IAM

Guía de usuario

Edición 01

Fecha 2022-11-08

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Marcas registradas y permisos

El logotipo HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.
Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Es posible que la totalidad o parte de los productos, las funcionalidades y/o los servicios que figuran en el presente documento no se encuentren dentro del alcance de un contrato vigente entre Huawei Cloud y el cliente. Las funcionalidades, los productos y los servicios adquiridos se limitan a los estipulados en el respectivo contrato. A menos que un contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en el presente documento constituye garantía alguna, ni expresa ni implícita.

Huawei está permanentemente preocupada por la calidad de los contenidos de este documento; sin embargo, ninguna declaración, información ni recomendación aquí contenida constituye garantía alguna, ni expresa ni implícita. La información contenida en este documento se encuentra sujeta a cambios sin previo aviso.

Huawei Cloud Computing Technologies Co., Ltd.

Dirección: Huawei Cloud Data Center Jiaoxinggong Road
Avenida Qianzhong
Nuevo distrito de Gui'an
Gui Zhou, 550029
República Popular China

Sitio web: https://www.huaweicloud.com/intl/es-us/

Índice

1 Antes de comenzar

Destinatarios

El Identity and Access Management (IAM) está destinado a administradores, entre los que se incluyen:

- Administrador de cuentas (con permisos completos para todos los servicios, incluido IAM)
- Usuarios de IAM agregados al grupo de **admin** (con permisos completos para todos los servicios, incluido IAM)
- Los usuarios de IAM asignados al rol de **Security Administrator** (con permisos para acceder a IAM)

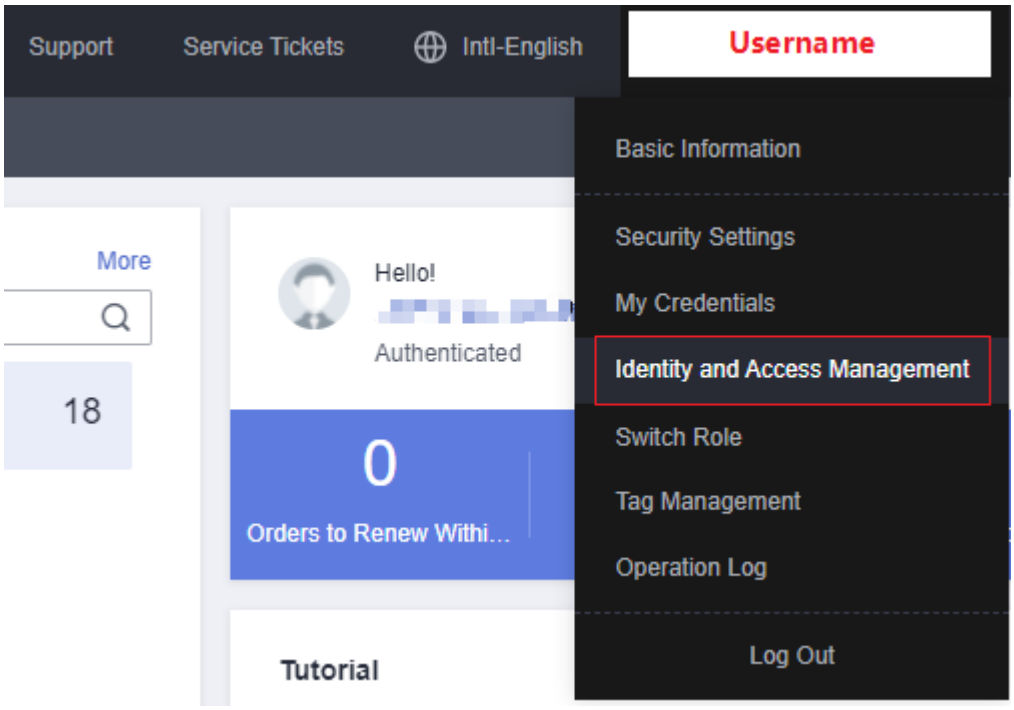
Si desea ver, auditar y realizar un seguimiento de los registros de las operaciones clave realizadas en IAM, habilite Cloud Trace Service (CTS). Para obtener más información, véase **12.1 Habilitación de CTS**.

Acceso a la consola IAM

Paso 1 Inicie sesión en Huawei Cloud y haga clic en **Console** en la esquina superior derecha.

Figura 1-1 Acceso a la consola

Paso 2 En la consola de gestión, coloque el puntero del ratón sobre el nombre de usuario en la esquina superior derecha y elija **Identity and Access Management** en la lista desplegable.



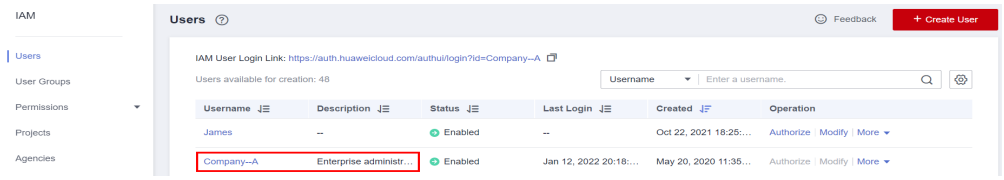
----Fin

Cuenta

Se crea una cuenta después de registrarse con éxito en Huawei Cloud. Su cuenta tiene permisos de acceso completos para sus recursos y realiza pagos por el uso de estos recursos. No puede modificar o eliminar su cuenta en IAM, pero puede hacerlo en My Account.

Después de iniciar sesión en su cuenta, verá un usuario marcado como **Enterprise administrator** en la página **Users** de la consola de IAM.

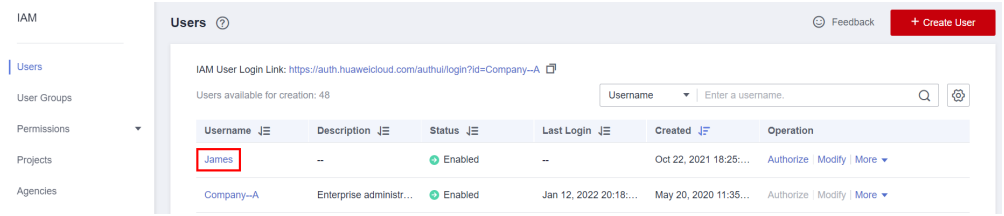
Figura 1-2 Usuario de IAM correspondiente a la cuenta



Usuario de IAM

Puede crear usuarios en IAM como administrador y asignar permisos para recursos específicos. Como se muestra en la siguiente figura, **James** es un usuario de IAM creado por el administrador. Los usuarios de IAM pueden iniciar sesión en Huawei Cloud con su nombre de cuenta, nombres de usuario y contraseñas, y luego usar recursos basados en los permisos asignados. Los usuarios de IAM no poseen recursos y no pueden realizar pagos. Usted usa su cuenta para pagar sus facturas.

Figura 1-3 Usuario de IAM creado por el administrador

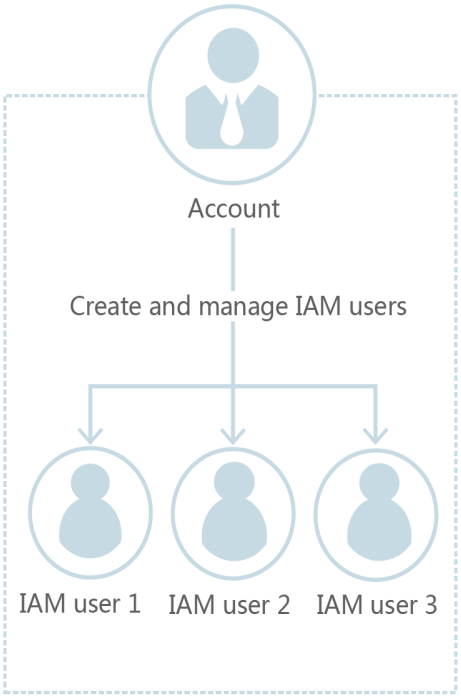


Relación entre una cuenta y sus usuarios de IAM

Una cuenta y sus usuarios de IAM comparten una relación padre-hijo. La cuenta es propietaria de los recursos y realiza pagos por los recursos utilizados por los usuarios de IAM. Tiene permisos completos para estos recursos.

Los usuarios de IAM son creados por el administrador de la cuenta y solo tienen los permisos otorgados por el administrador. El administrador puede modificar o revocar los permisos de los usuarios de IAM en cualquier momento. Las tarifas generadas por el uso de los recursos de los usuarios de IAM son pagadas por la cuenta.

Figura 1-4 Relación entre una cuenta y sus usuarios de IAM

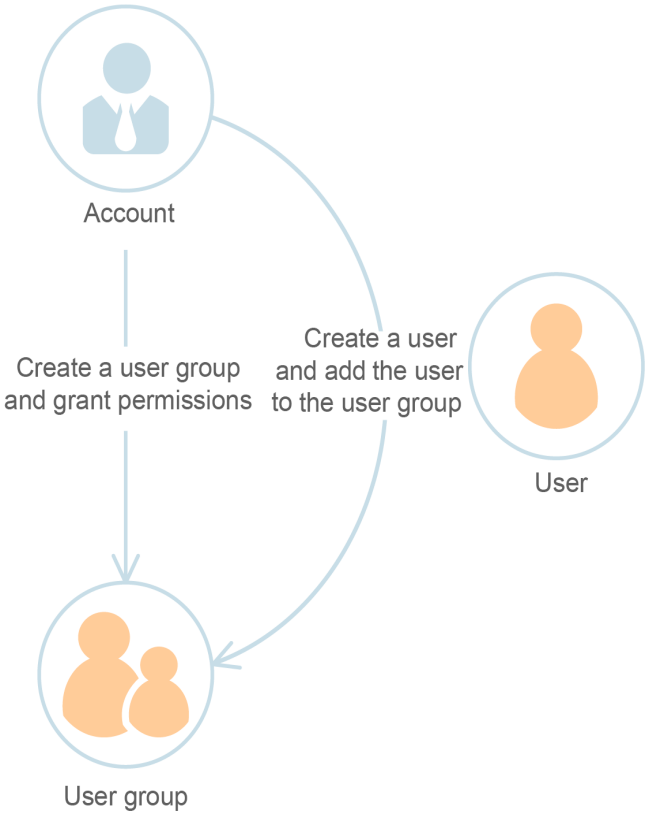


Grupo de usuario

Puede utilizar grupos de usuarios para asignar permisos a los usuarios de IAM. Después de agregar un usuario de IAM a un grupo de usuarios, el usuario tiene los permisos del grupo y puede realizar operaciones en servicios en la nube según lo especificado por los permisos. Si se agrega un usuario a varios grupos de usuarios, el usuario heredará los permisos asignados a todos estos grupos.

El grupo de usuarios predeterminado **admin** tiene todos los permisos necesarios para usar todos los recursos de la nube. Los usuarios de este grupo pueden realizar operaciones en todos los recursos, incluidas, entre otras, la creación de grupos de usuarios y usuarios, la modificación de permisos y la gestión de recursos.

Figura 1-5 Grupo de usuario



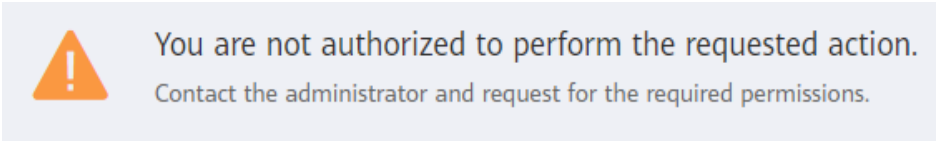
Permiso

IAM proporciona permisos comunes para diferentes servicios, como permisos de administrador y de solo lectura. Los nuevos usuarios de IAM no tienen ningún permiso asignado de forma predeterminada. El administrador debe agregarlos a uno o más grupos y adjuntar políticas o roles de permisos a estos grupos para que los usuarios de IAM puedan heredar permisos de los grupos. Los usuarios de IAM también pueden asignarse permisos a sí mismos A continuación, los usuarios de IAM pueden realizar operaciones específicas en servicios en la nube.

- Roles: un tipo de mecanismo de autorización de grano grueso que define permisos de nivel de servicio en función de las responsabilidades del usuario. Solo hay un número limitado de roles para conceder permisos a los usuarios. Al usar roles para conceder permisos, también debe asignar roles de dependencia. Los roles no son una opción ideal para la autorización detallada y el control de acceso seguro.
- Políticas: Un tipo de mecanismo de autorización detallado que define los permisos necesarios para realizar operaciones en recursos de nube específicos bajo ciertas condiciones. Este mecanismo permite una autorización basada en políticas más flexible sobre la base del principio de mínimo privilegio (PoLP). Por ejemplo, puede conceder a los usuarios de Elastic Cloud Server (ECS) solo los permisos necesarios para administrar un determinado tipo de recursos de ECS.

Cuando un usuario de IAM con permisos ECS únicamente accede a otros servicios, se mostrará un mensaje similar al siguiente.

Figura 1-6 Sin permisos

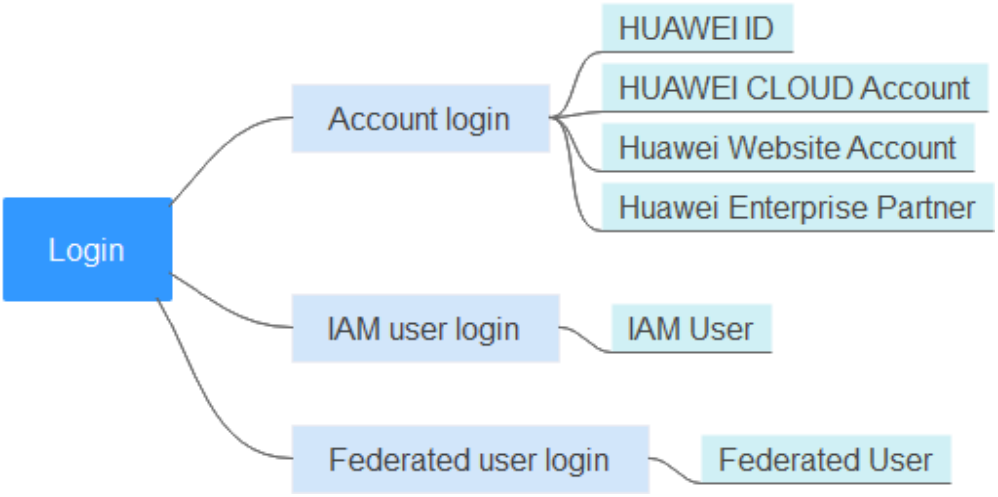


2 Inicio de sesión en Huawei Cloud

Puede iniciar sesión en Huawei Cloud con cualquiera de los siguientes métodos (consulte **Figura 2-1**):

- **Inicio de sesión con cuenta**: Inicie sesión con la cuenta que se creó cuando usa Huawei Cloud. Su cuenta tiene permisos de acceso completos para sus recursos y realiza pagos por el uso de estos recursos. Para iniciar sesión en Huawei Cloud con una cuenta, haga lo siguiente:
  - **ID de HUAWEI**: Un ID de HUAWEI es una identidad unificada que puedes usar para acceder a todos los servicios de Huawei. Es **diferente de una cuenta de Huawei Cloud**. Asegúrese de que ya ha registrado un ID de HUAWEI. Si no tiene un ID de HUAWEI, cree uno y utilícelo para habilitar los servicios en Huawei Cloud. Para obtener más información, consulte **Registro de un ID de HUAWEI y Habilitación de servicios de Huawei Cloud**.
  - **Cuenta de Huawei Cloud**: Use su cuenta de Huawei Cloud para iniciar sesión. Si es la primera vez que utiliza Huawei Cloud, **registre un ID de HUAWEI y habilite los servicios de Huawei Cloud**.
  - **Otras cuentas**: cuando inicie sesión con una **Huawei website account** o **Huawei enterprise partner account** por primera vez, asocie estas cuentas con una cuenta de Huawei Cloud existente o nueva. En el siguiente inicio de sesión, puede iniciar sesión directamente con la cuenta del sitio web de Huawei o la cuenta de socio empresarial de Huawei. Alternativamente, puede usar la cuenta de Huawei Cloud para iniciar sesión.
- **IAM user login**: los usuarios de IAM son creados por un **administrador** para usar servicios en la nube específicos.
  - **Usuario de IAM**: **Una cuenta y usuarios de IAM** comparten una relación padre-hijo. Los usuarios de IAM solo pueden usar servicios en la nube específicos basados en permisos asignados.
- **Inicio de sesión de usuario federado**: Los usuarios federados se registran con un IdP de empresa creado por el administrador en IAM.
  - **Usuario federado**: puede iniciar sesión en Huawei Cloud como usuario federado si ha obtenido el nombre del proveedor de identidad, la cuenta de Huawei Cloud utilizada para crear este proveedor de identidad y el nombre de usuario y la contraseña para iniciar sesión en su sistema de gestión empresarial.

Figura 2-1 Inicio de sesión en Huawei Cloud



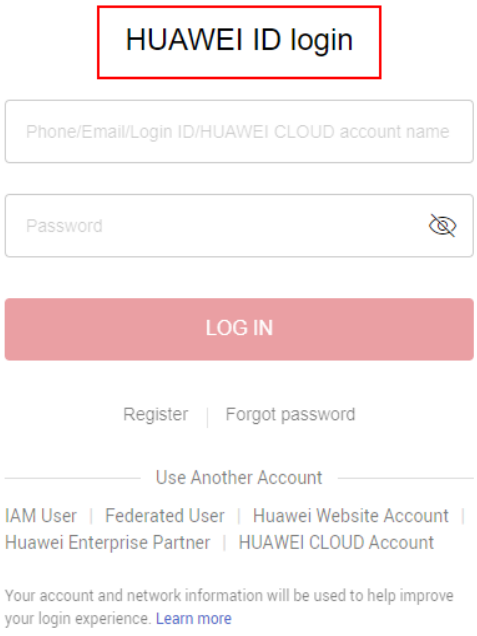
Iniciar sesión con un ID de HUAWEI

Un ID de HUAWEI es una identidad unificada que puedes usar para acceder a todos los servicios de Huawei. Puede registrar y gestionar un ID de HUAWEI en el sitio web de **ID de HUAWEI**. También puede **registrar un ID de HUAWEI y usarlo para habilitar los servicios de Huawei Cloud** en Huawei Cloud. Al iniciar sesión en la consola de Huawei Cloud con un ID de HUAWEI, puede introducir un número de teléfono móvil, una dirección de correo electrónico, un ID de inicio de sesión o un nombre de cuenta de Huawei Cloud.

Para iniciar sesión con un ID de HUAWEI, haga lo siguiente:

Paso 1 En la página de inicio de sesión, introduzca su número de teléfono móvil, dirección de correo electrónico, ID de inicio de sesión o nombre de cuenta de Huawei Cloud, introduzca la contraseña y, a continuación, haga clic en **LOG IN**.

Figura 2-2 Iniciar sesión con un ID de HUAWEI



NOTA

- Puede ingresar una cuenta de Huawei Cloud o un ID de HUAWEI que se haya utilizado para habilitar los servicios de Huawei Cloud.
- Si introduce un ID de HUAWEI cuyo número de teléfono móvil o dirección de correo electrónico se ha utilizado para habilitar los servicios de Huawei Cloud, vaya a **Paso 2**.
- Si introduce un ID de HUAWEI cuyo número de teléfono móvil o dirección de correo electrónico no se han utilizado para habilitar los servicios en la nube de Huawei, vaya a **Paso 3**.

Paso 2 Seleccione la cuenta que desea utilizar para iniciar sesión.

Si el número de teléfono móvil o la dirección de correo electrónico que ingresó se han utilizado para registrar un ID de HUAWEI y una cuenta de Huawei Cloud, seleccione una cuenta para iniciar sesión.

- Seleccione el ID de HUAWEI y haga clic en **OK**. A continuación, vaya a **Paso 3**.
- Seleccione la cuenta de Huawei Cloud y haga clic en **OK**. El inicio de sesión es exitoso.

Paso 3 Haga clic en **Get code**, introduzca el código de verificación y haga clic en **OK**.

Si ya ha asociado un número de teléfono móvil y una dirección de correo electrónico con su ID de HUAWEI, puede elegir la verificación del número de teléfono móvil o de la dirección de correo electrónico.

Paso 4 En **Trust this browser?** cuadro de diálogo, haga clic en **TRUST**.

Paso 5 En el cuadro de diálogo que se muestra, haga clic en **Enable HUAWEI CLOUD Services** o **Use Another HUAWEI CLOUD Account**.

- **Enable HUAWEI CLOUD Services**: Haga clic en este botón para habilitar servicios de Huawei Cloud para el ID de HUAWEI de modo que pueda usar el ID de HUAWEI para iniciar sesión en Huawei Cloud. Después de hacer clic en este botón, vaya a **Paso 6**.
- **Use Another HUAWEI CLOUD Account**: Haga clic en este botón para iniciar sesión con otra cuenta de Huawei Cloud. Después de hacer clic en este botón, vaya a **Paso 1**.

Paso 6 (Opcional) Si el número de teléfono móvil o la dirección de correo electrónico que ingresó se han utilizado para registrarse en las cuentas de Huawei Cloud, seleccione una cuenta y asóciela con su ID de HUAWEI.

