambda funciona mediante el envío de un evento de prueba proporcionado manualmente. La función procesa el evento de prueba como si el evento procediera de EventBridge. Puede definir varios eventos de prueba con valores diferentes para ejercitar todas las distintas partes del código. En este paso, envías un evento de prueba que indica que las etiquetas de una EC2 instancia de Amazon han cambiado y que las nuevas etiquetas no incluyen la clave ni el valor de etiqueta necesarios.

Para probar su función de Lambda

1. Vuelva a la ventana o pestaña de la consola Lambda y abra la pestaña Probar de la función Auto EC2Termination.
2. Elija Crear evento nuevo.
3. En Nombre del evento, escriba **`SampleBadTagChangeEvent`**.
4. En el campo Evento JSON, sustituya el texto por el evento de ejemplo que se muestra en el siguiente texto de ejemplo. No es necesario modificar las cuentas, la región o el ID de instancia para que este evento de prueba funcione correctamente.

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "valid-key"
```

```
    ],
    "tags": {
      "valid-key": "NOT-valid-value"
    },
    "service": "ec2",
    "resource-type": "instance",
    "version": 3
  }
}
```

5. Elija Save (Guardar) y, a continuación, elija Test (Probar).

   La prueba parece fallar, pero no pasa nada.

   Debería aparecer el siguiente error en la pestaña Resultados de la ejecución, en Respuesta.

```
{
  "errorType": "InvalidInstanceID.NotFound",
  "errorMessage": "The instance ID 'i-0000000aaaaaaaaaa' does not exist",
  ...
}
```

   El error se produce porque la instancia especificada en el evento de prueba no existe.

   La información de la pestaña Resultados de ejecución, en la sección Registros de funciones, demuestra que la función Lambda intentó detener una EC2 instancia correctamente. Sin embargo, falló porque el código inicialmente intentó una `DryRun` operación para detener la instancia, lo que indicaba que el ID de la instancia no era válido.

```
START RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44 Version: $LATEST
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    This
 instance is missing the required tag key or value -- attempting to stop the
 instance
2022-11-30T20:17:31.206Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Dryrun
 attempt failed
2022-11-30T20:17:31.207Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    ERROR   Invoke
 Error     {"errorType":"InvalidInstanceID.NotFound","errorMessage":"The instance
 ID 'i-0000000aaaaaaaaaa' does not
 exist","code":"InvalidInstanceID.NotFound","message":"The instance ID
 'i-0000000aaaaaaaaaa' does not
```

```
 exist","time":"2022-11-30T20:17:31.205Z","requestId":"a5192c3b-142d-4cec-
bdbc-685a9b7c7abf","statusCode":400,"retryable":false,"retryDelay":36.87870631147607,"stack
["InvalidInstanceID.NotFound: The instance ID 'i-0000000aaaaaaaaaa' does
 not exist","    at Request.extractError (/var/runtime/node_modules/aws-sdk/
lib/services/ec2.js:50:35)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:106:20)","    at Request.emit
 (/var/runtime/node_modules/aws-sdk/lib/sequential_executor.js:78:10)","    at
 Request.emit (/var/runtime/node_modules/aws-sdk/lib/request.js:686:14)","    at
 Request.transition (/var/runtime/node_modules/aws-sdk/lib/request.js:22:10)","
    at AcceptorStateMachine.runTo (/var/runtime/node_modules/aws-sdk/lib/
state_machine.js:14:12)","    at /var/runtime/node_modules/aws-sdk/lib/
state_machine.js:26:10","    at Request.<anonymous> (/var/runtime/node_modules/aws-
sdk/lib/request.js:38:9)","    at Request.<anonymous> (/var/runtime/node_modules/
aws-sdk/lib/request.js:688:12)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:116:18)"]}
END RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44
```

6. Para demostrar que el código no intenta detener la instancia cuando se usa la etiqueta correcta, puede crear y enviar otro evento de prueba.

   Seleccione la pestaña Prueba situada encima del Código fuente. La consola muestra el evento de SampleBadTagChangeEventprueba existente.

7. Elija Crear evento nuevo.
8. En Event Name (Nombre del evento), escriba **`SampleGoodTagChangeEvent`**.
9. En la línea 17, elimine **`NOT-`** para cambiar el valor a **`valid-value`**.
10. En la parte superior de la ventana de Evento de prueba, seleccione Guardar y, a continuación, seleccione Prueba.

    El resultado muestra lo siguiente, lo cual demuestra que la función reconoce la etiqueta como válida y no intenta cerrar la instancia.

    ```
    START RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4 Version: $LATEST
    2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    Tags
     changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
    2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    The
     instance has the required tag key and value -- no action
    END RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4
    ```

    Mantenga la consola Lambda abierta en su navegador.

Paso 4. Cree la EventBridge regla que inicia la función

Ahora puede crear una EventBridge regla que coincida con el evento y apunte a la función Lambda.

Para crear la regla EventBridge

1. En otra pestaña o ventana del navegador, abra la EventBridge consola en la página Crear regla.
2. En Nombre, escriba **`ec2-instance-rule`** y, a continuación, seleccione Siguiente.
3. Desplázate hacia abajo hasta Método de creación y selecciona Patrón personalizado (JSONeditor).
4. En el cuadro de edición, pegue el siguiente texto del patrón y, a continuación, seleccione Siguiente.