NOTA

Después de asociar una cuenta de Huawei Cloud con su ID de HUAWEI, puede usar el ID de HUAWEI para acceder a Huawei Cloud, desarrolladores de HUAWEI, VMALL y otros servicios de Huawei.

- Asociar una cuenta de Huawei Cloud con su ID de HUAWEI
  a. Seleccione una cuenta de Huawei Cloud y haga clic en **Next**.
  b. Ingrese la contraseña de la cuenta de Huawei Cloud y haga clic en **Next**.
  c. Confirme la información del ID de HUAWEI y haga clic en **OK**.
  d. Haga clic en **OK**. Se muestra la página de inicio de Huawei Cloud.

  NOTA

  - Después de realizar los pasos anteriores, su cuenta de Huawei Cloud se asocia con su ID de HUAWEI y no es válida. Necesita usar el ID de HUAWEI para el siguiente inicio de sesión.
  - Si la actualización falla, consulte "¿Qué puedo hacer si la actualización a un ID de HUAWEI falla?" en las *Preguntas frecuentes de IAM*.

- Habilitación de los servicios de Huawei Cloud

  Haga clic en **Skip This Step and Enable HUAWEI CLOUD Services**, y vaya a **Paso 7**.

Paso 7 En la página **Enable HUAWEI CLOUD Services**, lea los acuerdos de servicio y confirme que los acepta y, a continuación, haga clic en **Enable**.

Ahora puede usar el ID de HUAWEI para iniciar sesión en Huawei Cloud.

----Fin

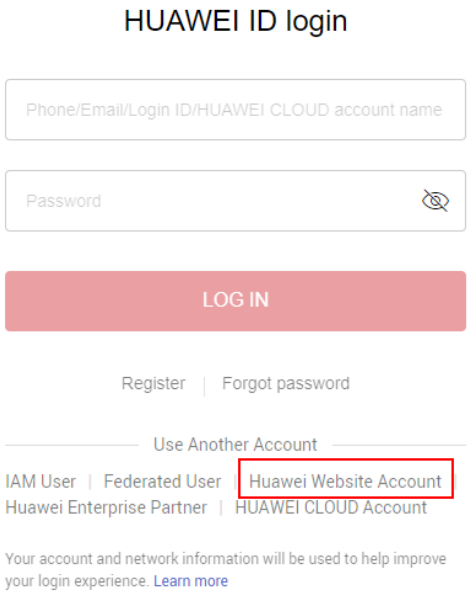
Iniciar sesión con otras cuentas

Si ya tiene una **cuenta de sitio web de Huawei** o **cuenta de socio empresarial de Huawei**, puede usarlos para iniciar sesión en Huawei Cloud sin memorizar credenciales adicionales.

El siguiente procedimiento describe cómo usar una cuenta del sitio web oficial de Huawei para iniciar sesión en Huawei Cloud.

Paso 1 En la página de inicio de sesión, haga clic en **Huawei Website Account**, como se muestra en la siguiente figura.

Figura 2-3 Iniciar sesión con una cuenta de sitio web de Huawei



Paso 2 Inicie sesión con su cuenta de sitio web de Huawei.

- Si este es el primer inicio de sesión, se le solicitará que vincule su cuenta de sitio web de Huawei con una cuenta de Huawei Cloud existente o nueva. Para crear una nueva cuenta de Huawei Cloud, ingresa el nombre de la cuenta, el número de teléfono móvil y el código de verificación. Haga clic en **Create and Bind**.
- Si este no es el primer inicio de sesión, puede iniciar sesión directamente con su cuenta del sitio web de Huawei.

La próxima vez que inicie sesión en la consola de Huawei Cloud, puede usar el nombre o el número de teléfono establecido en **Paso 2** para la cuenta de Huawei Cloud.

----Fin

Iniciar sesión con una cuenta de Huawei Cloud

Si tiene una cuenta de Huawei Cloud, puede usarla para iniciar sesión en Huawei Cloud. La cuenta es propietaria de los recursos que usted compra, realiza pagos por el uso de estos recursos y tiene permisos de acceso completos para ellos. Puede utilizar la cuenta para restablecer las contraseñas de usuario y asignar permisos. Cuando utilice la cuenta para iniciar sesión en la consola de Huawei Cloud, puede elegir iniciar sesión con la cuenta/correo electrónico o iniciar sesión con el número de teléfono móvil.

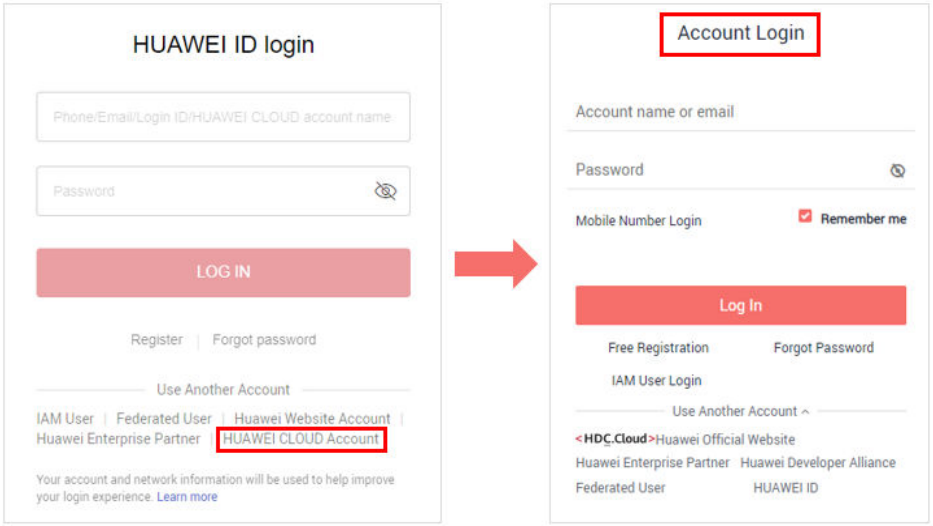
NOTA

Si su cuenta de Huawei Cloud se ha actualizado a un ID de HUAWEI, utilice el ID de HUAWEI para iniciar sesión. Para obtener más información, consulte **Iniciar sesión con un ID de HUAWEI**.

Para iniciar sesión con una cuenta de Huawei Cloud, haga lo siguiente:

Paso 1 En la página de inicio de sesión, haga clic en **HUAWEI CLOUD Account**.

Figura 2-4 Iniciar sesión con una cuenta de Huawei Cloud



Paso 2 Ingrese la información de su cuenta y haga clic en **Log In**.

- **Account name or email**: El nombre de la cuenta o la dirección de correo electrónico asociada a la cuenta.

  NOTA

  Los nombres de cuentas no distinguen entre mayúsculas y minúsculas.

- **Password**: La contraseña de inicio de sesión de la cuenta. Si ha olvidado su contraseña de inicio de sesión, **restablezca** su contraseña en la página de inicio de sesión.
- **Mobile Number Login**: Si ha olvidado el nombre de la cuenta, haga clic en **Mobile Number Login** e introduzca el número de móvil asociado y la contraseña de inicio de sesión para iniciar sesión.

----Fin

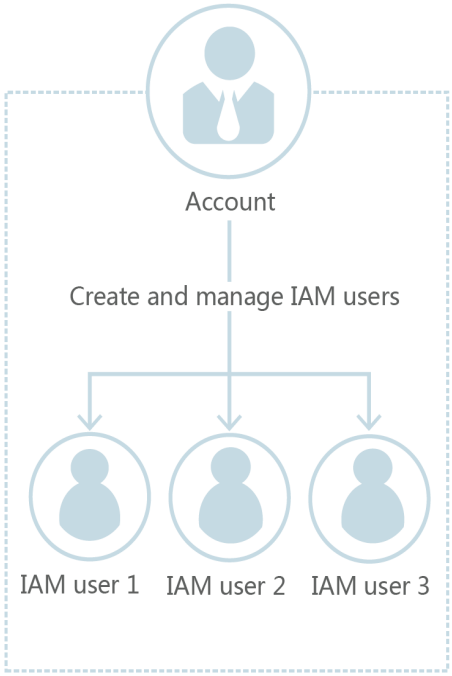
Inicio de sesión como usuario de IAM

Los usuarios de IAM pueden ser creados con su cuenta de Huawei Cloud o por un **administrador**. Cada usuario de IAM tiene sus propias credenciales de identidad (contraseña

y claves de acceso) y utiliza recursos en la nube basados en los permisos asignados. Los usuarios de IAM no poseen recursos y no pueden realizar pagos.

Su cuenta y los usuarios de IAM comparten una relación padre-hijo.

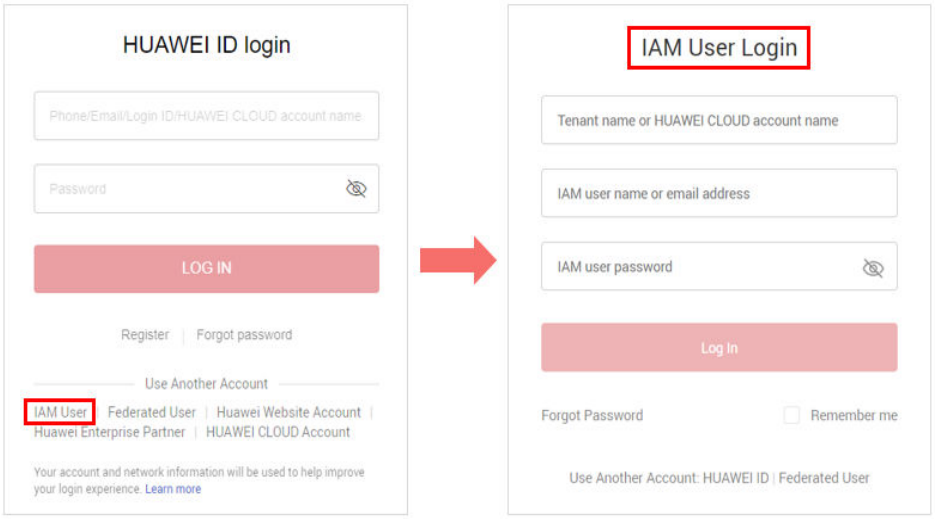
Figura 2-5 Usuarios de cuenta e IAM



Para iniciar sesión como usuario de IAM, haga lo siguiente:

Paso 1 Haga clic en **IAM User** en la página de inicio de sesión y, a continuación, introduzca su nombre de cuenta, nombre de usuario o dirección de correo electrónico de IAM y contraseña.

Figura 2-6 Inicio de sesión como usuario de IAM



- **Tenant name or HUAWEI CLOUD account name**: el nombre de la cuenta que se usó para crear el usuario de IAM, es decir, la **cuenta** de Huawei Cloud. Puede obtener el nombre de cuenta del **administrador**.
- **IAM user name or email address**: El nombre de usuario o dirección de correo electrónico del **usuario de IAM**. Puede obtener el nombre de usuario y la contraseña del **administrador**.
- **IAM user password**: La contraseña del usuario de IAM (no la contraseña de la cuenta).

Paso 2 Haga clic en **Log In**.

----Fin

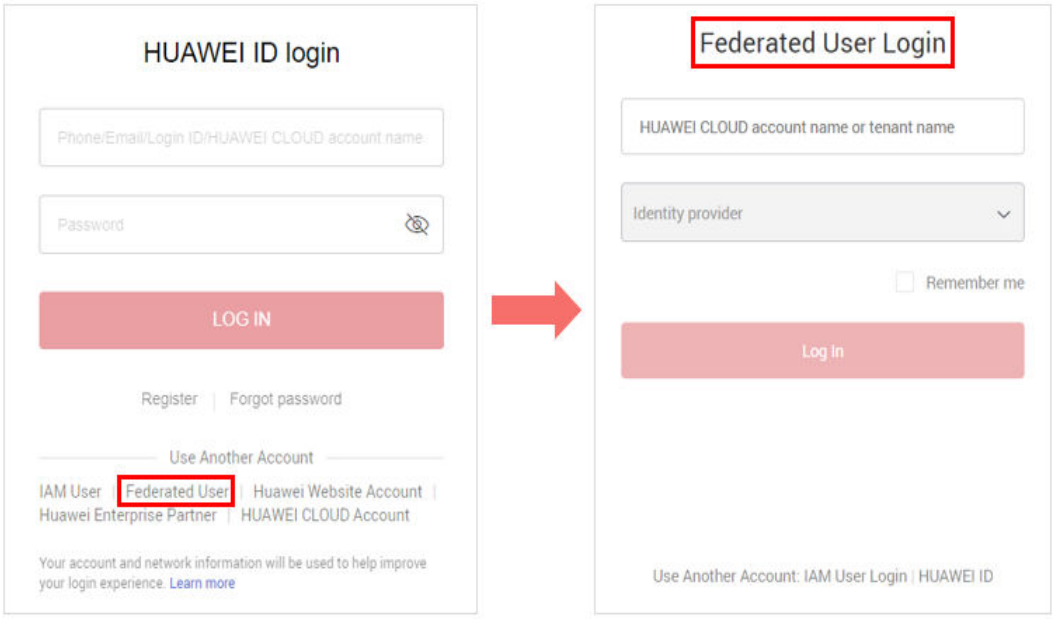
Inicio de sesión como usuario federado

Los usuarios federados se crean en un sistema de gestión empresarial. Después de que el administrador de la cuenta **cree una entidad IdP** en la consola IAM, los usuarios federados pueden iniciar sesión en Huawei Cloud y usar servicios en la nube basados en los permisos asignados. Para obtener más información, véase **9.1 Introducción**.

Puede iniciar sesión en Huawei Cloud como usuario federado si ha obtenido el nombre de su IdP, la cuenta de Huawei Cloud utilizada para crear un IdP y el nombre de usuario y la contraseña para iniciar sesión en su sistema de gestión empresarial.

Paso 1 En la página de inicio de sesión de Huawei Cloud, haga clic en **Federated User**, introduzca el nombre de la cuenta y seleccione un proveedor de identidad.

Figura 2-7 Inicio de sesión como usuario federado



- **Huawei Cloud account name or tenant name**: El nombre de la cuenta de Huawei Cloud que se utiliza para crear el proveedor de identidad. Puede obtener el nombre de cuenta del **administrador**.
- **Identity provider**: nombre del proveedor de identidad creado por el **administrador**. Puede obtener el nombre del proveedor de identidad del **administrador**.

Paso 2 Haga clic en **Log In**. Se muestra la página de inicio de sesión del sistema de gestión empresarial.

Paso 3 Introduzca su nombre de usuario y contraseña para acceder al sistema de gestión empresarial.

Paso 4 Haga clic en el botón de inicio de sesión.

----Fin

3 Usuarios de IAM

3.1 Creación de un usuario de IAM

Si usted es un **administrador** y ha comprado varios recursos en Huawei Cloud, como Elastic Cloud Servers (ECSs), Elastic Volume Service (EVS) discos, y Bare Metal Servers (BMSs), puede crear usuarios de IAM y concederles los permisos necesarios para realizar operaciones en recursos específicos. De esta manera, no es necesario compartir la contraseña de su cuenta.

Los nuevos usuarios de IAM no tienen ningún permiso asignado por defecto. Puede asignar permisos a los nuevos usuarios, o añadirlos a uno o más grupos y conceder permisos a estos grupos haciendo referencia a **Asignación de permisos a un grupo de usuarios** para que los usuarios puedan heredar los permisos de los grupos. Los usuarios pueden realizar operaciones específicas en servicios en la nube según lo especificado por los permisos.

El grupo de usuarios predeterminado **admin** tiene todos los permisos necesarios para usar todos los recursos de la nube. Los usuarios de este grupo pueden realizar operaciones en todos los recursos, incluidas, entre otras, la creación de grupos de usuarios y usuarios, la modificación de permisos y la gestión de recursos.

NOTA

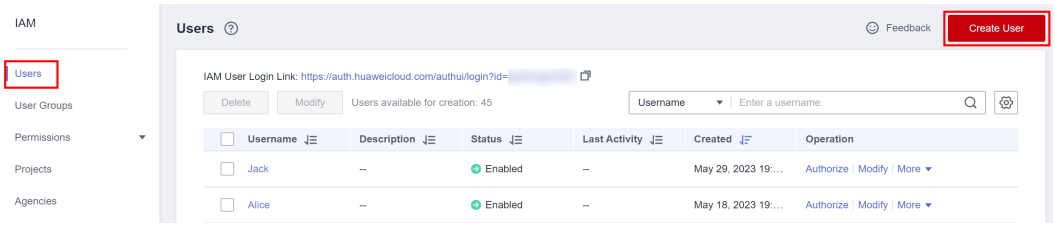
Si elimina un usuario y, a continuación, crea un nuevo usuario con el mismo nombre, deberá conceder de nuevo los permisos necesarios al nuevo usuario.

Procedimiento

Paso 1 Inicie sesión en la **consola de IAM** como administrador.

Paso 2 Elija **Users** en el panel de navegación izquierdo y haga clic en **Create User** en la esquina superior derecha.

Figura 3-1 Creación de un usuario de IAM



Paso 3 Especifique la información del usuario en la página **Create User**. Para crear más usuarios, haga clic en **Add User**. Puede agregar un máximo de 10 usuarios a la vez.

Figura 3-2 Especificación de los detalles del usuario

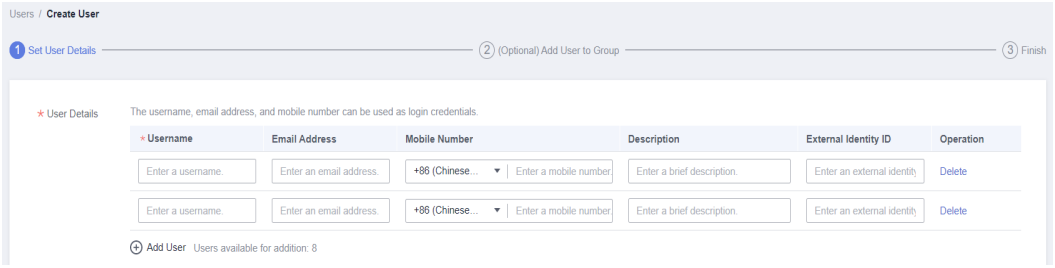


Tabla 3-1 Detalles del usuario

Parámetro	Descripción
Username	Este parámetro está definido por el usuario y no puede ser el mismo que el de cualquier otra cuenta o cualquier usuario de IAM en la cuenta.
Email Address	Este parámetro está definido por el usuario y no puede ser el mismo que el de cualquier otra cuenta o cualquier usuario de IAM en la cuenta. Se puede utilizar para autenticar al usuario de IAM y restablecer la contraseña.
Mobile Number	Este parámetro está definido por el usuario y no puede ser el mismo que el de cualquier otra cuenta o cualquier usuario de IAM en la cuenta. Se puede utilizar para autenticar al usuario de IAM y restablecer la contraseña.
External Identity ID	Identidad de un usuario de empresa en el SSO de usuario de IAM. El valor contiene un máximo de 128 caracteres. Este parámetro debe especificarse si desea configurar **federación de identidad por SAML** para un usuario de IAM.

Paso 4 Especifica **Access Type**.

Figura 3-3 Selección de tipos de acceso

Tabla 3-2 Tipos de acceso

Tipo de acceso	Descripción
Acceso programático	Permite a los usuarios acceder a servicios en la nube mediante herramientas de desarrollo como API, CLI y SDK.
Acceso de gestión de consola	Permite a los usuarios acceder a los servicios en la nube a través de la consola de gestión. Una contraseña es obligatoria para iniciar sesión.

Paso 5 Especifique **Credential Type**.

Figura 3-4 Selección de tipos de credenciales

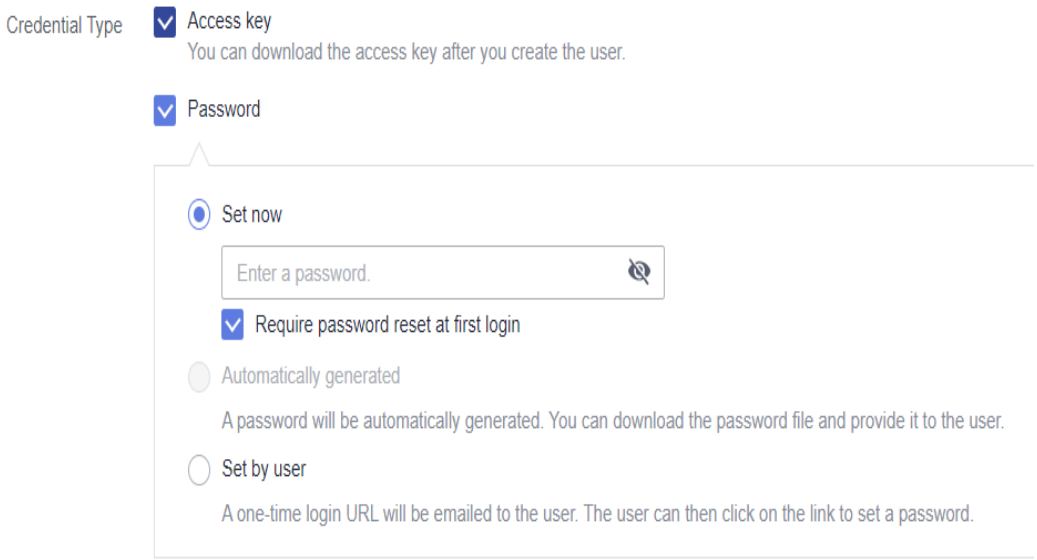


Tabla 3-3 Tipos de credenciales

Tipo de credencial	Descripción
Clave de acceso	Después de crear el usuario, puede descargar la **clave de acceso (AK/SK)** generada para el usuario. **Cada usuario puede tener un máximo de dos claves de acceso.**

Tipo de credencial		Descripción
Contraseña	Configurar ahora	Establezca una contraseña para el usuario y determine si debe requerir que el usuario restablezca la contraseña en el primer inicio de sesión. Si va a utilizar el usuario de IAM por sí mismo, le recomendamos que seleccione esta opción, introduzca una contraseña y anule la selección de **Require password reset at first login**.
	Generada automáticamente	El sistema genera automáticamente una contraseña de inicio de sesión para el usuario. Una vez creado el usuario, puede descargar el archivo de contraseña EXCEL y proporcionar la contraseña al usuario. El usuario puede usar esta contraseña para iniciar sesión. **Esta opción solo está disponible cuando se crea un único usuario.**
	Configurar por el usuario	Se enviará una URL de inicio de sesión única al usuario. El usuario puede hacer clic en el enlace para iniciar sesión en la consola y establecer una contraseña. Si no utiliza el usuario de IAM por sí mismo, seleccione esta opción e introduzca la dirección de correo electrónico y el número de teléfono móvil del usuario de IAM. El usuario puede entonces establecer una contraseña haciendo clic en la URL de inicio de sesión de una sola vez enviada por correo electrónico. La URL de inicio de sesión es válida durante **siete días**.