```
{
  "source": [
    "aws.tag"
  ],
  "detail-type": [
    "Tag Change on Resource"
  ],
  "detail": {
    "service": [
      "ec2"
    ],
    "resource-type": [
      "instance"
    ]
  }
}
```

   Esta regla hace coincidir `Tag Change on Resource` los eventos de EC2 las instancias de Amazon e invoca lo que especifiques como Target en el siguiente paso.
5. A continuación, añada la función de Lambda como destino. En el cuadro Destino 1, en Seleccione un destino, elija Función de Lambda.
6. En Función, selecciona la EC2Termination función automática que creaste anteriormente y, a continuación, selecciona Siguiente.
7. En la página Configurar etiquetas, elija Siguiente. A continuación, en la página Revisar y crear, elija Crear regla. Esto también otorga automáticamente permiso para EventBridge invocar la función Lambda especificada.

Paso 5. Comprobación de la solución completa

Para probar el resultado final, crea una EC2 instancia y observa lo que ocurre cuando cambias sus etiquetas.

Para probar la solución de supervisión con una instancia real

1. Abre la EC2consola de Amazon en la página de instancias.
2. Crea una EC2 instancia de Amazon. Antes de lanzarla, adjunte una etiqueta con la clave `valid-key` y el valor `valid-value`. Para obtener información sobre cómo crear y lanzar una instancia, consulta el paso 1: lanzar una instancia en la Guía del EC2 usuario de Amazon. En el procedimiento Para lanzar una instancia, en el paso 3, donde introduce la etiqueta de Nombre, también seleccione Añadir etiquetas adicionales, seleccione Añadir etiqueta y, a continuación, ingrese la Clave **`valid-key`** y el valor de **`valid-value`**. Puede continuar sin un par de claves si esta instancia es únicamente para los fines de este tutorial y planea eliminar esta instancia después de completarla. Vuelva a este tutorial cuando llegue al final del Paso 1; no es necesario que haga el Paso 2: conectarse a su instancia.
3. Copia el InstanceIdarchivo de la consola.
4. Cambie de la EC2 consola Amazon a la consola Lambda. Elija la EC2Termination función Automática, elija la pestaña Código y, a continuación, elija la pestaña index.js para editar el código.
5. Cambia la segunda entrada `InstanceList` pegando el valor que copiaste de la EC2 consola de Amazon. Asegúrese de que el valor de `RegionToMonitor` coincida con la región que contiene la instancia que pegó.
6. Elija Implementar para activar los cambios. La función ya está lista para activarse mediante cambios de etiqueta en esa instancia en la región especificada.
7. Cambie de la consola Lambda a la consola de AmazonEC2.
8. Cambie las Etiquetas adjuntas a la instancia eliminando la etiqueta de clave válida o cambiando el valor de esa clave.

> **Note**
>
> Para obtener información sobre cómo cambiar las etiquetas en una EC2 instancia de Amazon en ejecución, consulta Añadir y eliminar etiquetas en un recurso individual en la Guía del EC2 usuario de Amazon.

9. Espere unos segundos y, a continuación, actualice la consola. La instancia debería cambiar su Estado de instancia a Deteniendo y, a continuación, a Detenida.
10. Cambie de la EC2 consola Amazon a la consola Lambda con su función y elija la pestaña Monitor.
11. Seleccione la pestaña Registros y, en la tabla de invocaciones recientes, elija la entrada más reciente de la LogStreamcolumna.

    La CloudWatch consola de Amazon se abre en la página de registro de eventos para la última invocación de la función Lambda. La última entrada debería tener un aspecto similar al ejemplo siguiente.

```
2022-11-30T12:03:57.544-08:00    START RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac Version: $LATEST
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Tags changed on monitored EC2 instance ( arn:aws:ec2:us-
west-2:123456789012:instance/i-1234567890abcdef0 )
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO This instance is missing the required tag key or value --
 attempting to stop the instance
2022-11-30T12:03:58.488-08:00    2022-11-30T20:03:58.488Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Successfully stopped instance [ { CurrentState: { Code: 64,
 Name: 'stopping' }, InstanceId: 'i-1234567890abcdef0', PreviousState: { Code: 16,
 Name: 'running' } } ]
2022-11-30T12:03:58.546-08:00    END RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac
```

Resumen del tutorial

En este tutorial, se muestra cómo crear una EventBridge regla que coincida con un cambio de etiqueta en un evento de recurso para EC2 instancias de Amazon. La regla apuntaba a una función de Lambda que cierra automáticamente la instancia si no tiene la etiqueta requerida.

El EventBridge soporte de Amazon para los cambios de etiquetas en AWS resources abre la posibilidad de desarrollar la automatización basada en eventos en muchos Servicios de AWS. Combinar esta capacidad con AWS Lambda le proporciona herramientas para crear soluciones sin servidor que accedan AWS los recursos de forma segura, se escalan según la demanda y son rentables.

Otros posibles casos de uso del tag-change-on-resource EventBridge evento incluyen:

- Lanzar una advertencia si alguien accede al recurso desde una dirección IP inusual: use una etiqueta para almacenar la dirección IP de origen de cada visitante que acceda a su recurso. Los cambios en la etiqueta generan un CloudWatch evento. Puede usar ese evento para comparar la dirección IP de origen con una lista de direcciones IP válidas y activar un correo electrónico de advertencia si la dirección IP de origen no es válida.
- Supervise si hay cambios en el control de acceso basado en etiquetas de un recurso: si ha configurado el acceso a un recurso mediante el control de acceso basado en atributos (etiquetas) (ABAC), puede utilizar EventBridge los eventos generados por cualquier cambio en la etiqueta para solicitar una auditoría por parte de su equipo de seguridad.

Solución de problemas de cambios de etiquetas

La siguiente lista de comprobación puede resultar útil si se producen errores al intentar aplicar o cambiar etiquetas en los recursos seleccionados de los resultados de la consulta de Búsqueda de recursos para etiquetar.

- Es posible que el recurso ya tenga el número máximo de etiquetas. Por lo general, los recursos pueden tener un máximo de 50 etiquetas definidas por el usuario. AWS las etiquetas generadas no cuentan para el máximo de 50 etiquetas. Puede que otros usuarios también añadan etiquetas al mismo recurso a la vez, lo que podría aumentar las etiquetas del recurso al máximo.
- Algunos servicios permiten un conjunto de caracteres diferente (o restringen el conjunto de caracteres permitido) para crear etiquetas. Si ha añadido o cambiado etiquetas utilizando caracteres especiales, revise los requisitos de las etiquetas en la documentación del servicio del recurso para verificar que el servicio permite esos caracteres.
- Es posible que no tenga permisos para modificar las etiquetas del recurso. Si no tiene permisos para ver las etiquetas existentes de un recurso, no puede realizar cambios en las etiquetas del recurso.
- Puede que no tenga los permisos para cambiar el recurso. Otro administrador puede restringir los cambios en los metadatos del recurso.
- Otro usuario o proceso puede haber editado o eliminado el recurso. Por ejemplo, supongamos que se lanzó un recurso como parte de la creación de una pila AWS CloudFormation . Si la pila se eliminó o ya no está activa, es posible que el recurso ya no esté disponible.
- Puede que los cambios de etiquetas no se puedan llevar a cabo si un recurso está offline, ha terminado o si otras actualizaciones (como las actualizaciones de software) del recurso están en curso.
- Los cambios de etiqueta pueden fallar si cierra la pestaña del navegador o cambia la página antes de que se complete el cambio de etiqueta. Deje que los cambios de etiquetas se completen y espere a que el banner de operación realizada correctamente o fallida aparezca en la página antes de salir de ella.
- Si bien hay un límite de velocidad para el AWS Resource Groups Tagging API, el servicio que estás etiquetando puede imponer un límite diferente que podrías alcanzar antes del límite de etiquetado API de Resource Groups.

Volver a intentar los cambios de etiquetas erróneos

Si se produce un error en los cambios de etiquetas de al menos uno de los recursos seleccionados, el editor de etiquetas muestra un banner rojo en la parte inferior de la página. El banner muestra un mensaje de error para cada tipo de error que se produzca. Para cada error, el banner identifica los recursos específicos en los que el editor de etiquetas no ha podido realizar los cambios de etiqueta. Después de revisar y solucionar los errores, seleccione Volver a intentar los cambios de etiquetas en los recursos para volver a intentar los cambios solo en esos recursos en los que se haya producido un error en los cambios de etiqueta.

Seguridad en el editor de etiquetas

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

La seguridad es una responsabilidad compartida entre AWS y el usuario. 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. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican al editor de etiquetas, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad es determinada por el Servicio de AWS que utilice. Usted 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 el editor de etiquetas. En los siguientes temas, se le mostrará cómo configurar el editor de etiquetas para satisfacer sus objetivos de seguridad y conformidad.

Temas

Protección de datos en el editor de etiquetas

La AWS modelo de responsabilidad compartida se aplica a la protección de datos en Tag Editor. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en

la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido que está alojado en esta infraestructura. También es responsable de las tareas de configuración y administración de la seguridad del Servicios de AWS que utilices. Para obtener más información sobre la privacidad de los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte la AWS Modelo de responsabilidad compartida y entrada de GDPR blog sobre AWS Blog de seguridad.

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

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UtiliceSSL/TLSpara comunicarse con AWS recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Trabajar con CloudTrail senderos en AWS CloudTrail Guía del usuario.
- Uso AWS soluciones de cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder AWS a través de una interfaz de línea de comandos oAPI, utilice un FIPS punto final. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la Norma Federal de Procesamiento de Información (FIPS) 140-3.

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

Cifrado de datos

La información de etiquetado no está cifrada. Aunque no están cifradas, las etiquetas pueden contener información utilizada como parte de su estrategia de seguridad, por lo que es importante controlar quién puede acceder a las etiquetas de los recursos. Es especialmente importante que controle quién puede modificar las etiquetas, ya que ese acceso podría utilizarse para aumentar los permisos de una persona.

Cifrado en reposo

No existen formas adicionales de aislar el servicio o el tráfico de red que sean específicas del editor de etiquetas. Si corresponde, utilice AWS aislamiento específico. Puede utilizar el editor de etiquetas API y la consola en una nube privada virtual (VPC) para maximizar la privacidad y la seguridad de la infraestructura.

Cifrado en tránsito

Los datos del editor de etiquetas se cifran en tránsito a la base de datos interna del servicio para realizar copias de seguridad. Esto no es configurable por el usuario.

Administración de claves