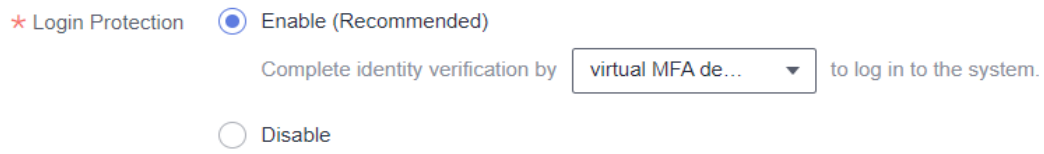
Tabla 3-4 Configuraciones recomendadas

Acceso de gestión de consola	Acceso programático	Tipo de credencial	Tipo de acceso recomendado	Tipo de credencial recomendado
Seleccionar	Deseleccionar	No hay requisitos especiales.	Acceso de gestión de consola	Contraseña
Deseleccionar	Seleccionar	No hay requisitos especiales.	Acceso programático	Clave de acceso
Deseleccionar	Seleccionar	**Se requiere una contraseña como credencial para el acceso programático** (requerido por algunas API).	Acceso programático	Contraseña

Acceso de gestión de consola	Acceso programático	Tipo de credencial	Tipo de acceso recomendado	Tipo de credencial recomendado
Seleccionar	Seleccionar	**La clave de acceso (introducida por el usuario de IAM) debe verificarse en la consola.** Por ejemplo, el usuario debe realizar una verificación de clave de acceso antes de crear un trabajo de migración de datos en la consola de Cloud Data Migration (CDM).	Acceso programático y acceso a la consola de gestión	Contraseña y clave de acceso

Paso 6 Configurar la protección de inicio de sesión. Este parámetro solo está disponible cuando se ha seleccionado **Management console access** para **Access Type**.

Figura 3-5 Habilitación de la protección de inicio de sesión

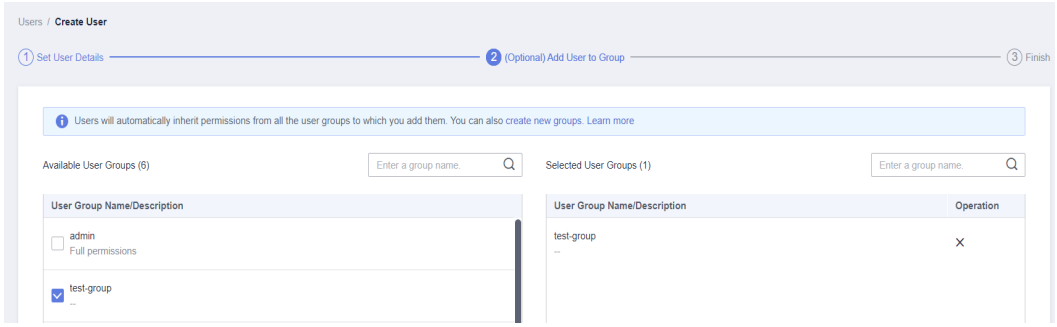


- **Enable (Recommend for account security)**: El usuario debe introducir un código de verificación además del nombre de usuario y la contraseña para iniciar sesión.

  Puede elegir la verificación de inicio de sesión basada en SMS, correo electrónico o MFA virtual.
- **Disable**: El usuario no necesita ingresar un código de verificación para iniciar sesión. Si desea habilitar la protección de inicio de sesión después de crear el usuario, consulte **Protección de inicio de sesión**.

Paso 7 Haga clic en **Next**. Seleccione los grupos de usuarios que desea agregar al usuario. El usuario heredará los permisos asignados a los grupos de usuarios.

Figura 3-6 Agregar el usuario a los grupos de usuarios



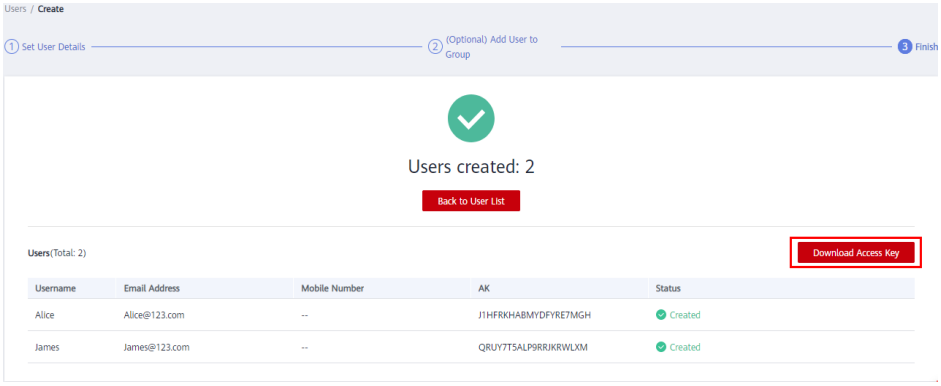
NOTA

- También puede crear un nuevo grupo y agregar el usuario a ese grupo.
- Si desea que el usuario sea administrador, agregue el usuario al grupo predeterminado **admin**.
- Puede agregar un usuario a un máximo de 10 grupos de usuarios.

Paso 8 Haga clic en **Create**.

- Si ha seleccionado **Access key** para **Credential Type** en **Paso 5**, puede descargar la clave de acceso en la página **Finish**.
- Si ha seleccionado **Password** > **Automatically generated** for **Credential Type** en **Paso 5**, puede descargar el archivo de contraseña en la página **Finish**.

Figura 3-7 Usuarios creados correctamente



----Fin

Operaciones relacionadas

- Los usuarios de IAM creados sin ser agregados a ningún grupo no tienen ningún permiso. El administrador puede asignar permisos a estos usuarios de IAM en la consola de IAM. Los usuarios de IAM también pueden asignarse permisos a sí mismos. A continuación, los usuarios pueden usar recursos en la nube basados en los permisos asignados. Para obtener más información, véase **3.2 Asignación de permisos a un usuario de IAM**.
- Las cuentas y los usuarios de IAM utilizan diferentes métodos para iniciar sesión. Para obtener más información sobre el inicio de sesión de usuario de IAM, consulte **3.3 Inicio de sesión como usuario de IAM**.

3.2 Asignación de permisos a un usuario de IAM

Los usuarios de IAM creados sin ser agregados a ningún grupo no tienen ningún permiso. El administrador puede asignar permisos a estos usuarios de IAM en la consola de IAM. Los usuarios de IAM también pueden asignarse permisos a sí mismos. Después de la autorización, los usuarios pueden usar recursos en la nube en su cuenta según lo especificado por sus permisos.

Restricciones

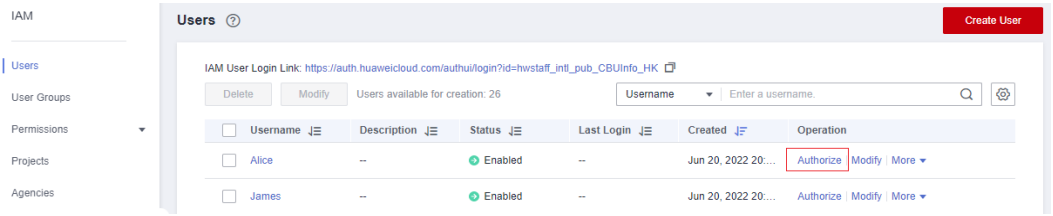
Se pueden asignar un máximo de 500 permisos (incluidos los permisos definidos por el sistema y las políticas personalizadas) a cada usuario de IAM para proyectos empresariales.

Procedimiento

Paso 1 Inicie sesión en la **consola de IAM** como administrador.

Paso 2 En la lista de usuarios, haga clic en **Authorize** en la fila que contiene el usuario de destino.

Figura 3-8 Autorización de un usuario de IAM

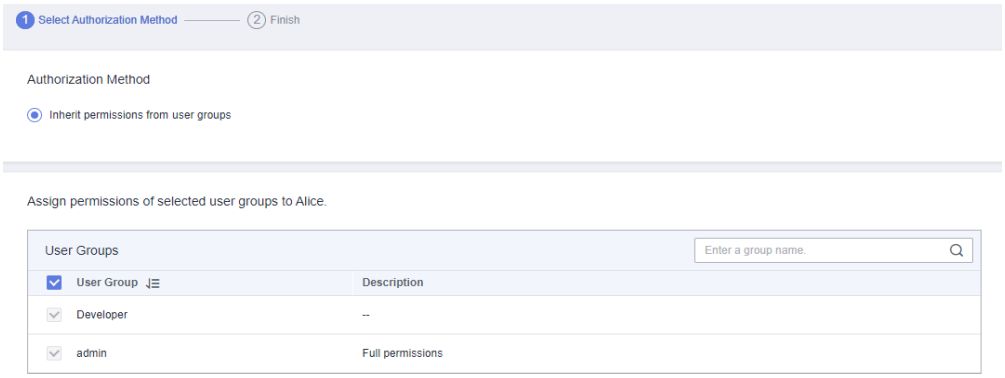


Paso 3 En la página **Authorize User**, seleccione un modo de autorización y permisos.

- **Inherit permissions from user groups**: Agregue el usuario de IAM a ciertos grupos para heredar sus permisos.

  Si selecciona esta opción, seleccione los grupos de usuarios a los que pertenecerá el usuario.

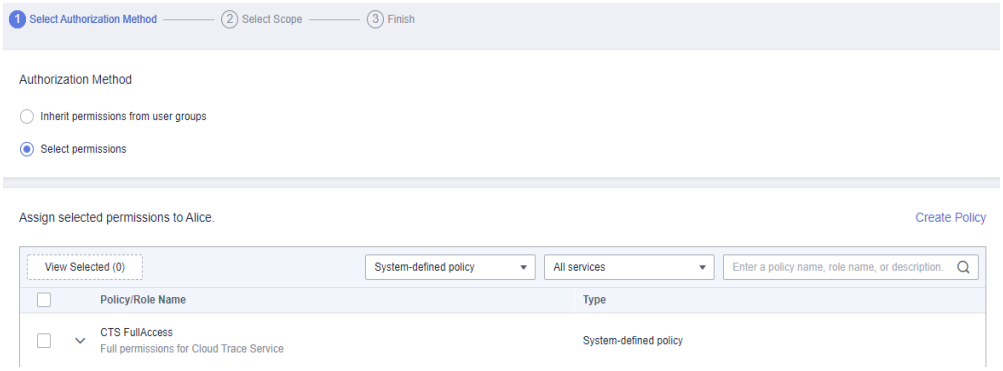
  Figura 3-9 La función de proyecto empresarial no está habilitada

- **Select permissions**: Asigne directamente permisos específicos al usuario de IAM. Puede asignar permisos directamente a los usuarios de IAM solo cuando Enterprise Project esté habilitado. Para habilitar Enterprise Project, consulte **Habilitación de la función del Enterprise Project**.

  Si selecciona esta opción, seleccione permisos, haga clic en **Next** en la parte inferior derecha y, a continuación, vaya a **Paso 4**.

  Figura 3-10 Función de proyecto empresarial habilitada

NOTA

- Si agrega un usuario de IAM al **admin** de grupo predeterminado, el usuario se convierte en administrador y puede realizar todas las operaciones en todos los servicios en la nube.
- Si agrega un usuario a varios grupos de usuarios, el usuario heredará los permisos asignados a estos grupos.
- **Para obtener detalles sobre los permisos definidos por el sistema de todos los servicios en la nube compatibles con IAM, consulte Permisos definidos por el sistema.**
- Si ha habilitado la gestión empresarial, no puede crear subproyectos en IAM.

Paso 4 En la página **Select Scope**, seleccione los proyectos de empresa a los que pueda acceder el usuario de IAM. No es necesario realizar este paso si ha seleccionado **Inherit permissions from user groups**.

Paso 5 Haga clic en **OK**.

Puede ir a la página **Permissions** > **Authorization** y ver o modificar los permisos del usuario de IAM.

----Fin

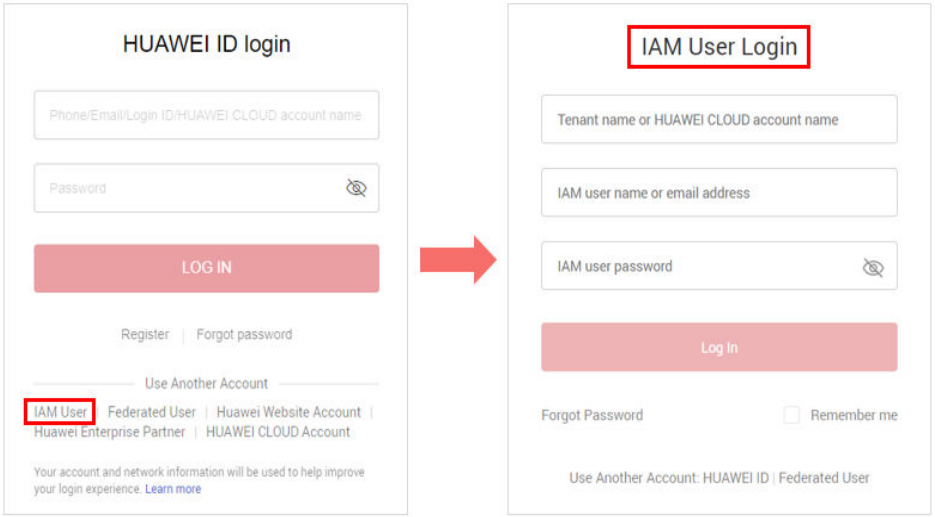
3.3 Inicio de sesión como usuario de IAM

Para iniciar sesión como usuario de IAM, puede elegir **IAM User** en la página de inicio de sesión u obtener el enlace de inicio de sesión de usuario de IAM del administrador.

Método 1: Iniciar sesión haciendo clic en el usuario de IAM

Paso 1 Haga clic en **IAM User** en la página de inicio de sesión y, a continuación, introduzca su nombre de cuenta, nombre de usuario o dirección de correo electrónico de IAM y contraseña.

Figura 3-11 Inicio de sesión como usuario de IAM



- **Tenant name or HUAWEI CLOUD account name**: el nombre de la cuenta que se usó para crear el usuario de IAM, es decir, la **cuenta** de Huawei Cloud. Puede obtener el nombre de cuenta del **administrador**.

- **IAM user name or email address**: El nombre de usuario o dirección de correo electrónico del **usuario de IAM**. Puede obtener el nombre de usuario y la contraseña del **administrador**.
- **IAM user password**: La contraseña del usuario de IAM (no la contraseña de la cuenta).

Paso 2 Haga clic en **Log In**.

NOTA

- Si no se ha agregado a ningún grupo, no tiene permisos para acceder a ningún servicio en la nube. En este caso, póngase en contacto con el administrador y solicite los permisos necesarios (ver **4.1 Creación de un grupo de usuarios y asignación de permisos** y **4.2 Agregar o quitar usuarios de un grupo de usuarios**).
- Si ha sido agregado al **admin** de grupo predeterminado, tiene permisos de administrador y puede realizar todas las operaciones en todos los servicios en la nube.

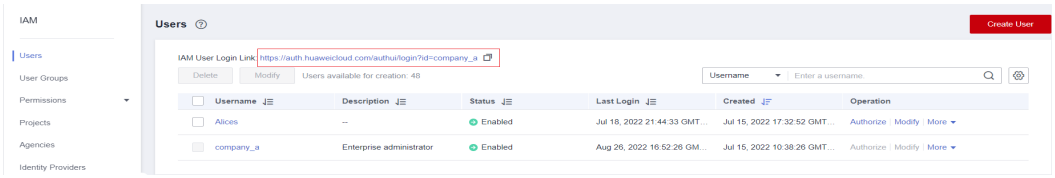
----Fin

Method : Logging In Using the IAM User Login Link

You can obtain the IAM user login link from the administrator and then log in using this link. When you visit the link, the system displays the login page and automatically populates the account name. You only need to enter your username and password.

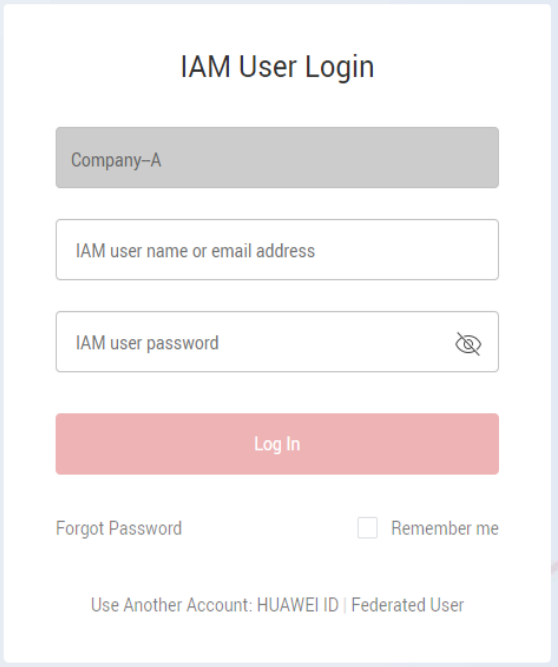
Paso 1 Obtain the IAM user login link from the administrator, who can copy the login link from the **IAM console**.

Figura 3-12 IAM user login link



Paso 2 Paste the link into the address bar of a browser, press **Enter**, and enter the IAM user name/email address and password, and click **Log In**.

Figura 3-13 Logging in using the IAM user login link

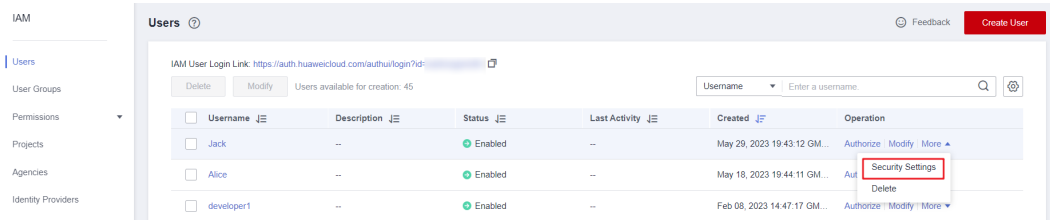


----Fin

3.4 Consulta o modificación de información de usuario de IAM

Como administrador, puede modificar la información básica sobre un usuario de IAM, cambiar la configuración de seguridad del usuario y los grupos a los que pertenece el usuario y ver o eliminar los permisos asignados. Para ver o modificar la información del usuario, haga clic en **Security Settings** en la fila que contiene el usuario de IAM.

Figura 3-14 Ir a la página de configuración de seguridad del usuario de IAM



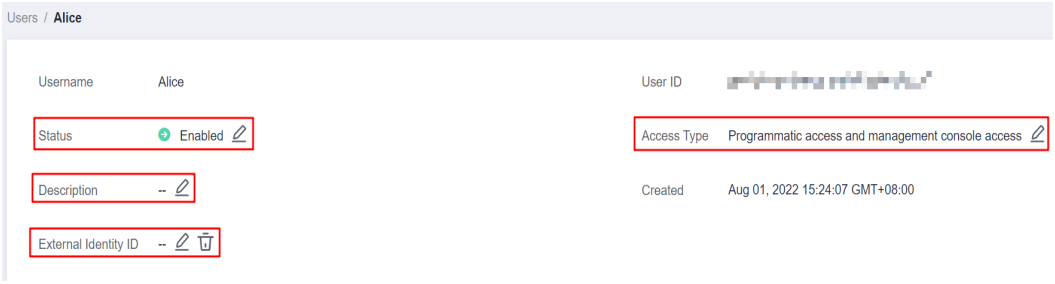
Para ajustar las columnas de elementos que se muestran en la lista, haga clic en  . Las columnas **Username** y **Operation** se muestran de forma predeterminada y la columna **Status** no se puede quitar. También puede seleccionar **Description**, **Last Activity**, **Created**, **Access Type**, **Virtual MFA Status**, **Password Age**, **Access Key (Status, Age, and AK)** y **External Identity ID**.

Si inicia sesión en la consola u obtiene un token más de una vez en un lapso de 5 minutos, la columna **Last Activity** solo muestra su primera hora de inicio de sesión.

Información básica

Puede ver la información básica de cada usuario de IAM. El nombre de usuario, el ID de usuario y la hora de creación no se pueden modificar.

Figura 3-15 Modificación del estado, el tipo de acceso, la descripción y el ID de identidad externo de un usuario de IAM



- **Status**: Los nuevos usuarios de IAM están habilitados de forma predeterminada. Puede establecer el **Status** en **Disabled** para deshabilitar un usuario de IAM. Un usuario deshabilitado ya no puede iniciar sesión en Huawei Cloud a través de la consola de gestión o el acceso programático. Los usuarios de IAM también pueden modificar sus estados.
- **Access Type**: Puede cambiar el tipo de acceso del usuario de IAM.

  NOTA

  - Preste atención a lo siguiente cuando establezca el tipo de acceso de un usuario de IAM:
    - Si el usuario **accede a los servicios en la nube solo mediante la consola de gestión**, especifique el tipo de acceso como **Management console access** y el tipo de credencial como **Password**.
    - Si el usuario **accede a los servicios en la nube solo a través de llamadas programáticas**, especifique el tipo de acceso como **Programmatic access** y el tipo de credencial como **Access key**.
    - Si el usuario **necesita usar una contraseña como credencial para el acceso programático** a ciertas API, especifique el tipo de acceso como **Programmatic access** y el tipo de credencial como **Password**.
    - Si el usuario necesita **realizar la verificación de la clave de acceso** al utilizar determinados servicios en la consola, como crear un trabajo de migración de datos en la consola de Cloud Data Migration (CDM), especifique el tipo de acceso como **Programmatic access** y **Management console access** y el tipo de credencial como **Access Key** y **Password**.
  - Si el tipo de acceso del usuario es **Programmatic access** o tanto **Programmatic access** como **Management console access**, anular la selección de **Management console access** restringirá el acceso del usuario a los servicios en la nube. Tenga cuidado cuando realice esta operación.
- **Description**: Puede modificar la descripción del usuario IAM.
- **External Identity ID**: Identifica a un usuario de empresa en el inicio de sesión federado mediante SSO.

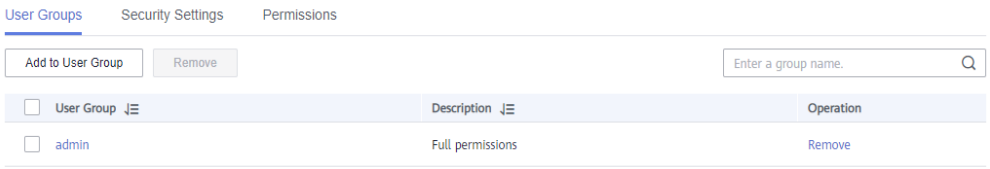
Grupos de usuarios

Un usuario de IAM hereda los permisos de los grupos a los que pertenece el usuario. Puede cambiar los permisos asignados a un usuario de IAM cambiando los grupos a los que pertenece el usuario. Para modificar los permisos de un grupo de usuarios, vea **4.4 Consulta o modificación de la información del grupo de usuarios**.

Su cuenta pertenece al **admin** de grupo predeterminado, que no se puede cambiar.

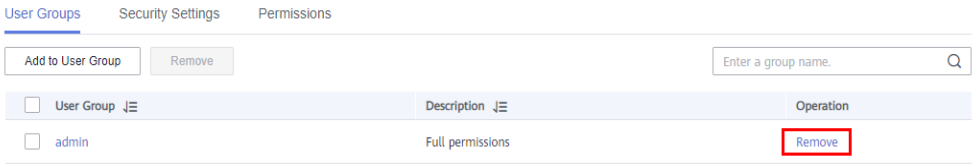
- Haga clic en **Add to User Group** y seleccione uno o más grupos a los que pertenecerá el usuario. A continuación, el usuario hereda los permisos de estos grupos.

Figura 3-16 Agregar el usuario a un grupo de usuarios



- Haga clic en **Remove** a la derecha de un grupo de usuarios y haga clic en **Yes**. El usuario ya no tiene los permisos asignados al grupo.

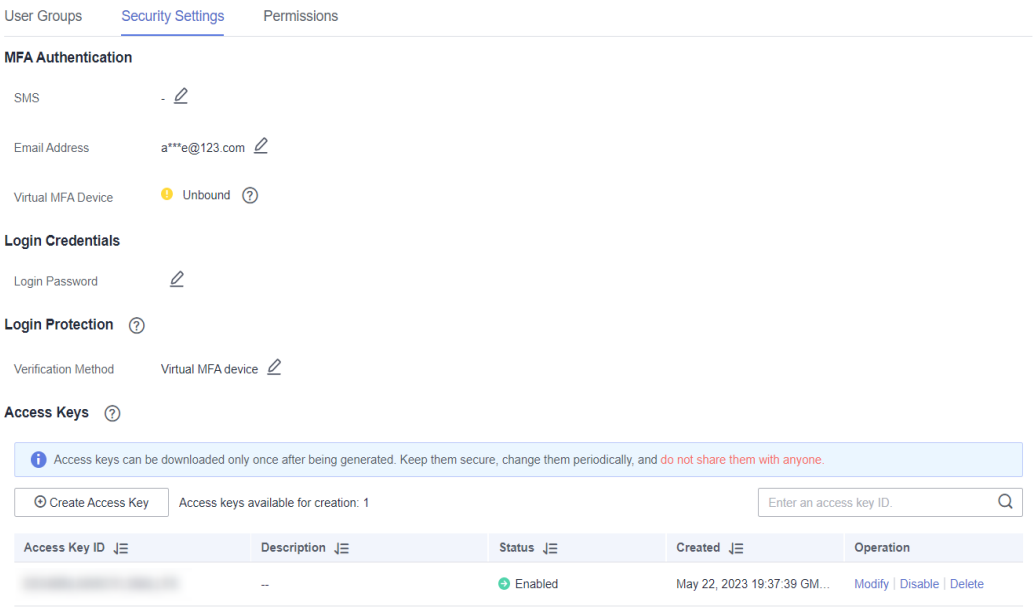
Figura 3-17 Eliminación del usuario de un grupo de usuarios



Configuraciones de seguridad

Como administrador, puede modificar el dispositivo MFA, la credencial de inicio de sesión, la protección de inicio de sesión y las claves de acceso de un usuario de IAM en esta página. Si es usuario de IAM y necesita cambiar su número de teléfono móvil, dirección de correo electrónico o dispositivo MFA virtual, consulte **8.1 Descripción general de configuración de seguridad**.

Figura 3-18 Configuración de seguridad del usuario de IAM



- **MFA Authentication**: puede cambiar la configuración de autenticación multifactor (MFA) de un usuario de IAM en la página **Security Settings**.
  - Cambiar o eliminar el número de teléfono móvil o la dirección de correo electrónico del usuario.

    NOTA

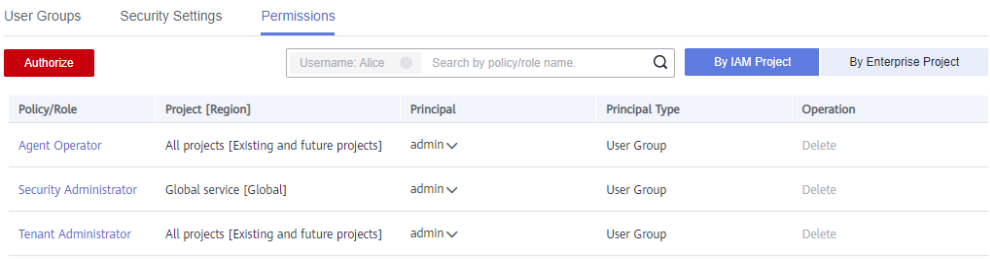
    El número de teléfono móvil y la dirección de correo electrónico del usuario de IAM no pueden ser los mismos que los de su cuenta u otros usuarios de IAM.
  - Quitar el dispositivo MFA virtual del usuario. Para obtener más información acerca de la autenticación MFA y el dispositivo MFA virtual, consulte **11 Autenticación MFA y dispositivo MFA virtual**.
- **Login Credentials**: Puede cambiar la contraseña de inicio de sesión del usuario de IAM. Para obtener más información, consulte **3.6 Cambiar la contraseña de inicio de sesión de un usuario de IAM**. También puede eliminar la contraseña de inicio de sesión del usuario. Esto deshabilitará su acceso a Huawei Cloud. Tenga cuidado al realizar esta operación.
- **Login Protection**: Puede cambiar el método de verificación de inicio de sesión del usuario de IAM. Hay tres métodos de verificación disponibles: dispositivo MFA virtual, SMS y correo electrónico.

  Esta opción está deshabilitada de forma predeterminada. Si habilita esta opción, el usuario tendrá que introducir un código de verificación además del nombre de usuario y la contraseña al iniciar sesión en la consola.
- **Access Keys**: Puede gestionar las claves de acceso del usuario de IAM. Para obtener más información, consulte **3.7 Gestión de claves de acceso para un usuario de IAM**.

Permisos

Puede ver o eliminar los permisos de los usuarios de IAM. Para modificar los permisos de los usuarios de IAM, consulte **Grupos de usuarios**.

Figura 3-19 Permisos asignados a un usuario de IAM



Para ver todos los registros de autorización de su cuenta, consulte **5.5 Registros de autorización**.

NOTA

Al eliminar los permisos de un usuario de IAM se eliminarán los permisos asignados al grupo al que pertenece el usuario. Todos los usuarios del grupo ya no tendrán los permisos. Tenga cuidado cuando realice esta operación.

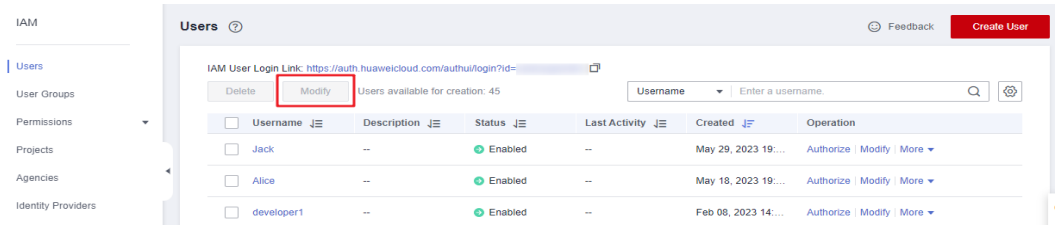
Modificación por lotes de la información del usuario de IAM

IAM le permite modificar por lotes el estado, el tipo de acceso, el método de verificación, la contraseña de inicio de sesión, el número de teléfono móvil y la dirección de correo electrónico de los usuarios de IAM. A continuación se describe cómo modificar por lotes el estado de los usuarios de IAM. Los métodos para modificar otra información sobre los usuarios son similares a este método.

Paso 1 Inicie sesión en la **consola de IAM**. En el panel de navegación, elija **Users**.

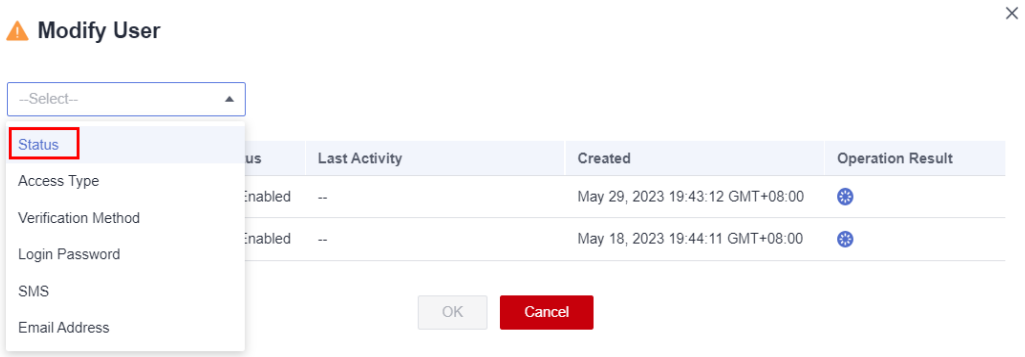
Paso 2 En la lista de usuarios, seleccione los usuarios cuya información desee modificar y haga clic en **Modify** encima de la lista de usuarios.

Figura 3-20 Modificación de la información de usuario



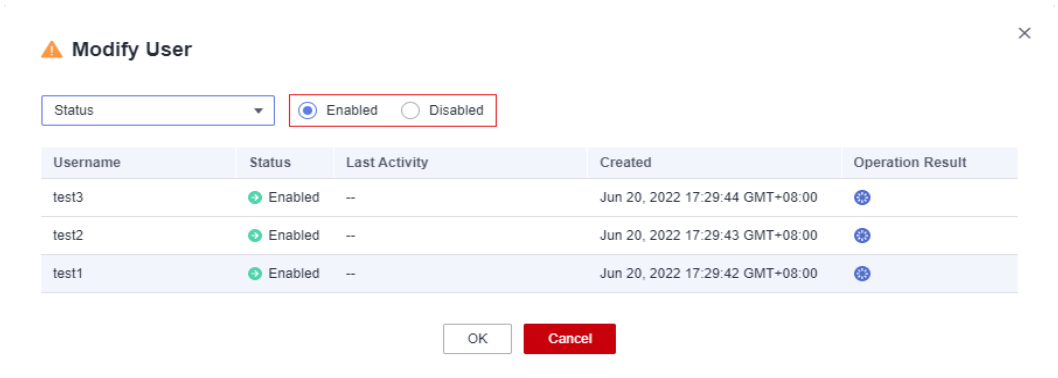
Paso 3 Seleccione el atributo que desea modificar. En este ejemplo, seleccione **Status** en la lista desplegable.

Figura 3-21 Selección del estado de atributo



Paso 4 Seleccione el estado de destino que se va a configurar para los usuarios de IAM seleccionados.

Figura 3-22 Selección del estado de destino



> **NOTA**
>
> Asegúrese de que este usuario ya no está en uso. La desactivación de un usuario activo puede afectar a los servicios.

Paso 5 Haga clic en **OK**.

Paso 6 En el cuadro de diálogo mostrado, haga clic en **OK** para confirmar el cambio.

----Fin

3.5 Eliminación de un usuario de IAM

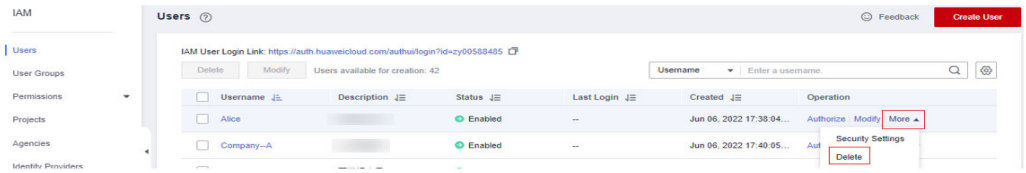
> **ATENCIÓN**
>
> Después de eliminar un usuario de IAM, ya no podrá iniciar sesión y su nombre de usuario, contraseña, claves de acceso y autorizaciones se borrarán y no se podrán recuperar.
>
> - Asegúrese de que los usuarios que se van a eliminar ya no son necesarios. Si no está seguro, desactívelos en lugar de eliminarlos para que se puedan activar si se producen errores en el servicio. Para deshabilitar un usuario de IAM individual, consulte **Información básica**. Para deshabilitar varios usuarios de IAM a la vez, consulte **Modificación por lotes de la información del usuario de IAM**.
> - Para quitar un usuario de IAM de un grupo de usuarios, consulte **4.2 Agregar o quitar usuarios de un grupo de usuarios**.
> - Los usuarios de IAM pueden eliminarse a sí mismos.

Eliminación de un usuario de IAM

Paso 1 Inicie sesión en la **consola de IAM**. En el panel de navegación, elija **Users**.

Paso 2 Elija **More** > **Delete** en la fila que contiene el usuario de IAM que desea eliminar y haga clic en **Yes**.

Figura 3-23 Eliminación de un usuario de IAM



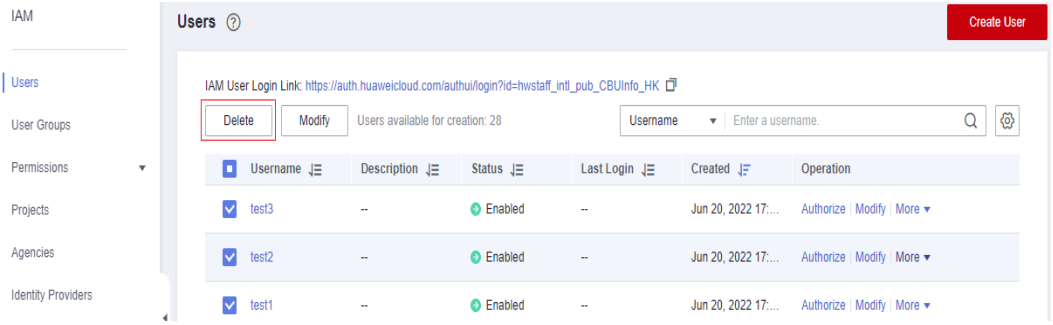
----Fin

Eliminación por lotes de usuarios de IAM

Paso 1 Inicie sesión en la **consola de IAM**. En el panel de navegación, elija **Users**.

Paso 2 En la lista de usuarios, seleccione los usuarios que desea eliminar y haga clic en **Delete** encima de la lista de usuarios.

Figura 3-24 Eliminación por lotes de usuarios de IAM



Paso 3 En el cuadro de diálogo que se muestra, haga clic en **Yes**.

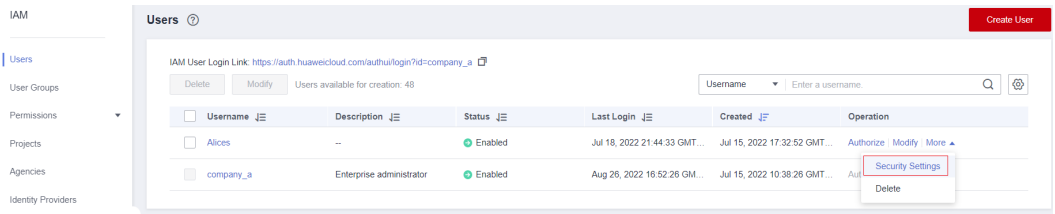
----Fin

3.6 Cambiar la contraseña de inicio de sesión de un usuario de IAM

Como administrador, puede restablecer la contraseña de un usuario de IAM si el usuario ha olvidado la contraseña y no se ha vinculado al usuario ninguna dirección de correo electrónico o número de teléfono móvil.

Para restablecer la contraseña de inicio de sesión de un usuario de IAM, haga clic en **Security Settings** en la fila que contiene al usuario, haga clic en junto a **Login Password** en el área **Login Credentials** y seleccione un tipo de contraseña.

Figura 3-25 Cambiar la contraseña de un usuario de IAM



NOTA

- Puede restablecer la contraseña de un usuario de IAM en la página **Security Settings**.
- La contraseña del usuario de IAM generada automáticamente para su cuenta no se puede cambiar en la pestaña **Security Settings**. Para cambiar la contraseña, vaya a la página **Basic Information** de My Account.
- Los usuarios de IAM pueden cambiar sus contraseñas en la pestaña **Información básica**. Si desea cambiar la contraseña de su cuenta, consulte **¿Cómo cambio mi contraseña?**

- **Set by user**: Una URL de inicio de sesión única será enviada por correo electrónico al usuario. El usuario puede hacer clic en el enlace para configurar una contraseña.
- **Automatically generated**: Una contraseña se generará automáticamente y luego se enviará al usuario por correo electrónico.
- **Set now**: Usted establece una nueva contraseña y envía la nueva contraseña al usuario.

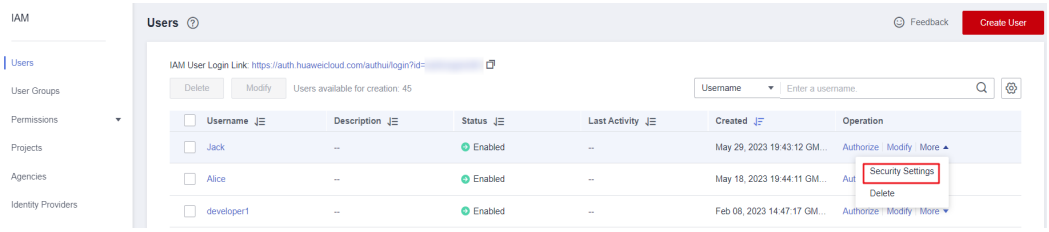
3.7 Gestión de claves de acceso para un usuario de IAM

Una clave de acceso consiste en un par ID de clave de acceso (AK) y clave de acceso secreta (SK). Puede usar una clave de acceso para acceder a Huawei Cloud mediante herramientas de desarrollo, incluidas API, CLI y SDK. Las claves de acceso no se pueden utilizar para iniciar sesión en la consola. AK es un identificador único utilizado junto con SK para firmar solicitudes criptográficamente, asegurando que las solicitudes sean secretas, completas y correctas.