Actualmente, el editor de etiquetas no está integrado con AWS Key Management Service y no es compatible AWS KMS keys.

Privacidad del tráfico entre redes

Tag Editor se utiliza HTTPS para todas las transmisiones entre los usuarios de Tag Editor y AWS. El editor de etiquetas usa transport layer security (TLS) 1.3, pero también es compatible con TLS 1.2.

Administración de identidades y accesos para el editor de etiquetas

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de Tag Editor. IAMes una Servicio de AWS que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Tag Editor.

Usuario de servicio: si utiliza el servicio del editor de etiquetas para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características del editor de etiquetas 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 el editor de etiquetas, consulte Solución de problemas de identidades y accesos en el editor de etiquetas.

Administrador de servicio: si está a cargo de los recursos del editor de etiquetas en su empresa, es probable que tenga acceso completo al editor de etiquetas. Su trabajo consiste en determinar a qué características y recursos del editor de etiquetas deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos deIAM. Para obtener más información sobre cómo su empresa puede utilizar IAM Tag Editor, consulteCómo funciona el editor de etiquetas con IAM.

IAMadministrador: si es IAM administrador, puede que desee obtener más información sobre cómo puede redactar políticas para administrar el acceso a Tag Editor. Para ver ejemplos de políticas de Tag Editor basadas en la identidad que puede utilizarIAM, consulte. Ejemplos de políticas basadas en identidad del editor de etiquetas

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como IAM usuario o asumiendo un IAM rol. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAMIdentity Center), 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, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

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

Si accede AWS mediante programación, AWS incluye un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar AWS API las solicitudes en la Guía del IAM usuario.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactorial en la Guía del AWS IAM Identity Center usuario y Uso de la autenticación multifactorial (MFA) AWS en la Guía del IAM usuario.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste 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 tareas que requieren que inicie sesión como usuario root, consulte Tareas que requieren credenciales de usuario root en la Guía del IAM usuario.

Usuarios y grupos

Un IAMusuario es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas

y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración en la Guía del IAM usuario.

Un IAMgrupo es una identidad que especifica un conjunto de IAM usuarios. 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 para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

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 de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un IAM usuario (en lugar de un rol) en la Guía del IAM usuario.

Roles

Un IAMrol es una identidad dentro de ti Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console cambiando de rol. Puede asumir un rol llamando a una AWS API operación AWS CLI o o utilizando una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte Métodos para asumir un rol en la Guía del IAM usuario.

IAMlos roles 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 sobre los roles para la federación, consulte Creación de un rol para un proveedor de identidad externo en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en. IAM Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos IAM de usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.

- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los recursos entre cuentas IAM en la Guía del IAM usuario.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros. Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual 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 al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a an Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener detalles sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar sesiones de acceso.
  - Función de servicio: una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.
  - Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales

temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del IAM usuario.

Administración de acceso mediante políticas

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

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

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

IAMlas políticas definen los 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 esa política puede obtener información sobre el rol de AWS Management Console AWS CLI, el o el AWS API.

Políticas basadas en identidad

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

Las políticas basadas en identidades 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 adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para saber cómo elegir entre una política gestionada o una política integrada, consulte Elegir entre políticas gestionadas y políticas integradas en la Guía del IAM usuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

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

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Amazon S3 AWS WAF y Amazon VPC son ejemplos de servicios compatiblesACLs. Para obtener más informaciónACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. 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 función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAMusuario o rol). 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 los límites de los permisos para IAM las entidades en la Guía del IAMusuario.

- Políticas de control de servicios (SCPs): SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. SCPLimita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre OrganizationsSCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- 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 identidades 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 obtener más información, consulte las políticas de sesión en la Guía del IAM usuario.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del IAM usuario.

Cómo funciona el editor de etiquetas con IAM

Antes de administrar el IAM acceso al Tag Editor, debe saber qué IAM funciones están disponibles para su uso con Tag Editor. Para obtener una visión general de cómo Servicios de AWS funcionan el Tag Editor y otras IAM herramientas, consulta Servicios de AWS cómo funcionan IAM en la Guía del IAM usuario.

Temas

- Políticas basadas en identidad del editor de etiquetas
- Políticas basadas en recursos

- Autorización basada en etiquetas
- IAMFunciones del editor de etiquetas

Políticas basadas en identidad del editor de etiquetas

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, además de las condiciones en las que se permiten o deniegan las acciones. El editor de etiquetas admite acciones, claves de condición y recursos específicos. Para obtener más información sobre todos los elementos que se utilizan en una JSON política, consulte la referencia sobre los elementos IAM JSON de la política en la Guía del IAMusuario.

Acciones

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

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

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

Las acciones de políticas en el editor de etiquetas utilizan el siguiente prefijo antes de la acción: `tag:`. Las acciones del editor de etiquetas se realizan completamente en la consola, pero tienen el prefijo `tag` en las entradas de registro.

Por ejemplo, para conceder permiso a alguien para etiquetar un recurso con la `tag:TagResources` API operación, debes incluir la `tag:TagResources` acción en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. El editor de etiquetas define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

Para especificar varias acciones de etiquetado en una única instrucción, sepárelas con comas del siguiente modo.