Como administrador, puede gestionar las claves de acceso para los usuarios de IAM que han olvidado sus claves de acceso y no tienen acceso a la consola.

Elija **More** > **Security Settings** en la fila que contiene el usuario de IAM y, a continuación, cree o elimine las claves de acceso en el área **Access Keys**.

Figura 3-26 Gestión de claves de acceso para un usuario de IAM



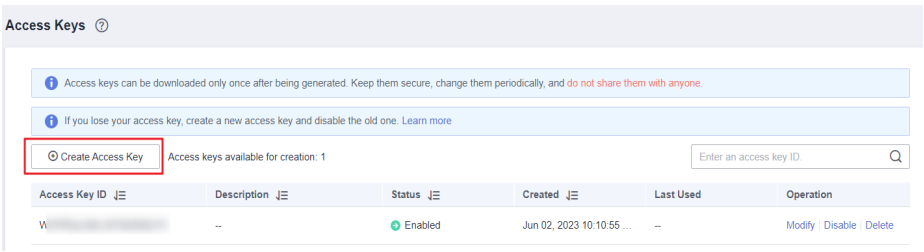
NOTA

- Los usuarios federados solo pueden crear credenciales de acceso temporales (AK/SK temporales y securityTokens). Para obtener más información, consulte **Clave de acceso temporal (para usuarios federados)**.
- Si un usuario está autorizado a usar la consola, el usuario puede **gestionar claves de acceso** en la página **My Credentials**.
- Las claves de acceso son credenciales de identidad que se usan para invocar a las API. El administrador de la cuenta y los usuarios de IAM solo pueden usar sus propias claves de acceso para invocar a las API.
- Si se utiliza una clave de acceso más de una vez en un lapso de 15 minutos, la columna **Last Used** del área **Access Keys** solo muestra el primer tiempo de uso.

- Creación de una clave de acceso

  a. Haga clic en **Create Access Key**.

  Figura 3-27 Creación de una clave de acceso

> **NOTA**
>
> Cada usuario tiene un máximo de dos claves de acceso, y las claves de acceso son válidas permanentemente. Por motivos de seguridad, cambie las claves de acceso de los usuarios de IAM periódicamente.

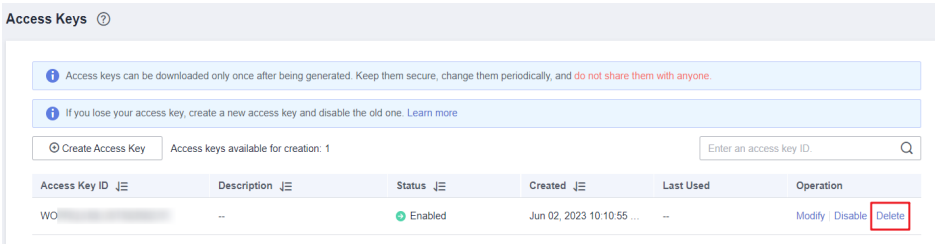
b. (Opcional) Si la protección de operación está activada, debe introducir un código de verificación o una contraseña.

c. Haga clic en **OK**. Se genera automáticamente una clave de acceso. Descargue la clave de acceso y proporciónela al usuario.

- Eliminación de una clave de acceso

a. En la lista de claves de acceso, haga clic en **Delete** en la fila que contiene la clave de acceso que se eliminará.

Figura 3-28 Eliminación de una clave de acceso



b. (Opcional) Si la protección de operación está activada, debe introducir un código de verificación o una contraseña.

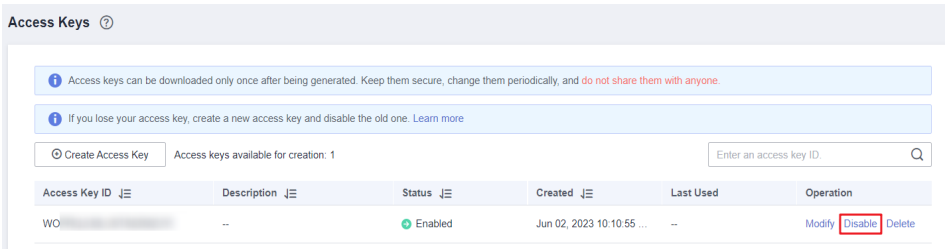
c. Haga clic en **Yes**.

- Activación/desactivación de una clave de acceso

  Las nuevas claves de acceso están habilitadas de forma predeterminada. Para desactivar una clave de acceso, realice los siguientes pasos:

a. En la lista de claves de acceso, haga clic en **Disable** en la fila que contiene la clave de acceso que desea deshabilitar.

Figura 3-29 Desactivación de una clave de acceso



b. (Opcional) Si la protección de operación está activada, debe introducir un código de verificación o una contraseña y hacer clic en **Yes**.

El método de habilitar una clave de acceso es similar al de deshabilitar una clave de acceso.

4 Grupos de usuarios y autorización

4.1 Creación de un grupo de usuarios y asignación de permisos

Como administrador, puede crear grupos de usuarios y concederles permisos adjuntando políticas o roles. Los usuarios que agregue a los grupos de usuarios heredan permisos de las políticas o roles. Los usuarios de IAM pueden asignarse permisos a sí mismos. IAM proporciona permisos generales (como permisos de administrador o de solo lectura) para cada servicio en la nube, que puede asignar a grupos de usuarios. Los usuarios de los grupos pueden utilizar los servicios en la nube basados en los permisos asignados. Para obtener más información, véase **3.2 Asignación de permisos a un usuario de IAM**. **Para obtener más información sobre permisos definidos por sistema de todos los servicios en la nube, consulte Permisos definidos por sistema**.

Prerrequisitos

Antes de crear un grupo de usuarios, obtenga información sobre lo siguiente:

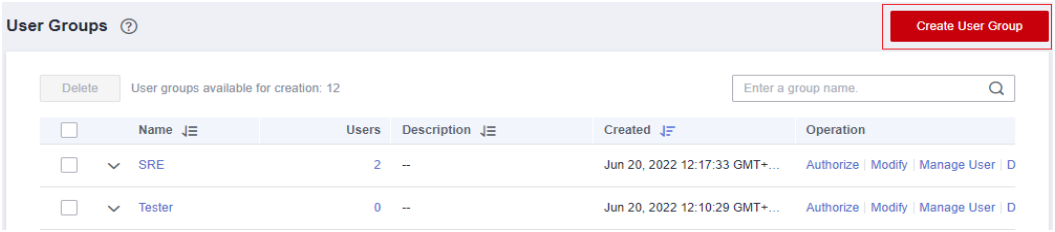
- Comprenda los **conceptos básicos** de permisos.
- Conozca **permisos definidos por el sistema** proporcionados por IAM.

Crear un grupo de usuarios

Paso 1 Inicie sesión en la **consola de IAM** como el administrador.

Paso 2 En la consola de IAM, elija **User Groups** en el panel de navegación y haga clic en **Create User Group** en la esquina superior derecha.

Figura 4-1 Creación de un grupo de usuarios



Paso 3 En la página mostrada, escriba un nombre de grupo de usuarios.

Paso 4 Haga clic en **OK**.

NOTA

Puede crear un máximo de 20 grupos de usuarios. Para crear más grupos de usuarios, aumente la cuota haciendo referencia a **¿Cómo puedo aumentar mi cuota?**

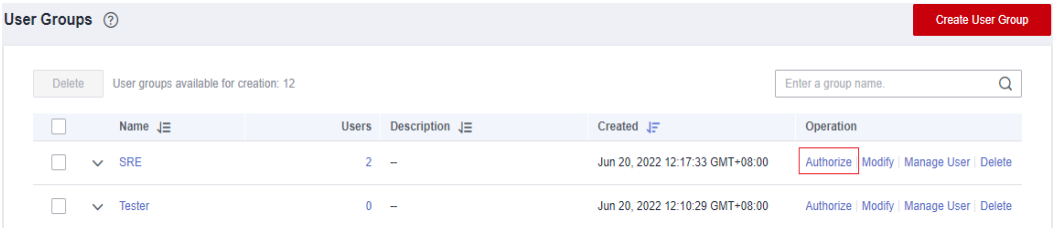
----Fin

Asignación de permisos a un grupo de usuarios

Para asignar permisos a un grupo de usuarios, haga lo siguiente. Para revocar los permisos de un grupo de usuarios, vea **4.5 Revocación de permisos de un grupo de usuarios**.

Paso 1 En la lista de grupos de usuarios, haga clic en **Authorize** en la fila que contiene el grupo de usuarios creado.

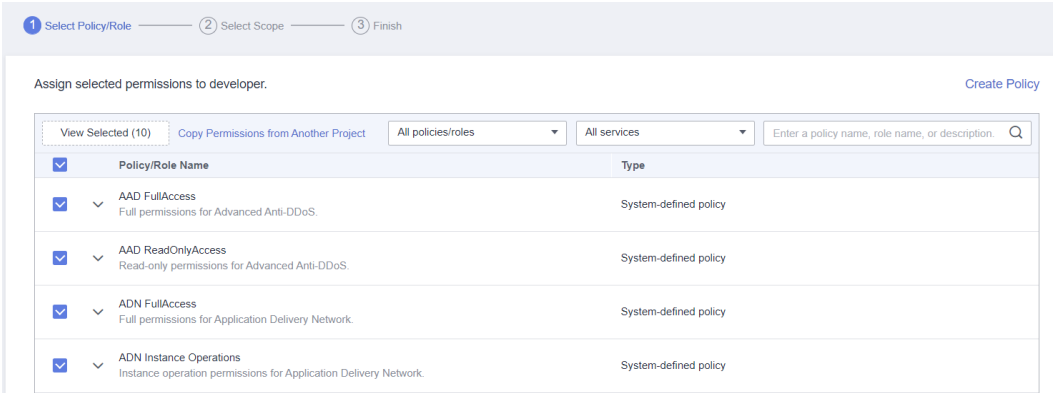
Figura 4-2 Ir a la página de autorización de grupo de usuarios



Paso 2 En la página **Authorize User Group**, seleccione los permisos que se asignarán al grupo de usuarios y haga clic en **Next**.

Si las políticas definidas por el sistema no cumplen sus requisitos, haga clic en **Create Policy** en la parte superior derecha para crear políticas personalizadas. Puede usarlos para complementar las políticas definidas por el sistema para un control de permisos refinado. Para obtener más información, véase **5.6.1 Creación de una política personalizada**.

Figura 4-3 Selección de permisos



Paso 3 Especifique el ámbito. El sistema recomienda automáticamente un ámbito de autorización para los permisos seleccionados. **Tabla 4-1** describe todos los ámbitos de autorización proporcionados por IAM.

Tabla 4-1 Ámbitos de autorización

Ámbito	Descripción
Todos los recursos	Los usuarios de IAM pueden usar los recursos de todos los proyectos específicos de la región y los servicios globales de su cuenta en función de los permisos asignados.
Proyectos empresariales	Los usuarios de IAM pueden utilizar los recursos de los proyectos de empresa seleccionados en función de los permisos asignados. Esta opción solo está disponible cuando Enterprise Project está habilitado. Para obtener más información sobre proyectos empresariales, consulte **Qué es Enterprise Project Management Service**. Para habilitar el proyecto empresarial, consulte **Habilitación de la función de Enterprise Project**.
Proyectos de regiones específicas	Los usuarios de IAM pueden utilizar los recursos de los proyectos específicos de la región que seleccione en función de los permisos asignados. Si ha seleccionado permisos de servicio global y ha especificado el ámbito como **Region-specific projects**, los permisos de servicio global se aplicarán a todos los recursos de forma predeterminada. Los permisos seleccionados para los servicios de nivel de proyecto se aplicarán a los proyectos específicos de la región que seleccione.
Servicios globales	Los usuarios de IAM pueden utilizar servicios globales basados en los permisos asignados. Los servicios globales se despliegan sin especificar regiones físicas. Los usuarios de IAM no necesitan especificar una región al acceder a estos servicios, como Object Storage Service (OBS) y Content Delivery Network (CDN). Si ha seleccionado permisos de servicio de nivel de proyecto y ha especificado el ámbito como **Global services**, los permisos de servicio de nivel de proyecto se aplicarán a todos los recursos de forma predeterminada. Los permisos seleccionados para los servicios globales se seguirán aplicando a los servicios globales que seleccione.

Paso 4 Haga clic en **OK**.

----Fin

Tabla 4-2 enumera los permisos comunes. Para obtener la lista completa de permisos específicos del servicio, vea **Permisos definidos por sistema**.

NOTA

- Si agrega un usuario a varios grupos, el usuario heredará todos los permisos asignados a estos grupos.
- Para obtener más información acerca de la gestión de permisos, consulte **Asignación de permisos al personal de O&M**, **4.6 Asignación de roles de dependencia** y **5.6.3 Casos de uso de políticas personalizadas**.

Tabla 4-2 Permisos comunes

Categoría	Nombre de política/rol	Descripción	Alcance de la autorización
Gestión general	FullAccess	Permisos completos para los servicios que admiten el control de acceso basado en políticas.	Todos
Gestión de recursos	Tenant Administrator	Permisos de administrador para todos los servicios excepto IAM.	Todos
Consulta de recursos	Tenant Guest	Permisos de solo lectura para todos los recursos.	Todos
Gestión de usuarios de IAM	Administrador de seguridad	Permisos de administrador para IAM.	Servicios globales
Gestión de contabilidad	Administrador de BSS	Permisos de administrador para el Centro de facturación, incluida la gestión de facturas, pedidos, contratos y renovaciones, y la visualización de facturas. **NOTA** Esta función depende del rol de **BSS Administrator** para que surta efecto.	Proyectos de regiones específicas
Cómputo O&M	ECS FullAccess	Permisos de administrador para ECS.	Proyectos de regiones específicas
	CCE FullAccess	Permisos de administrador para Cloud Container Engine (CCE).	Proyectos de regiones específicas

Categoría	Nombre de política/rol	Descripción	Alcance de la autorización
	CCI FullAccess	Permisos de administrador para la instancia de contenedor de nube (CCI).	Proyectos de regiones específicas
	BMS FullAccess	Permisos de administrador para Bare Metal Server (BMS).	Proyectos de regiones específicas
	IMS FullAccess	Permisos de administrador para Image Management Service (IMS).	Proyectos de regiones específicas
	AutoScaling FullAccess	Permisos de administrador para Auto Scaling (AS).	Proyectos de regiones específicas
Red O&M	VPC FullAccess	Permisos de administrador para Virtual Private Cloud (VPC).	Proyectos de regiones específicas
	ELB FullAccess	Permisos de administrador para Elastic Load Balance (ELB).	Proyectos de regiones específicas
O&M de base de datos	RDS FullAccess	Permisos de administrador para Relational Database Service (RDS).	Proyectos de regiones específicas
	DDS FullAccess	Permisos de administrador para Document Database Service (DDS).	Proyectos de regiones específicas
	DDM FullAccess	Permisos de administrador para Distributed Database Middleware (DDM).	Proyectos de regiones específicas
Seguridad O&M	Anti-DDoS Administrator	Permisos de administrador para Anti-DDoS.	Proyectos de regiones específicas
	AAD Administrator	Permisos de administrador para Advanced Anti-DDoS (AAD).	Proyectos de regiones específicas
	WAF Administrator	Permisos de administrador para Web Application Firewall (WAF).	Proyectos de regiones específicas
	VSS Administrator	Permisos de administrador para Vulnerability Scan Service (VSS).	Proyectos de regiones específicas
	CGS Administrator	Permisos de administrador para Container Guard Service (CGS).	Proyectos de regiones específicas

Categoría	Nombre de política/rol	Descripción	Alcance de la autorización
	KMS Administrator	Permisos de administrador para Key Management Service (KMS), que se ha renombrado como Data Encryption Workshop (DEW).	Proyectos de regiones específicas
	DBSS System Administrator	Permisos de administrador para Database Security Service (DBSS).	Proyectos de regiones específicas
	SES Administrator	Permisos de administrador para Security Expert Service (SES).	Proyectos de regiones específicas
	SC Administrator	Permisos de administrador para SSL Certificate Manager (SCM).	Proyectos de regiones específicas

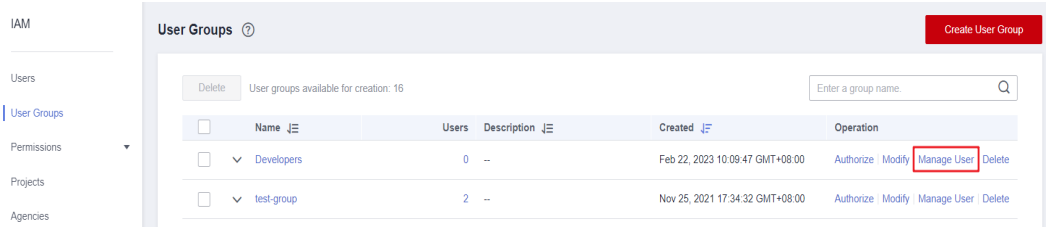
4.2 Agregar o quitar usuarios de un grupo de usuarios

Un usuario hereda los permisos de los grupos a los que pertenece el usuario. Para cambiar los permisos de un usuario, agregue el usuario a un nuevo grupo o quite el usuario de un grupo existente.

Adición de usuarios a un grupo de usuarios

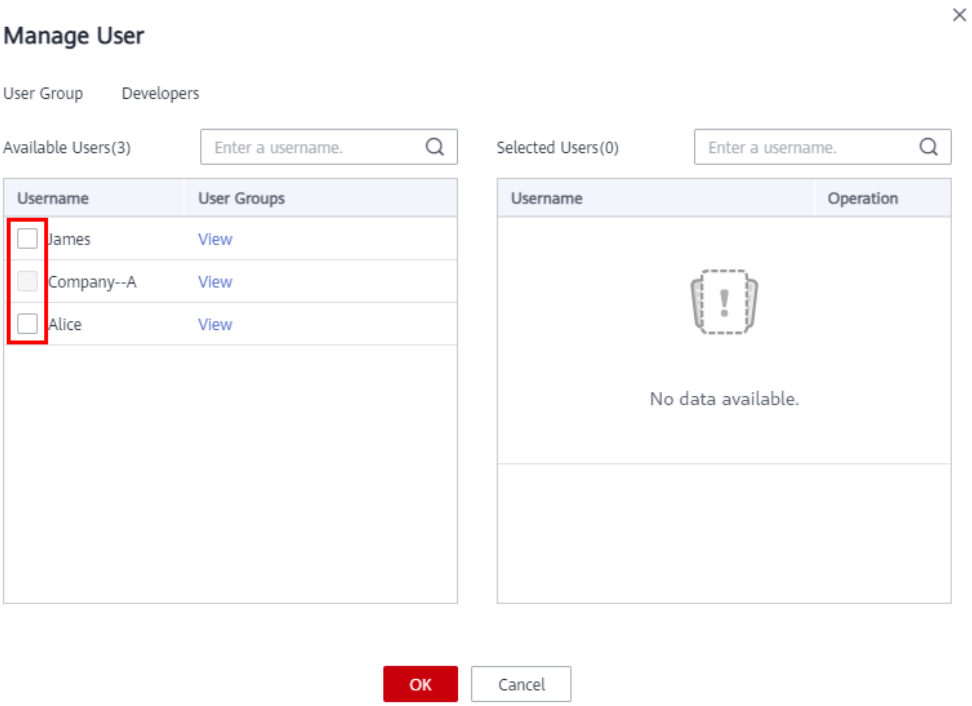
Paso 1 En la lista de grupos de usuarios, haga clic en **Manage User** en la fila que contiene el grupo de usuarios de destino.

Figura 4-4 Gestión de usuarios



Paso 2 En el cuadro de diálogo **Manage User**, seleccione los nombres de usuario que desea agregar.

Figura 4-5 Selección de usuarios



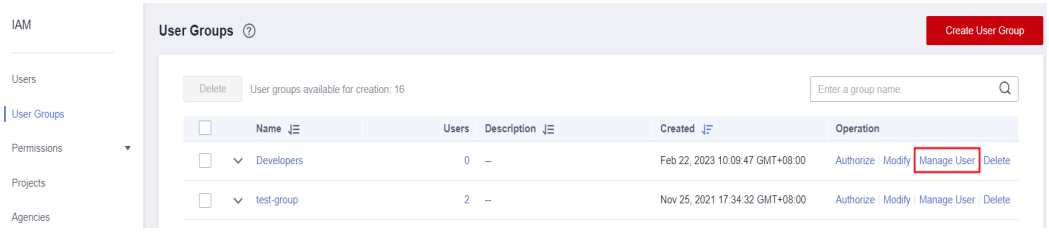
Paso 3 Haga clic en **OK**.