```
"Action": [
      "tag:action1",
```

```
        "tag:action2",
        "tag:action3"
```

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

```
"Action": "tag:Get*"
```

A fin de conocer una lista completa de acciones del editor de etiquetas, consulte Actions, resources, and condition keys for Tag Editor en la Referencia de autorizaciones de servicio.

Recursos

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

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

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

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

El editor de etiquetas no cuenta con ningún recurso propio. En su lugar, manipula los metadatos (etiquetas) que se adjuntan a los recursos creados por otros Servicios de AWS.

Claves de condición

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

El elemento `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 mediante una `OR` operación lógica. 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 a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte los elementos IAM de la política: variables y etiquetas en la Guía del IAM usuario.

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

El editor de etiquetas no define ninguna clave de condición específica del servicio.

Ejemplos

Para ver ejemplos de políticas basadas en identidad del editor de etiquetas, consulte Ejemplos de políticas basadas en identidad del editor de etiquetas.

Políticas basadas en recursos

El editor de etiquetas no admite políticas basadas en recursos porque no define ninguno de sus propios recursos.

Autorización basada en etiquetas

La autorización basada en etiquetas forma parte de la estrategia de seguridad denominada control de acceso basado en atributos ()ABAC.

Para controlar el acceso a un recurso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Puede aplicar etiquetas a un recurso al crear o actualizar el recurso.

Para consultar un ejemplo de política basada en la identidad para limitar el acceso a un recurso en función de las etiquetas de ese recurso, consulte Visualización de grupos basados en etiquetas. Para

obtener más información sobre el control de acceso basado en atributos (ABAC), consulte ¿Para qué sirve? ABAC AWS en la Guía del IAMusuario.

IAMFunciones del editor de etiquetas

Un IAMrol es una entidad dentro de ti Cuenta de AWS que tiene permisos específicos. El editor de etiquetas no tiene ni utiliza roles de servicio.

Uso de credenciales temporales con el editor de etiquetas

En Tag Editor, puedes usar credenciales temporales para iniciar sesión en la federación, asumir un IAM rol o asumir un rol multicuenta. Para obtener credenciales de seguridad temporales, puede llamar a AWS STS API operaciones como AssumeRoleo GetFederationToken.

Roles vinculados al servicio

Los roles vinculados al servicio permiten acceder Servicios de AWS a los recursos de otros servicios para completar una acción en su nombre.

El editor de etiquetas de no tiene ni usa un rol vinculado a servicios.

Roles de servicio

Esta característica permite que un servicio asuma un rol de servicio en su nombre.

El editor de etiquetas no tiene ni utiliza roles de servicio.

Ejemplos de políticas basadas en identidad del editor de etiquetas

Por defecto, las entidades principales de IAM, como roles y usuarios, no tienen permiso para crear o modificar etiquetas. Tampoco pueden realizar tareas mediante la AWS Management Console, 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 operaciones de API concretas en los recursos concretos que necesiten. El administrador debe adjuntar esas políticas a las entidades principales que necesiten esos permisos.

Para obtener instrucciones 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 sobre las políticas
- Uso de la consola del editor de etiquetas y la API de etiquetado de grupos de recursos
- Cómo permitir a los usuarios consultar sus propios permisos
- Visualización de grupos basados en etiquetas

Prácticas recomendadas sobre las políticas

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

- Comience con las políticas administradas de 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 de AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para los 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 del 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.
- Utilice 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 políticas 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 de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice 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. El analizador de acceso de IAM proporciona más de 100 verificaciones

de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. xPara 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 la MFA a sus políticas. Para obtener más información, consulte Configuración de acceso a una API protegida por MFA en la Guía del usuario de IAM.

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

Uso de la consola del editor de etiquetas y la API de etiquetado de grupos de recursos

Para acceder a la consola del editor de etiquetas y a la API de etiquetado de grupos de recursos, debe disponer de un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de las etiquetas adjuntas en los recursos en su Cuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola y los comandos de la API no funcionarán según lo previsto para las entidades principales de IAM con esa política.

Para asegurarse de que esas entidades principales puedan seguir utilizando el editor de etiquetas, adjunte la siguiente política (o una política que contenga los permisos enumerados en la siguiente política) a las entidades. Para obtener más información, consulte Agregar de permisos a un usuario en la Guía del usuario de IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:List*"
      ],
```

```
      "Resource": "*"
    }
  ]
}
```

Para obtener más información sobre cómo conceder acceso a la API de etiquetado del editor de etiquetas y etiquetado de grupos de recursos, consulteConcesión de permisos para utilizar el editor de etiquetas.

Cómo permitir a los usuarios 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 asocian a la identidad de sus usuarios. Esta política incluye permisos para realizar 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": "*"
        }
    ]
}
```

Visualización de grupos basados en etiquetas

Puede utilizar las condiciones de su política basada en la identidad para controlar el acceso a los recursos del editor de etiquetas basados en etiquetas. Este ejemplo muestra cómo puede crear una política que permita visualizar un recurso, en este ejemplo, un grupo de recursos. Sin embargo, el permiso se concede solo si la etiqueta de grupo `project` tiene el mismo valor que la etiqueta `project` adjunta a la entidad principal de seguridad que llama.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name"
        },
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
            }
        }
    ]
}
```

También puede adjuntar esta política al usuario de en su cuenta. Si un usuario con la clave de etiqueta `project` y el valor de etiqueta `alpha` intenta ver un grupo de recursos, el grupo también debe estar etiquetado `project=alpha`. De lo contrario, se deniega el acceso al usuario. La clave de la etiqueta de condición `project` coincide con los nombres de las claves de condición `Project` y `project` porque no distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

Solución de problemas de identidades y accesos en el editor de etiquetas

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con el editor de etiquetas e IAM.

Temas

No tengo permiso para realizar una acción en el editor de etiquetas

Si la AWS Management Console le indica que no tiene autorización para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

El siguiente ejemplo de error se produce cuando el usuario `mateojackson` intenta utilizar la consola para ver las etiquetas de un recurso pero no tiene permisos `tag:GetTagKeys`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 tag:GetTagKeys on resource: arn:aws:resource-groups::us-west-2:123456789012:resource-
type/my-test-resource
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso `my-test-resource` mediante la acción `tag:GetTagKeys`.

No estoy autorizado a realizar actividades como: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol al editor de etiquetas.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en el editor de etiquetas. Sin embargo, la acción requiere que el servicio cuente con permisos que concede un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

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

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

Registro y monitoreo en el editor de etiquetas

Todas las acciones del editor de etiquetas están registradas en AWS CloudTrail.

Registrar llamadas a la API del editor de etiquetas con CloudTrail

El editor de etiquetas está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un Servicio de AWS usuario del editor de etiquetas. CloudTrail captura todas las llamadas a la API de Tag Editor como eventos, incluidas las llamadas desde la consola de Tag Editor y las llamadas de código a la API de etiquetado de Resource Groups. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para Tag Editor. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por Tag Editor CloudTrail, puedes determinar la solicitud que se realizó a Tag Editor, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información al respecto CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información sobre el editor de etiquetas en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Tag Editor o en la consola de Tag Editor, esa actividad se registra en un CloudTrail evento junto con otros Servicio de AWS eventos del historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para mantener un registro continuo de eventos en la Cuenta de AWS, incluidos los eventos del editor de etiquetas, cree un registro de seguimiento. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de

seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otros Servicios de AWS para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte los siguientes recursos:

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

Todas las acciones del editor de etiquetas se registran CloudTrail y se documentan en la referencia de la API del editor de etiquetas. Las acciones del editor de etiquetas en la consola CloudTrail las registra y se muestran como eventos con `tagging.amazonaws.com` el `eventSource`.

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

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

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

Comprender las entradas del archivo de registro del editor de etiquetas

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud 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. CloudTrail Los archivos de registro no son un registro de pila ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661372702",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661372702",
        "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": "2022-08-24T20:25:03Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-24T20:27:14Z",
    "eventSource": "tagging.amazonaws.com",
    "eventName": "TagResources",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.65",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resourcegroupstaggingapi.tag-resources",
    "requestParameters": {
        "resourceARNList": [
            "arn:aws:events:us-east-1:123456789012:rule/SecretsManagerMonitorRule"
        ],
        "tags": {
            "owner": "alice"
        }
    },
    "responseElements": {
        "failedResourcesMap": {}
    },
    "requestID": "8f9ea891-4125-460c-802f-26c11EXAMPLE",
```