----Fin

Eliminación de usuarios de un grupo de usuarios

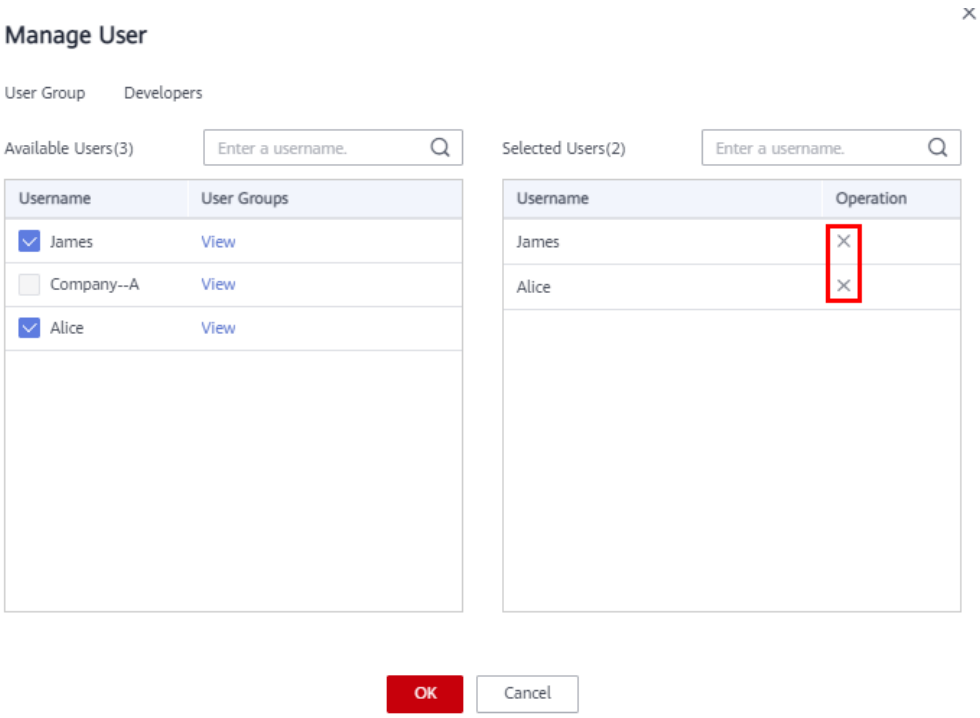
Paso 1 En la lista de grupos de usuarios, haga clic en **Manage User** en la fila que contiene el grupo de usuarios de destino.

Figura 4-6 Gestión de usuarios



Paso 2 En el área **Selected Users**, localice el usuario que desea eliminar y haga clic en el botón ×. A continuación, haga clic en **OK**.

Figura 4-7 Eliminación de usuarios de un grupo de usuarios



----Fin

4.3 Eliminación de un grupo de usuarios

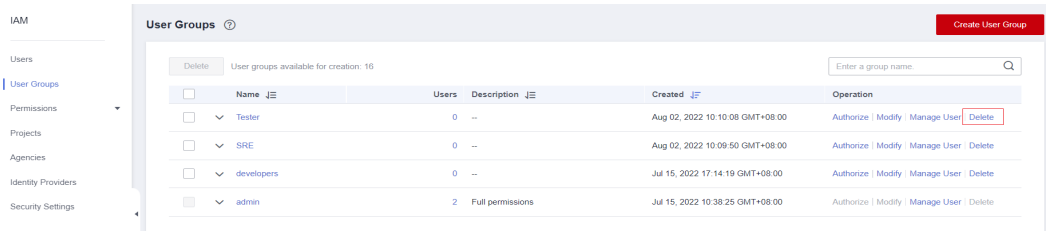
Procedimiento

Para eliminar un grupo de usuarios, haga lo siguiente:

Paso 1 Inicie sesión en la **consola de IAM**. En el panel de navegación, elija **User Groups**.

Paso 2 En la lista de grupos de usuarios, haga clic en **Delete** en la fila que contiene el grupo de usuarios que se va a eliminar.

Figura 4-8 Eliminación de un grupo de usuarios



Paso 3 En el cuadro de diálogo que se muestra, haga clic en **Yes**.

----Fin

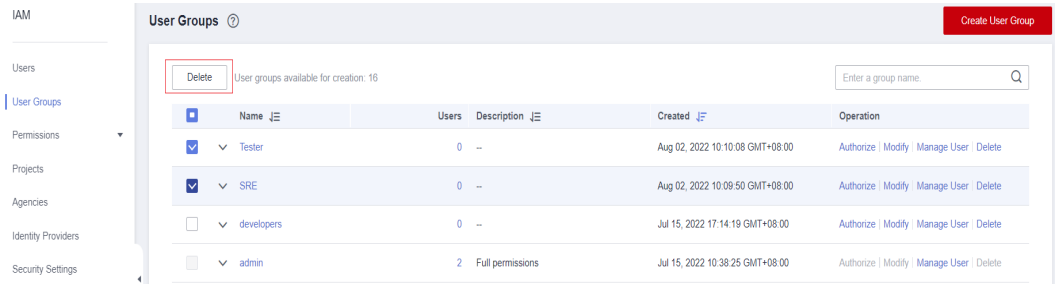
Eliminación de grupos de usuarios por lotes

Para eliminar varios grupos de usuarios a la vez, haga lo siguiente:

Paso 1 Inicie sesión en la **consola de IAM**. En el panel de navegación, elija **User Groups**.

Paso 2 En la lista de grupos de usuarios, seleccione los grupos de usuarios que desea eliminar y haga clic en **Delete** encima de la lista.

Figura 4-9 Eliminación de grupos de usuarios por lotes



Paso 3 En el cuadro de diálogo que se muestra, haga clic en **Yes**.

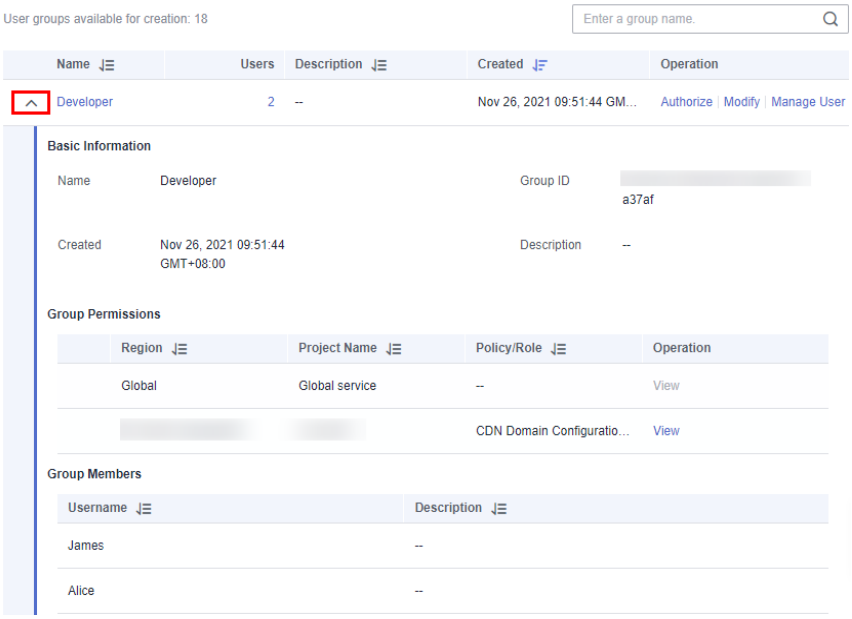
----Fin

4.4 Consulta o modificación de la información del grupo de usuarios

Consulta de la información del grupo de usuarios

En la lista de grupos de usuarios, haga clic en junto a un grupo de usuarios para ver su información básica, los permisos asignados y los usuarios gestionados.

Figura 4-10 Consulta de la información del grupo de usuarios



Modificación de permisos de grupo de usuarios

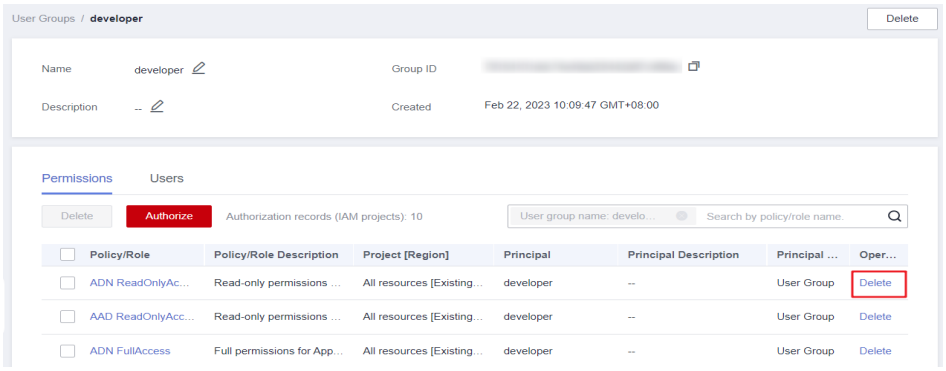
Ver o modificar permisos de grupo de usuarios.

NOTA

- La modificación de los permisos de un grupo de usuarios afecta a los permisos de todos los usuarios del grupo de usuarios. Tenga cuidado cuando realice esta operación.
- No se pueden modificar los permisos del **admin** de grupo de usuarios predeterminado.

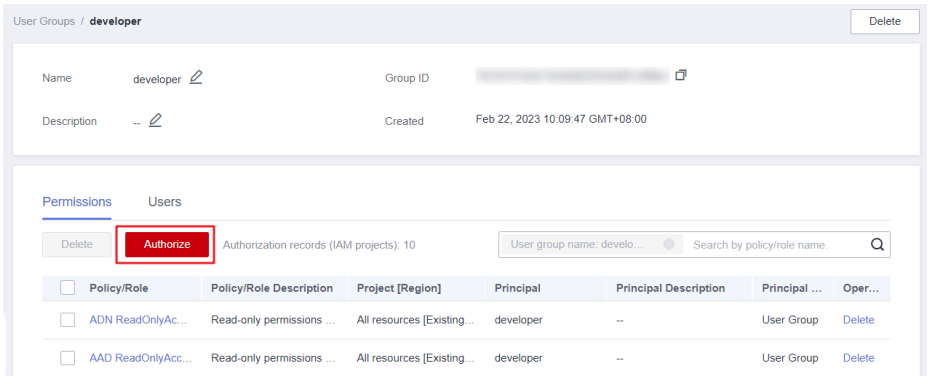
1. Haga clic en el nombre de un grupo de usuarios (por ejemplo, **Developers**) para ir a la página de detalles y ver los permisos de grupo en la pestaña **Permissions**.
2. Haga clic en **Delete** en la fila que contiene el rol o la política que desea eliminar.

Figura 4-11 Eliminación de un permiso asignado



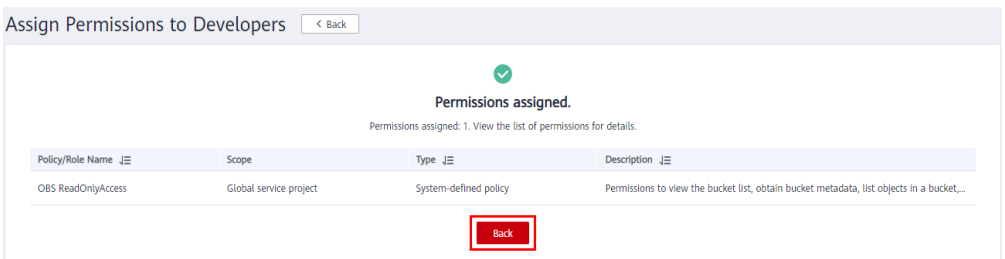
3. Haga clic en **Yes**.
4. En la pestaña **Permissions**, haga clic en **Authorize**.

Figura 4-12 Asignación de permisos a un grupo de usuarios



5. Seleccione los permisos y un ámbito deseados y haga clic en **OK**.
6. Vuelva a la pestaña **Permissions** para ver los permisos de grupo modificados.

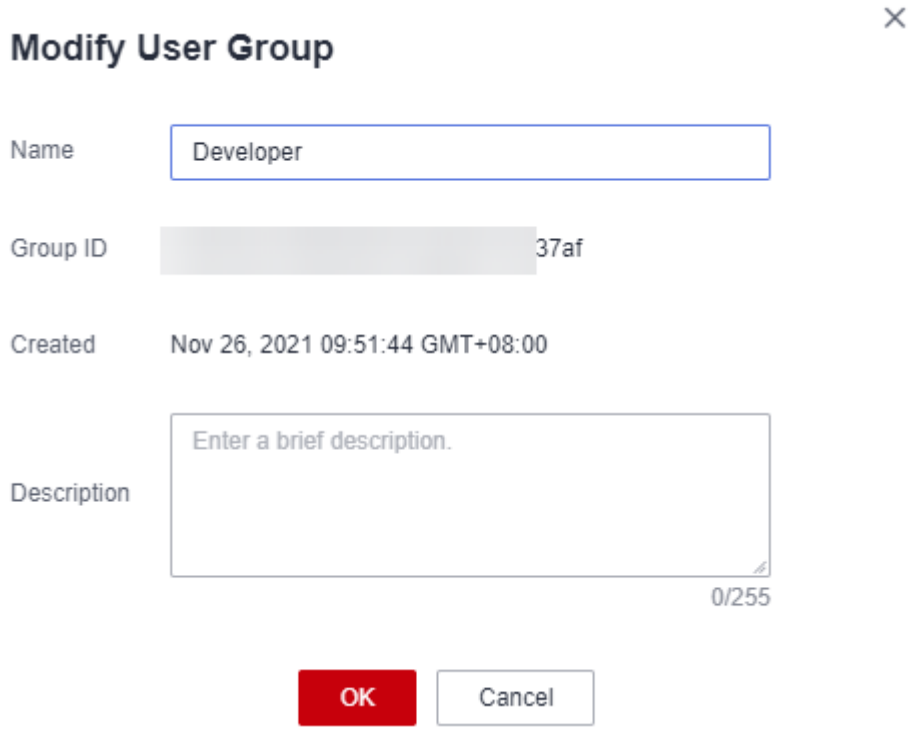
Figura 4-13 Volver a la pestaña Permissions



Modificación del nombre y la descripción de un grupo de usuarios

En la lista de grupos de usuarios, haga clic en **Modify** en la fila que contiene el grupo de usuarios cuyo nombre y descripción desea modificar, y modifique el nombre y la descripción.

Figura 4-14 Modificación del nombre y la descripción del grupo de usuarios



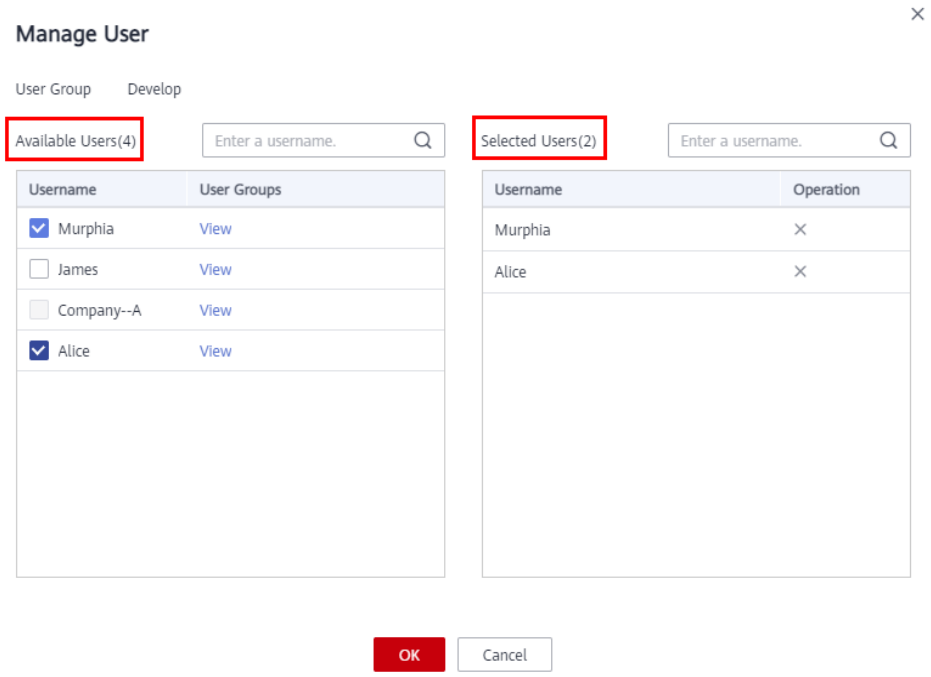
NOTA

Si se ha configurado un nombre de grupo de usuarios en las reglas de conversión de identidad de un proveedor de identidad, al modificar el nombre de grupo de usuarios se producirá un error en las reglas de conversión de identidad. Tenga cuidado cuando realice esta operación.

Gestión de usuarios

Paso 1 En la lista de grupos de usuarios, haga clic en **Manage User** en la fila que contiene el grupo de usuarios que desea modificar.

Figura 4-15 Gestión de usuarios en el grupo



Paso 2 En el área **Available Users**, seleccione los usuarios que desea agregar al grupo de usuarios.

Paso 3 En el área **Selected Users**, quite usuarios del grupo de usuarios.

----Fin

NOTA

Para el **admin** de grupo predeterminado, solo puede gestionar a sus usuarios y no puede modificar su descripción o permisos.

4.5 Revocación de permisos de un grupo de usuarios

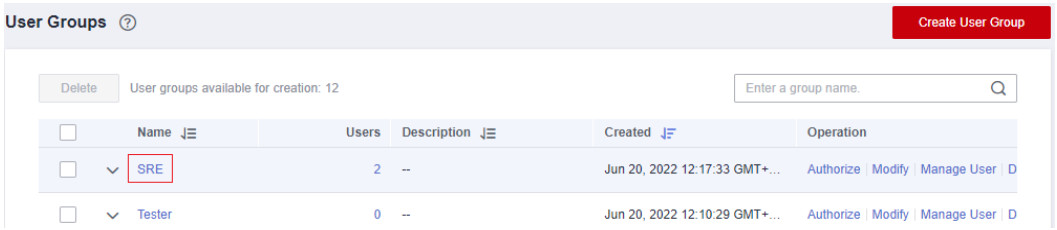
Procedimiento

Para revocar una política o un rol asociado a un grupo de usuarios, haga lo siguiente:

Paso 1 Inicie sesión en la **consola de IAM**. En el panel de navegación, elija **User Groups**.

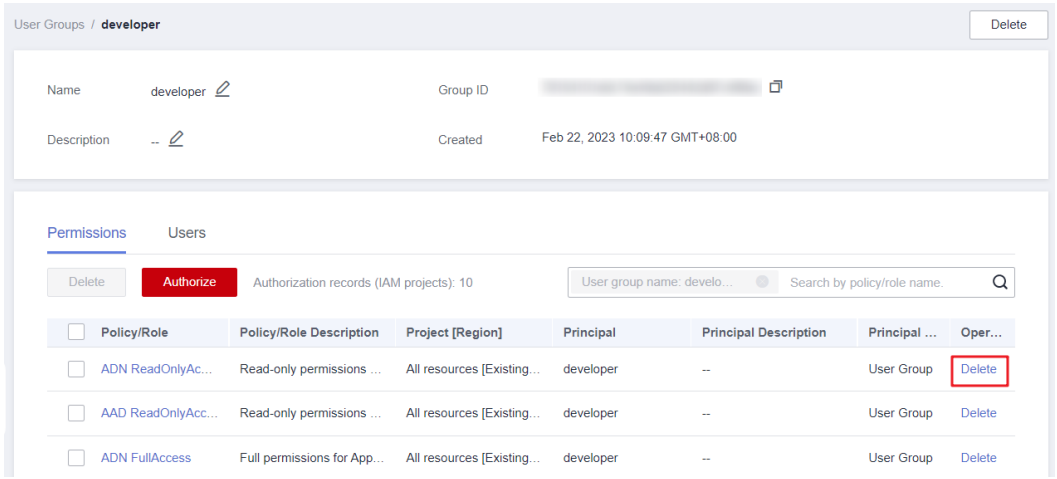
Paso 2 Haga clic en el nombre del grupo de usuarios para ir a la página de detalles del grupo.

Figura 4-16 Hacer clic en un nombre de grupo de usuarios



Paso 3 En la pestaña **Permissions**, haga clic en **Delete** en la fila que contiene el rol o la política que desea eliminar.

Figura 4-17 Revocación de permisos



Paso 4 En el cuadro de diálogo que se muestra, haga clic en **Yes**.

----Fin

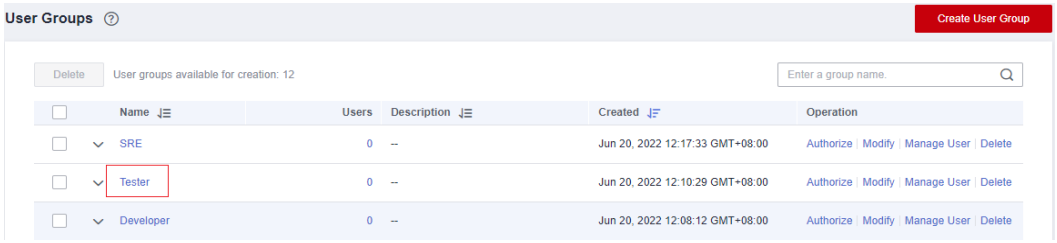
Revocación por lotes de permisos de un grupo de usuarios

Para revocar varias directivas o roles asociados a un grupo de usuarios, haga lo siguiente:

Paso 1 Inicie sesión en la **consola de IAM**. En el panel de navegación, elija **User Groups**.