```
    "eventID": "b2c9322a-aad7-424b-8f0b-423daEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "tagging.us-east-1.amazonaws.com"
    }
}
```


Validación de la conformidad en el editor de etiquetas

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

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

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

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

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

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, por ejemplo PCIDSS, cumpliendo con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en el editor de etiquetas

El editor de etiquetas realiza copias de seguridad automatizadas en los recursos del servicio interno. Estas copias de seguridad no son configurables por el usuario. Las copias de seguridad se cifran, tanto en reposo como en tránsito. El editor de etiquetas almacena datos de clientes en Amazon DynamoDB.

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS 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 latencia. Con las zonas de disponibilidad, puede diseñar y utilizar

aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Si elimina etiquetas accidentalmente, póngase en contacto con el AWS SupportCentro.

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 el editor de etiquetas

El editor de etiquetas no proporciona formas adicionales de aislar el tráfico de red o de servicio. Si corresponde, use un aislamiento específico AWS. Puede usar la API y la consola del editor de etiquetas en una nube privada virtual (VPC) para ayudar a maximizar la privacidad y la seguridad de la infraestructura.

Puede utilizar llamadas a la API publicadas en AWS para acceder al editor de etiquetas 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) 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 principal de seguridad de AWS Identity and Access Management (IAM). También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

El editor de etiquetas no admite las políticas basadas en recursos.

Puede llamar a las operaciones del editor de etiquetas de la API desde cualquier ubicación de red, pero el editor de etiquetas admite políticas de acceso basadas en recursos, que pueden incluir restricciones en función de la dirección IP de origen. También puede utilizar políticas del editor de etiquetas para controlar el acceso desde puntos de enlace específicos de Amazon Virtual Private Cloud (Amazon VPC) o VPC específicas. Este enfoque aísla con eficacia el acceso de red a un recurso determinado únicamente desde la VPC específica de la red de AWS.

Service Quotas

En la siguiente tabla se proporciona información sobre las Service Quotas del editor de etiquetas.

Actualmente, estas cuotas no se pueden ajustar mediante la Consola Service Quotas. Póngase en contacto con AWS Support.

Nombre	Predeterminado
Etiquetas adjuntas por recurso	50 etiquetas definidas por el usuario (las etiquetas AWS generadas no se tienen en cuenta para este límite).
Nombre de la clave de etiqueta	Mínimo de 1, máximo 128 caracteres Unicode en UTF -8. Los caracteres permitidos incluyen espacios, números y letras, además de los siguientes caracteres especiales: `_ . : / = + - @` Los nombres de clave no pueden empezar `aws:` por él porque ese prefijo está reservado para su AWS uso. **Note** Algunos Servicios de AWS tienen restricciones adicionales de caracteres o longitud. Para obtener más información, consulte

Nombre	Predeterminado
	la documentación del servicio específico.
Tag value (Valor de etiqueta)	Un mínimo de 0 y un máximo de 256 caracteres Unicode en UTF -8. Los caracteres permitidos incluyen espacios, números y letras, además de los siguientes caracteres especiales: `_ . : / = + - @` **Note** Algunas Servicios de AWS tienen restricciones adicionales de caracteres o longitud. Para obtener más información, consulte la documentación del servicio específico.
Tasa de llamadas a la GetResourcesAPIoperación	Máximo de 15 llamadas por segundo

Nombre	Predeterminado	
Tasa de llamadas a las siguientes API operaciones: • TagResources • UntagResources • GetTagKeys • GetTagValues	Máximo de 5 llamadas por segundo	

Historial de documentos del editor de etiquetas

Cambio	Descripción	Fecha