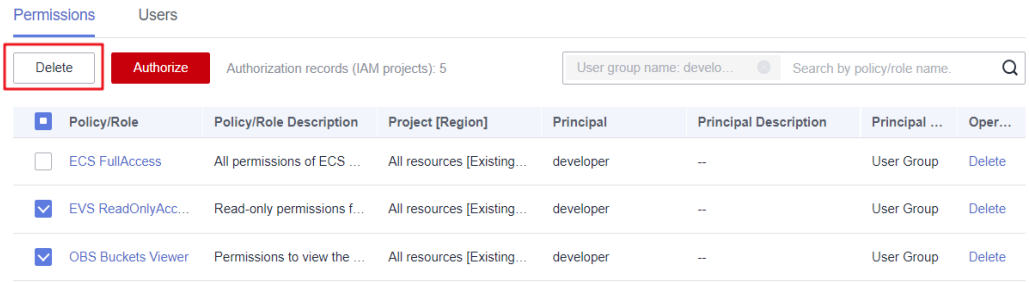
Paso 2 Haga clic en el nombre del grupo de usuarios para ir a la página de detalles del grupo.

Figura 4-18 Consulta de un grupo de usuarios



Paso 3 En la página **Permissions**, seleccione los roles o políticas que desea eliminar y haga clic en **Delete** encima de la lista.

Figura 4-19 Permisos de revocación por lotes



Paso 4 En el cuadro de diálogo que se muestra, haga clic en **Yes**.

----Fin

4.6 Asignación de roles de dependencia

Los servicios de Huawei Cloud interactúan entre sí. Los roles de algunos servicios solo tienen efecto si se asignan junto con los roles de otros servicios.

Procedimiento

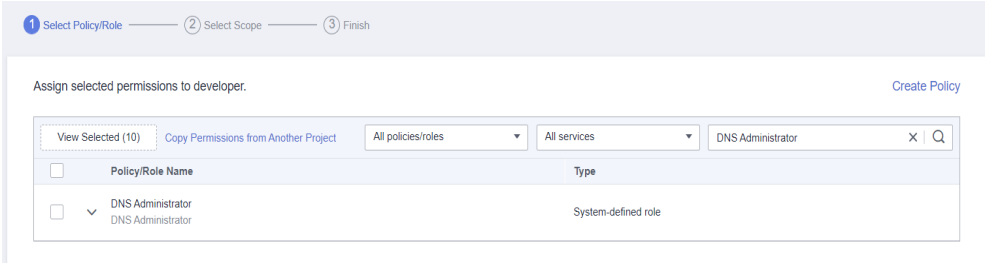
Paso 1 Inicie sesión en la **consola de IAM** como administrador.

Paso 2 En la lista de grupos de usuarios, haga clic en **Authorize** en la fila que contiene el grupo de usuarios creado.

Paso 3 En la página mostrada, busque un rol en el cuadro de búsqueda en la esquina superior derecha.

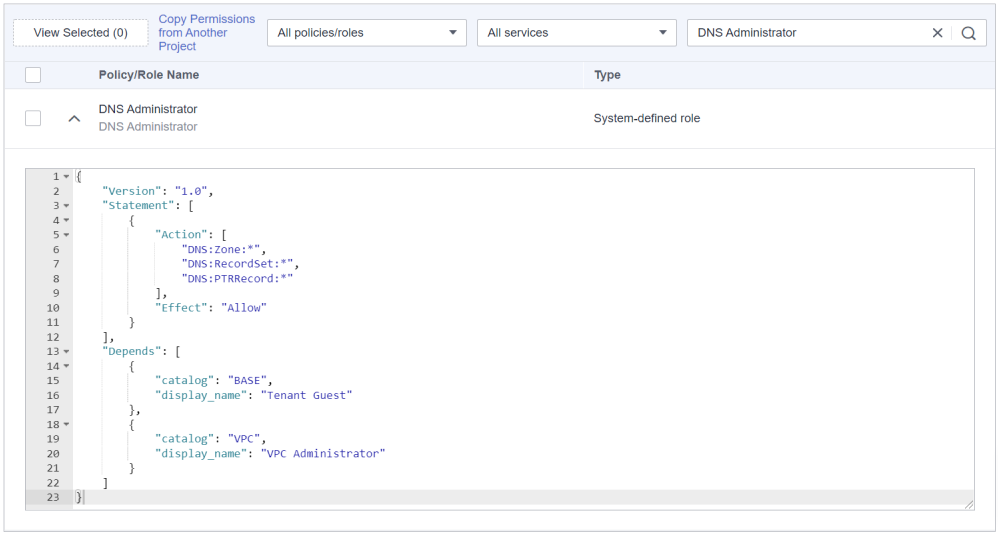
Paso 4 Seleccione el rol de destino. El sistema selecciona automáticamente los roles de dependencia.

Figura 4-20 Selección de un rol



Paso 5 Haga clic en junto al rol para ver las dependencias.

Figura 4-21 Consulta de dependencias



Por ejemplo, el rol **DNS Administrator** contiene el parámetro **Depends** que especifica los roles de dependencia. Cuando asigna la función **DNS Administrator** a un grupo de usuarios, también debe asignar las funciones **Tenant Guest** y **VPC Administrator** al grupo para el mismo proyecto.

Paso 6 Haga clic en **OK**.

----Fin

5 Gestión de permisos

5.1 Conceptos básicos

Permiso

De forma predeterminada, los usuarios de IAM no tienen permisos. Para asignar permisos a los usuarios de IAM, agréguelos a uno o más grupos y adjunte políticas o roles a estos grupos. A continuación, los usuarios heredan permisos de los grupos a los que pertenecen los usuarios y pueden realizar operaciones específicas en servicios en la nube.

Tipo de permiso

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: un tipo de mecanismo de autorización de grano grueso que define permisos de nivel de servicio en función de las responsabilidades del usuario. IAM proporciona un número limitado de roles para la gestión de permisos. Al usar roles para conceder permisos, también debe asignar roles de dependencia. Los roles no son una opción ideal para la autorización detallada y el control de acceso seguro.
- Políticas: Un tipo de mecanismo de autorización detallado que define los permisos necesarios para realizar operaciones en recursos de nube específicos bajo ciertas condiciones. Este mecanismo permite una autorización basada en políticas más flexible y un control de acceso seguro. Por ejemplo, puede conceder a los usuarios de ECS solo los permisos necesarios para gestionar un determinado tipo de recursos de ECS.

  IAM admite tanto **políticas definidas por el sistema** como **políticas personalizadas**.

Política definida por el sistema

Una política definida por el sistema define las acciones comunes de un servicio en la nube. Las políticas definidas por el sistema se pueden utilizar para asignar permisos a grupos de usuarios y no se pueden modificar. **Para obtener más información sobre las políticas definidas por el sistema de todos los servicios en la nube, consulte**Permisos del sistema.

Si no hay políticas definidas por el sistema para un servicio específico, indica que IAM no admite este servicio. Puede **enviar un ticket de servicio** y solicitar la gestión de permisos en IAM.

Política personalizada

Puede crear políticas personalizadas mediante las acciones admitidas por los servicios en la nube para complementar las políticas definidas por el sistema y lograr un control de acceso más refinado. Puede crear políticas personalizadas en el editor visual o en la vista JSON.

5.2 Roles

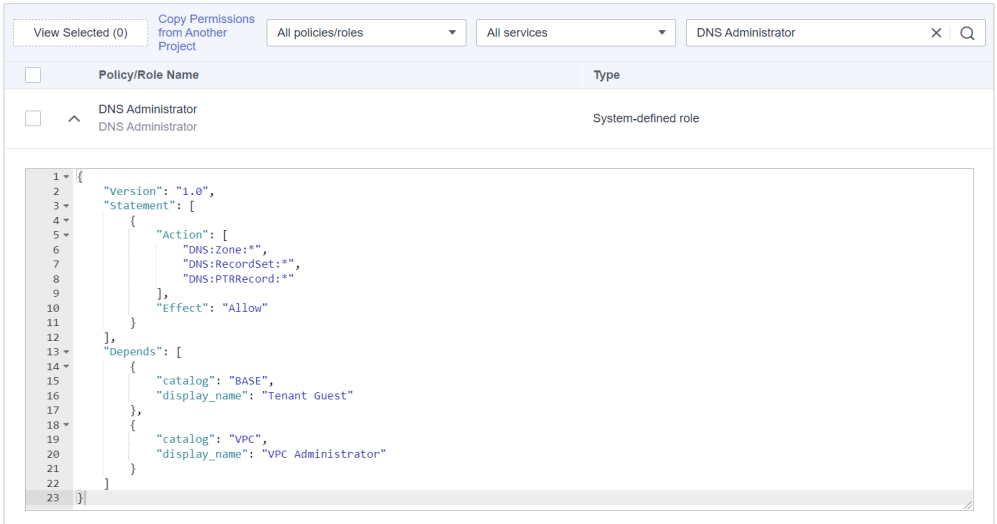
Los roles son un tipo de mecanismo de autorización de grano grueso que define permisos de nivel de servicio en función de las responsabilidades del usuario. IAM proporciona un número limitado de roles para la gestión de permisos.

Servicios de Huawei Cloud interactúan entre sí. Los roles de algunos servicios solo tienen efecto si se asignan junto con los roles de otros servicios. Para obtener más información, consulte **4.6 Asignación de roles de dependencia**.

Contenido de rol

Cuando utilice roles para asignar permisos, puede seleccionar un rol y hacer clic en para ver los detalles del rol. En esta sección se utiliza la función **DNS Administrator** como ejemplo para describir el contenido de la función.

Figura 5-1 Contenido de la función Administrador de DNS




```
{
    "Version": "1.0",
```



```
    "Statement": [
        {
            "Action": [
                "DNS:Zone:*",
                "DNS:RecordSet:*",
                "DNS:PTRRecord:*"
            ],
            "Effect": "Allow"
        }
    ],
    "Depends": [
        {
            "catalog": "BASE",
            "display_name": "Tenant Guest"
        },
        {
            "catalog": "VPC",
            "display_name": "VPC Administrator"
        }
    ]
}
```

Descripción del parámetro

Tabla 5-1 Descripción del parámetro

Parámetro		Descripción	Valor
Version		Versión de rol.	**1.0**: indica el control de acceso basado en roles.
Statement	Action	Operaciones a realizar en el servicio.	Formato: "*Service name*:*Resource type*:*Operation*". **DNS:Zone:***: Permisos para realizar todas las operaciones en las zonas del servicio de nombres de dominio (DNS).
	Effect	Determina si se permiten o deniegan las operaciones definidas en la acción.	● Allow ● Deny **NOTA** Si un rol otorga los efectos Allow y Deny para la misma acción, el Deny tiene prioridad.
Depends	catalog	Nombre del servicio al que pertenece una función de dependencia.	Nombre del servicio. Ejemplo: **BASE** y **VPC**.

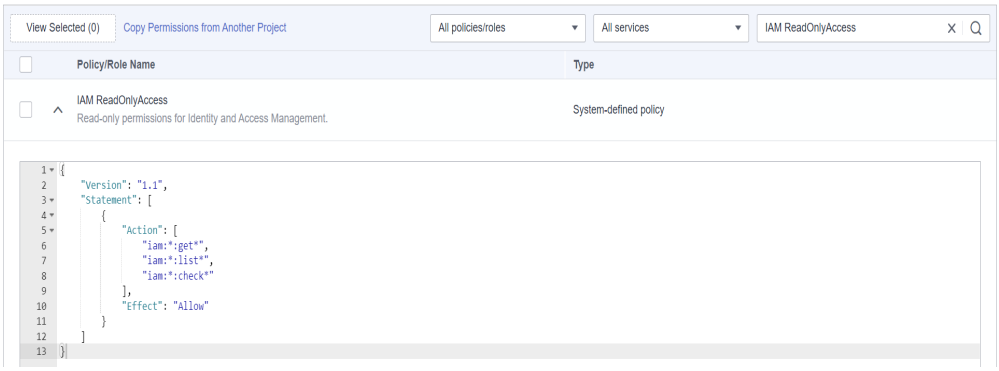
Parámetro		Descripción	Valor
	display_name	Nombre del rol de dependencia.	Nombre del rol. **NOTA** Cuando asigna la función **DNS Administrator** a un grupo de usuarios, también debe asignar las funciones **Tenant Guest** y **VPC Administrator** al grupo para el mismo proyecto. Para obtener más información acerca de las dependencias, vea **Permisos de sistema**.

5.3 Políticas

5.3.1 Contenido de la política

Cuando asigna permisos a un grupo de usuarios, puede hacer clic en a la izquierda de un nombre de política para ver sus detalles. En esta sección se utiliza la política definida por el sistema **IAM ReadOnlyAccess** como ejemplo.

Figura 5-2 Contenido de la Política de ReadOnlyAccess de IAM




```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "iam:*:get*",
                "iam:*:list*",
                "iam:*:check*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

5.3.2 Sintaxis de política

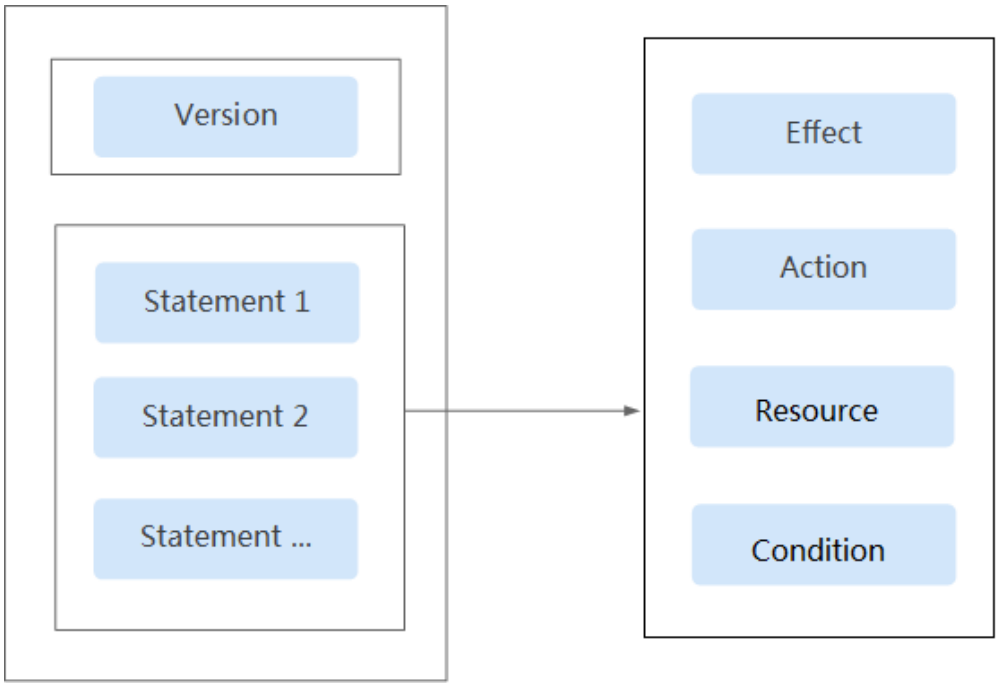
A continuación se utiliza una política personalizada para OBS como ejemplo para describir la sintaxis.


```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:bucket:ListAllMyBuckets",
                "obs:bucket:HeadBucket",
                "obs:bucket:ListBucket",
                "obs:bucket:GetBucketLocation"
            ],
            "Condition": {
                "StringEndWithIfExists": {
                    "g:UserName": [
                        "specialCharactor"
                    ]
                },
                "Bool": {
                    "g:MFAPresent": [
                        "true"
                    ]
                }
            },
            "Resource": [
                "obs:*:*:bucket:*"
            ]
        }
    ]
}
```

Estructura de políticas

Una política consiste en una versión y una o más sentencias (que indican diferentes acciones).

Figura 5-3 Estructura de políticas



Parámetros de política

Los parámetros de directiva incluyen **Version** y **Statement**, que se describen en la tabla siguiente. Puede crear políticas personalizadas especificando los parámetros. Para obtener más información, véase **5.6.3 Casos de uso de políticas personalizadas**.

Tabla 5-2 Parámetros de política

Parámetro		Descripción	Valor
Version		Versión de política.	**1.1**: indica el control de acceso basado en políticas.
Statement	Effect	Determina si se permiten o deniegan las operaciones definidas en la acción.	● Allow ● Deny **NOTA** Si una acción tiene efectos Allow y Deny, el efecto Deny tiene prioridad.
	Action	Operaciones a realizar en el servicio.	Formato: "*Service name*:*Resource type*:*Operation*". Se admiten caracteres carácter comodín (*), que indican todas las opciones. Ejemplo: **obs:bucket:ListAllMybuckets**: Permisos para listar todos los buckets OBS. Vea todas las acciones del servicio en su *Referencia de API*, por ejemplo, consulte **Acciones admitidas de OBS**.
	Condition	Determina cuándo entra en vigor una política. Una condición consiste en una **clave de condición** y un **operador**.	Formato: "*Condition operator*:{*Condition key*:[*Value 1*,*Value 2*]}" Si establece varias condiciones, la política solo tendrá efecto cuando se cumplan todas las condiciones. Ejemplo: **StringEndWithIfExists": {"g:UserName": ["specialCharactor"]}**: La instrucción es válida para usuarios cuyos nombres terminan con **specialCharactor**.

Parámetro		Descripción	Valor
	Resource	Recursos sobre los que entra en vigor la política.	Formato: *Service name*:*Region*:*Account ID*:*Resource type*:*Resource path*. Se admiten caracteres carácter comodín (*). Para obtener más información sobre los servicios en la nube que admiten la autorización a nivel de recursos y los tipos de recursos admitidos, consulte **Servicios en la nube compatibles con la autorización a nivel de recursos mediante IAM**. Ejemplo: ● **obs:*:*:bucket:***: Todos los buckets de OBS. ● **obs:*:*:object:my-bucket/my-object/***: Todos los objetos del directorio **my-object** del bucket **my-bucket**.

- **Condition key**

  Una clave de condición es una clave en el elemento **Condition** de una sentencia. Hay claves de condición globales y de nivel de servicio.

  – Las claves de condición globales (comenzando con **g**:) se aplican a todas las operaciones. IAM proporciona **common global condition keys** y **special global condition keys**.

    ■ Claves de condición globales comunes: Los servicios en la nube no necesitan proporcionar información de identidad del usuario. En su lugar, IAM abstrae automáticamente la información del usuario y autentica a los usuarios. Para obtener más información, véase **Tabla 5-3**.

    ■ Claves de condición global especiales: IAM obtiene información de condición de los servicios en la nube para la autenticación. Solo algunos servicios en la nube admiten claves de condición globales especiales.

  – Las claves de condición de nivel de servicio (comenzando con una abreviatura de nombre de servicio, por ejemplo, **obs**:) solo se aplican a las operaciones en el servicio especificado. Para obtener más información, consulte la guía del usuario del servicio en la nube correspondiente, por ejemplo, consulte **Condiciones de solicitud de OBS**.

Tabla 5-3 Claves de condición global comunes

Clave de condición global	Tipo	Descripción
g:CurrentTime	Time	Tiempo en la que se recibe una solicitud de autenticación. La hora está en formato ISO 8601, por ejemplo **2012-11-11T23:59:59Z**. (**Ver una política de ejemplo que utiliza esta clave de condición**)

Clave de condición global	Tipo	Descripción
g:DomainName	String	Nombre de la cuenta del solicitante. (**Ver una política de ejemplo que utiliza esta clave de condición**)
g:MFAPresent	Boolean	Si se obtiene un token a través de la autenticación MFA. (**Ver una política de ejemplo que utiliza esta clave de condición**)
g:MFAAge	Number	Período de validez de un token obtenido mediante autenticación MFA. Esta condición debe usarse junto con **g:MFAPresent**. (**Ver una política de ejemplo que utiliza esta clave de condición**)
g:ProjectName	String	Nombre del proyecto. (**Ver una política de ejemplo que utiliza esta clave de condición**)
g:ServiceName	String	Nombre del servicio. (**Ver una política de ejemplo que utiliza esta clave de condición**)
g:UserId	String	ID de usuario de IAM. (**Ver una política de ejemplo que utiliza esta clave de condición**)
g:UserName	String	Nombre de usuario IAM. (**Ver una política de ejemplo que utiliza esta clave de condición**)

Tabla 5-4 Claves de condición global especiales

Clave de condición global	Tipo	Descripción
g:SourceIp	IP Address	Dirección IP del usuario que envía una solicitud.
g:SourceVpc	String	ID de VPC del usuario que envía una solicitud.
g:SourceVpce	String	ID de punto de conexión de VPC del usuario que envía una solicitud.
g:TagKeys	String	Clave de etiqueta de recurso.
g:ResourceTag/{TagKey}	String	Valor de clave de etiqueta de recurso.

a. **g:CurrentTime**

   Ejemplo: La siguiente política otorga permiso para crear roles personalizados en IAM desde el 1 de marzo de 2023, 08:00 GMT+08:00 hasta el 30 de marzo de 2023, 08:00 GMT+08:00. El valor de la clave de condición **g:CurrentTime** está en formato UTC.