Se han actualizado los permisos para evaluar el cumplimiento en toda la organización	Se actualizaron los permisos para evaluar el cumplimiento en toda la organización para incluir los permisos que ayudan a acceder al informe de cumplimiento.	28 de agosto de 2024
Contenido actualizado	Se actualizaron los títulos de los temas y se reorganizó el contenido para mejorar la legibilidad y la visibilidad.	25 de julio de 2024
Etiquetar contenido de Referencia general de AWS se trasladó a esta guía	Los temas sobre cómo etiquetar tus AWS los recursos se movieron del Referencia general de AWS a esta guía.	24 de marzo de 2023
IAMactualización de mejores prácticas	Guía actualizada para alinearla con las IAM mejores prácticas. Para obtener más información, consulte las mejores prácticas de seguridad en IAM.	3 de enero de 2023
Mover la documentación del editor de etiquetas a su propia guía	La documentación del editor de etiquetas ahora se incluye en su propia guía de usuario en lugar de formar parte del AWS Resource Groups Guía del usuario.	13 de diciembre de 2022
Compruebe el cumplimiento de las políticas de etiquetas	Después de crear y adjuntar políticas de etiquetas a las	26 de noviembre de 2019

	cuentas mediante AWS Organizations, puede encontrar etiquetas no conformes en los recursos de las cuentas de su organizac ión.	
El editor de etiquetas ahora permite encontrar recursos sin etiquetar	Ahora puede buscar recursos en el editor de etiquetas que no tengan valores de etiqueta aplicados para una clave de etiqueta específica.	18 de junio de 2019
La consola del editor de etiquetas sale de AWS Systems Manager consola	La consola del editor de etiquetas ahora es independi ente de la consola de Systems Manager. Aunque todavía puede encontrar los punteros a la consola del Editor de etiquetas en la barra de navegación izquierda de Systems Manager, puede abrir la consola del Editor de etiquetas directamente desde el menú desplegable de la parte superior izquierda del AWS Management Console.	5 de junio de 2019
Las herramientas del editor de etiquetas antiguas y heredadas ya no están disponibles	Se han eliminado las menciones a los editores de etiquetas antiguos, clásicos o antiguos; estas herramien tas ya no están disponibles en AWS. En su lugar, utilice el editor de etiquetas.	14 de mayo de 2019

El editor de etiquetas ahora admite el etiquetado de recursos en varias regiones	El editor de etiquetas ahora le permite buscar y administrar las etiquetas de recursos en varias regiones, con su región actual añadida a las consultas de recursos por defecto.	2 de mayo de 2019
El editor de etiquetas ahora permite exportar los resultados de las consultas a un CSV	Puede exportar los resultados de una consulta de la página Buscar recursos para etiquetar a un archivo CSV con formato. Se muestra una nueva columna de región en los resultados de la consulta del editor de etiquetas. El editor de etiquetas ahora le permite buscar los recursos que tienen valores vacíos para una clave de etiqueta específica. Los valores de clave se completan de forma automática a medida que escribe un valor único entre las claves existentes.	2 de abril de 2019

El editor de etiquetas ahora admite la adición de todos los tipos de recursos a una consulta	Puede aplicar etiquetas hasta a un máximo de 20 tipos de recursos individuales en una única operación o puede elegir Todos los tipos de recursos para consultar todos los tipos de recursos de una región. Se ha añadido la finalización automática al campo Clave de etiqueta de una consulta para ayudar a habilitar claves de etiquetas consistentes entre recursos. Si los cambios de etiqueta fallan en algunos recursos, puede volver a intentar los cambios de etiquetas solo en los recursos en los que han fallado los cambios de etiqueta.	19 de marzo de 2019
El editor de etiquetas ahora admite varios tipos de recursos en una búsqueda	Puede aplicar etiquetas a un máximo de 20 tipos de recursos en una sola operación. También puede elegir que columnas que le aparecen en los resultado s de búsqueda, incluidas las columnas de cada clave de etiqueta única que aparecen en sus resultados de búsqueda o en los recursos seleccionados de los resultado s.	26 de febrero de 2019

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.