```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        "DateGreaterThan": {
                                "g:CurrentTime":
["2023-03-01T00:00:00Z"]
                        },
                        "DateLessThan": {
                                "g:CurrentTime":
["2023-03-30T00:00:00Z"]
                        }
                }
        }]
}
```

b. **g: DomainName**

Ejemplo: La siguiente política solo permite que el usuario **zhangsan** cree roles personalizados en IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        "StringEquals": {
                                "g:DomainName": ["zhangsan"]
                        }
                }
        }]
}
```

c. **g:MFAPresent**

Ejemplo: La siguiente política permite a los usuarios que obtengan credenciales mediante MFA crear roles personalizados en IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        "Bool": {
                                "g:MFAPresent": ["true"]
                        }
                }
        }]
}
```

d. **g:MFAAge**

Ejemplo: La siguiente política permite a los usuarios que obtengan credenciales mediante MFA con un período válido superior a 900s crear roles personalizados en IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        " NumberGreaterThanEquals ": {
                                "g:MFAAge": ["900"]
                        }
                }
        }]
}
```


e. **g:ProjectName**

Ejemplo: La siguiente política permite a los usuarios que obtengan credenciales de **CN North-Beijing** crear roles personalizados en IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        " StringEquals ": {
                                "g: ProjectName ": ["cn-north-4"]
                        }
                }
        }]
}
```

f. **g: ServiceName**

Ejemplo: La siguiente política permite a los usuarios acceder a todos los servicios excepto IAM. El valor de esta clave de condición coincide con **Service Name** en la solicitud de autenticación.

```
{
        "Version": "1.1",
        "Statement": [{
                "Action": [
                        "*:*:*"
                ],
                "Effect": "Allow",
                "Condition": {
                        "StringNotEqualsIgnoreCase": {
                                "g:ServiceName": [
                                        "iam"
                                ]
                        }
                }
        }]
}
```

g. **g: UserId**

Ejemplo: La siguiente política solo permite al usuario cuyo ID sea **xxxxxxxxxxx…** crear roles personalizados en IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        "StringEquals": {
                                "g: UserId ": ["xxxxxxxxxxx…"]
                        }
                }
        }]
}
```

h. **g: UserName**

Ejemplo: La siguiente política solo permite que el usuario **lisi** cree roles personalizados en IAM.

```
{
        "Version": "1.1",
        "Statement": [{
                "Effect": "Allow",
                "Action": ["iam:roles:createRoles"],
                "Condition": {
                        "StringEquals": {
                                "g: UserName ": ["lisi"]
```



```
                        }
                    }
            }]
}
```

– Claves de condición multivalor

i. ForAllValues: Comprueba si el valor de cada miembro del conjunto de solicitudes es un subconjunto del conjunto de claves de condición. La condición devuelve true si cada valor de clave de la solicitud coincide con al menos un valor de la política.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ims:images:share"
            ],
            "Condition": {
                "ForAllValues:StringEquals": {
                    "ims:TargetOrgPaths": [
                        "orgPath1",
                        "orgPath2",
                        "orgPath3"
                    ]
                }
            }
        }
    ]
}
```

Esta política muestra cómo usar el calificador ForAllValues con el operador de condición StringEquals. La condición determina si se permite el uso compartido con las cuentas de miembro en la ruta de organización orgPath1, orgPath2 o orgPath3.

Supongamos que un usuario realiza una solicitud para compartir IMS con las cuentas de miembro en las rutas de organización orgPath1 y orgPath3. Se permite la solicitud porque los atributos solicitados del usuario coinciden con los valores especificados en la política.

Si la solicitud del usuario incluye orgPath1, orgPath2, orgPath3 y orgPath4, la solicitud falla porque orgPath4 no está incluida en el operador de condición.

ii. ForAnyValue: Prueba si al menos un miembro del conjunto de valores de solicitud coincide con al menos un miembro del conjunto de valores de clave de condición. La condición devuelve true si cualquiera de los valores de clave de la solicitud coincide con cualquiera de los valores de condición de la política. Para ninguna clave coincidente o un conjunto de datos nulo, la condición devuelve false.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ims:images:share"
            ],
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "ims:TargetOrgPaths": [
                        "orgPath1",
                        "orgPath2",
                        "orgPath3"
                    ]
                }
```



```
                }
            }
        ]
}
```

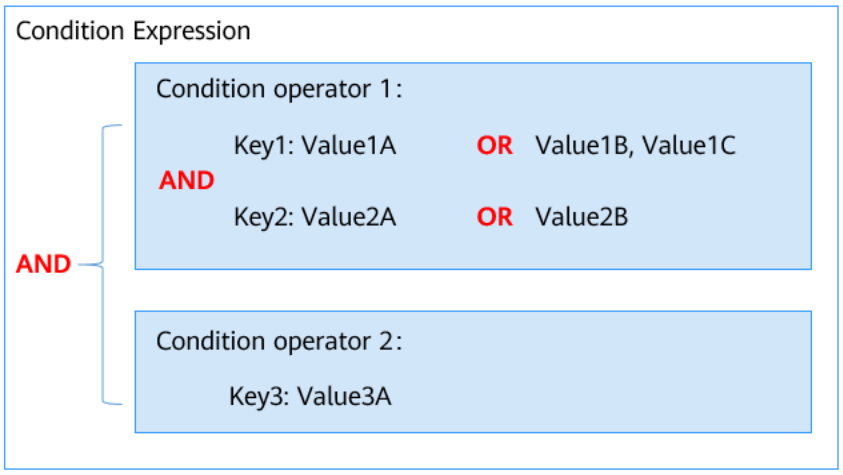
Esta política muestra cómo usar el calificador ForAnyValue con el operador de condición StringEquals. La condición determina si se permite el uso compartido con las cuentas de miembro en la ruta de organización orgPath1, orgPath2 o orgPath3.

Supongamos que un usuario realiza una solicitud para compartir IMS con las cuentas de miembro en la ruta de organización orgPath1 o orgPath4. Se permite la solicitud porque los atributos solicitados del usuario coinciden con los valores especificados en la política.

Si el usuario inicia una solicitud para compartir IMS con las cuentas de miembro en la ruta de organización orgPath4 o orgPath5, la solicitud falla porque orgPath4 y orgPath5 no están incluidos en el operador de condición.

Condition operators

Figura 5-4 Operadores de condiciones



a. Si un único operador de condición incluye múltiples valores para una clave, ese operador de condición se evalúa usando un OR lógico. La condición devuelve **true** si alguno de los valores de clave de la solicitud coincide con cualquiera de los valores de condición de la política.

AVISO

Para los operadores de condiciones coincidentes anulados (como StringNotEquals), el valor de solicitud no puede coincidir con ninguno de los valores de condición basándose en los operadores de condición.

b. Si la política tiene varios operadores de condiciones o varias claves conectadas a un único operador de condiciones, las condiciones se evalúan mediante un AND lógico.

- **Operator**

Un operador, una clave de condición y un valor de condición juntos constituyen una declaración de condición completa. Una política solo entra en vigor cuando se cumplen las condiciones de solicitud. El sufijo de operador **IfExists** indica que una política entra en vigor si un valor de solicitud está vacío o cumple la condición especificada. Por ejemplo, si se selecciona el operador **StringEqualsIfExists** para una política, la política tiene efecto si un valor de solicitud está vacío o es igual al valor de condición especificado. Los operadores son operadores de cadena. No distinguen entre mayúsculas y minúsculas a menos que se especifique lo contrario.

– Operadores de condición de string

Tabla 5-5 Operadores de condición de string

Tipo	Operador	Descripción
String	StringEquals	Coincidencia exacta, sensible a mayúsculas y minúsculas
	StringNotEquals	Coincidencia negativa, sensible a mayúsculas y minúsculas
	StringEqualsIgnoreCase	Coincidencia exacta
	StringNotEqualsIgnore-Case	Coincidencia negativa
	StringMatch	Coincidencia sensible a mayúsculas y minúsculas. Los valores son expresiones regulares que admiten solo comodines de coincidencia de varios caracteres (*) y comodines de coincidencia de un solo carácter (?).
	StringNotMatch	Coincidencia negativa sensible a mayúsculas y minúsculas. Los valores son expresiones regulares que admiten solo comodines de coincidencia de varios caracteres (*) y comodines de coincidencia de un solo carácter (?).

Por ejemplo, la siguiente sentencia contiene un elemento de condición que utiliza "g:DomainName" para especificar que el principal cuyo nombre de dominio es "ZhangSan" puede obtener el contenido y los metadatos del objeto.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:object:GetObject"
            ],
            "Condition": {
                "StringEquals": {
                    "g:DomainName": [
                        "ZhangSan"
                    ]
                }
```



```
            }
        }
    ]
}
```

– Operadores de condición numérica

Tabla 5-6 Operadores de condición numérica

Tipo	Operador	Descripción
Number	NumberEquals	Coincidencia
	NumberNotEquals	Coincidencia negativa
	NumberLessThan	Coincidencia de "menos que"
	NumberLessThanEquals	Coincidencia "Menos que o igual"
	NumberGreaterThan	Coincidencia de "mayor que"
	NumberGreaterThanEquals	Coincidencia "mayor que o igual"

Por ejemplo, la siguiente sentencia contiene un elemento de condición que utiliza el operador de condición "NumericLessThanEquals" con la clave "obs:max-keys" para especificar que el solicitante puede enumerar hasta 10 objetos en "example_bucket" a la vez.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:bucket:ListBucket"
            ],
            "Resource": [
                "OBS:*:*:bucket:example_bucket"
            ],
            "Condition": {
                "NumberLessThanEquals": {
                    "obs:max-keys": [
                        "10"
                    ]
                }
            }
        }
    ]
}
```

– Operadores de condición de fecha

Tabla 5-7 Operadores de condición de fecha

Tipo	Operador	Descripción
Date	DateLessThan	Coincidencia antes de una fecha y hora específicas

Tipo	Operador	Descripción
	DateLessThanEquals	Coincidencia en o antes de una fecha y hora específicas
	DateGreaterThan	Coincidencia después de una fecha y hora específicas
	DateGreaterThanEquals	Coincidencia en o después de una fecha y hora específicas

Por ejemplo, la siguiente sentencia contiene un elemento de condición que utiliza el operador de condición "DateLessThan" con la clave "g:CurrentTime" para especificar que el solicitante puede crear buckets solo antes del 1 de agosto de 2022.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:bucket:CreateBucket"
            ],
            "Condition": {
                "DateLessThan": {
                    "g:CurrentTime": [
                        "2022-08-01T00:00:00Z"
                    ]
                }
            }
        }
    ]
}
```

– Operadores de condición Bool

Tabla 5-8 Operadores de condición Bool

Tipo	Operador	Descripción
Bool	Bool	Las condiciones booleanas permiten construir elementos de condición que restringen el acceso basándose en la comparación de una clave con "true" o "false".

Por ejemplo, esta política basada en identidad utiliza el operador de condición Bool con la clave "g:MFAPresent" para permitir que solo los solicitantes con MFA habilitado puedan modificar las claves de acceso permanente especificadas.

```
{
    "Version": "1.1",
    "Statement": [
        {
```



```
            "Effect": "Allow",
            "Action": [
                "iam:credentials:updateCredential"
            ],
            "Condition": {
                "Bool": {
                    "g:MFAPresent": [
                        "true"
                    ]
                }
            }
        }
    ]
}
```

– Operadores de condición Null

Tabla 5-9 Operadores de condición Null

Tipo	Operador	Descripción
Null	Null	Utilice un operador de condición Null para comprobar si una clave de condición está ausente en el momento de la autorización. En la sentencia de política, use "true" (la clave no existe o es nula) o "false" (la clave existe y su valor no es nulo).

Por ejemplo, puede usar este operador de condición para especificar que solo se permiten las solicitudes de creación de buckets desde las VPC.

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                " obs:bucket:CreateBucket"
            ],
            "Condition": {
                "Null": {
                    "obs:SourceVpc": [
                        "false"
                    ]
                }
            }
        }
    ]
}
```

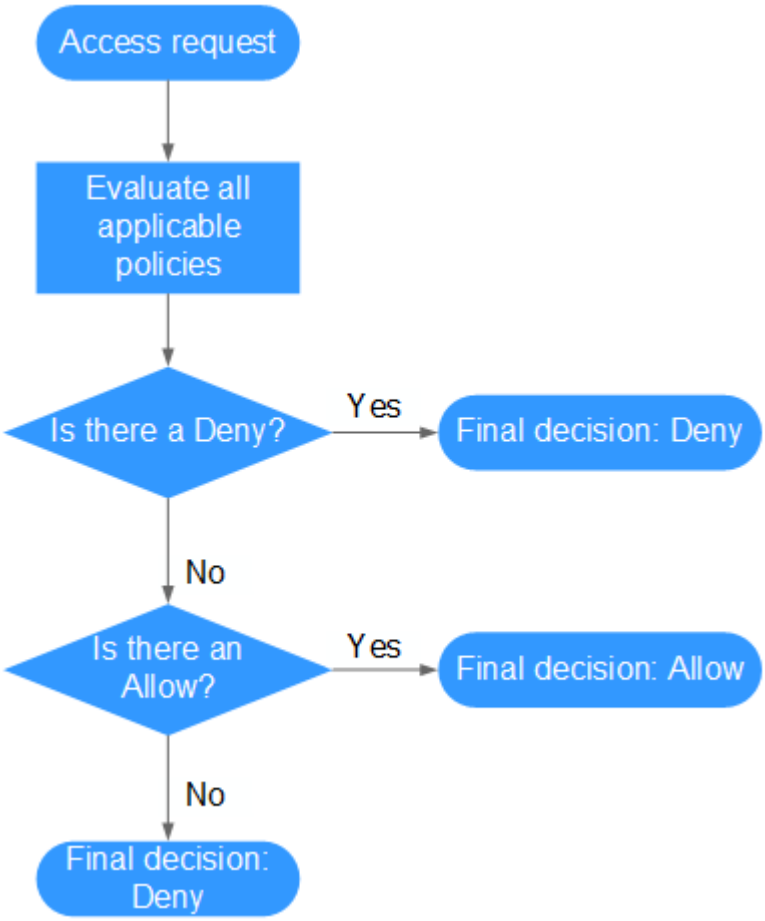
– Sufijo del operador IfExists

Puede agregar "IfExists" al final de cualquier nombre de operador de condición, excepto la "Null condition", por ejemplo, StringEqualsIfExists. Si la clave de política está presente en el contexto de la solicitud, procese la clave como se especifica en la política. Si la clave no está presente, evalúe el elemento de condición como true.

5.3.3 Proceso de autenticación

Cuando un usuario inicia una solicitud de acceso, el sistema autentica la solicitud basándose en las acciones de las directivas que se han asociado al grupo al que pertenece el usuario. El siguiente diagrama muestra el proceso de autenticación.

Figura 5-5 Proceso de autenticación



1. Un usuario inicia una solicitud de acceso.
2. El sistema busca un Deny entre las acciones aplicables de las políticas de las que el usuario obtiene permisos. Si el sistema encuentra un Deny aplicable, devuelve una decisión de Deny, y la autenticación finaliza.
3. Si no se encuentra ningún Deny aplicable, el sistema busca un Allow que se aplicaría a la solicitud. Si el sistema encuentra un Allow aplicable, devuelve una decisión de Allow y la autenticación finaliza.
4. Si no se encuentra ningún permiso aplicable, el sistema devuelve una decisión de Deny y la autenticación finaliza.

5.4 Cambios en los nombres de políticas definidos por el sistema

Todas las políticas definidas por el sistema (anteriormente llamadas "políticas de grano fino") han sido renombradas y los nuevos nombres entrarán en vigor a partir del 6 de febrero de 2020 a las 22:30:00 GMT+08:00. Este cambio no afecta a sus servicios. Las políticas originales definidas por el sistema son la versión 1.0, y las nuevas directivas definidas por el sistema son la versión 1.1. IAM es compatible con ambas versiones.

Tabla 5-10 Nombres de política originales y actuales definidos por el sistema

Servicio	Original	Actual
AOM	AOM Admin	AOM FullAccess
	AOM Viewer	AOM ReadOnlyAccess
APM	APM Admin	APM FullAccess
	APM Viewer	APM ReadOnlyAccess
Auto Scaling	AutoScaling Admin	AutoScaling FullAccess
	AutoScaling Viewer	AutoScaling ReadOnlyAccess
BMS	BMS Admin	BMS FullAccess
	BMS User	BMS CommonOperations
	BMS Viewer	BMS ReadOnlyAccess
BSS	EnterpriseProject_BSS_Administrator	EnterpriseProject BSS FullAccess
CBR	CBR Admin	CBR FullAccess
	CBR User	CBR BackupsAndVaults-FullAccess
	CBR Viewer	CBR ReadOnlyAccess
CCE	CCE Admin	CCE FullAccess
	CCE Viewer	CCE ReadOnlyAccess
CCI	CCI Admin	CCI FullAccess
	CCI Viewer	CCI ReadOnlyAccess
CDM	CDM Admin	CDM FullAccess
	CDM Operator	CDM FullAccessExceptUpdateEIP
	CDM Viewer	CDM ReadOnlyAccess

Servicio	Original	Actual
	CDM User	CDM CommonOperations
CDN	CDN Domain Configuration Operator	CDN DomainConfigureAccess
	CDN Domain Viewer	CDN DomainReadOnlyAccess
	CDN Logs Viewer	CDN LogsReadOnlyAccess
	CDN Refresh And Preheat Operator	CDN RefreshAndPreheatAccess
	CDN Statistics Viewer	CDN StatisticsReadOnlyAccess
CES	CES Admin	CES FullAccess
	CES Viewer	CES ReadOnlyAccess
CS	CS Admin	CS FullAccess
	CS Viewer	CS ReadOnlyAccess
	CS User	CS CommonOperations
CSE	CSE Admin	CSE FullAccess
	CSE Viewer	CSE ReadOnlyAccess
DCS	DCS Admin	DCS FullAccess
	DCS Viewer	DCS ReadOnlyAccess
	DCS User	DCS UseAccess
DDM	DDM Admin	DDM FullAccess
	DDM Viewer	DDM ReadOnlyAccess
	DDM User	DDM CommonOperations
DDS	DDS Admin	DDS FullAccess
	DDS DBA	DDS ManageAccess
	DDS Viewer	DDS ReadOnlyAccess
DLF	DLF Admin	DLF FullAccess
	DLF Developer	DLF Development
	DLF Operator	DLF OperationAndMaintenanceAccess
	DLF Viewer	DLF ReadOnlyAccess
DMS	DMS Admin	DMS FullAccess

Servicio	Original	Actual
	DMS Viewer	DMS ReadOnlyAccess
	DMS User	DMS UseAccess
DNS	DNS Admin	DNS FullAccess
	DNS Viewer	DNS ReadOnlyAccess
DSS	DSS Admin	DSS FullAccess
	DSS Viewer	DSS ReadOnlyAccess
DWS	DWS Admin	DWS FullAccess
	DWS Viewer	DWS ReadOnlyAccess
ECS	ECS Admin	ECS FullAccess
	ECS Viewer	ECS ReadOnlyAccess
	ECS User	ECS CommonOperations
ELB	ELB Admin	ELB FullAccess
	ELB Viewer	ELB ReadOnlyAccess
EPS	EPS Admin	EPS FullAccess
	EPS Viewer	EPS ReadOnlyAccess
EVS	EVS Admin	EVS FullAccess
	EVS Viewer	EVS ReadOnlyAccess
GES	GES Admin	GES FullAccess
	GES Viewer	GES ReadOnlyAccess
	GES User	GES Development
ICITY	iCity Admin	iCity FullAccess
	iCity Viewer	iCity ReadOnlyAccess
IMS	IMS Admin	IMS FullAccess
	IMS Viewer	IMS ReadOnlyAccess
Image Recognition	Image Recognition User	Image Recognition FullAccess
KMS	DEW Keypair Admin	DEW KeypairFullAccess
	DEW Keypair Viewer	DEW KeypairReadOnlyAccess
	KMS CMK Admin	KMS CMKFullAccess
LTS	LTS Admin	LTS FullAccess

Servicio	Original	Actual
	LTS Viewer	LTS ReadOnlyAccess
MRS	MRS Admin	MRS FullAccess
	MRS Viewer	MRS ReadOnlyAccess
	MRS User	MRS CommonOperations
ModelArts	ModelArts Admin	ModelArts FullAccess
	ModelArts User	ModelArts CommonOperations
Moderation	Moderation User	Moderation FullAccess
NAT	NAT Admin	NAT FullAccess
	NAT Viewer	NAT ReadOnlyAccess
OBS	OBS Operator	OBS OperateAccess
	OBS Viewer	OBS ReadOnlyAccess
RDS	RDS Admin	RDS FullAccess
	RDS DBA	RDS ManageAccess
	RDS Viewer	RDS ReadOnlyAccess
RES	RES Admin	RES FullAccess
	RES Viewer	RES ReadOnlyAccess
ROMA Connect	ROMA Admin	ROMA FullAccess
	ROMA Viewer	ROMA ReadOnlyAccess
SCM	SCM Admin	SCM FullAccess
	SCM Viewer	SCM ReadOnlyAccess
	SCM Viewer	SCM ReadOnlyAccess
SFS	SFS Admin	SFS FullAccess
	SFS Viewer	SFS ReadOnlyAccess
SFS Turbo	SFS Turbo Administrator	SFS Turbo FullAccess
	SFS Turbo Viewer	SFS Turbo ReadOnlyAccess
ServiceStage	ServiceStage Admin	ServiceStage FullAccess
	ServiceStage Developer	ServiceStage Development
	ServiceStage Viewer	ServiceStage ReadOnlyAccess
VPC	VPC Admin	VPC FullAccess

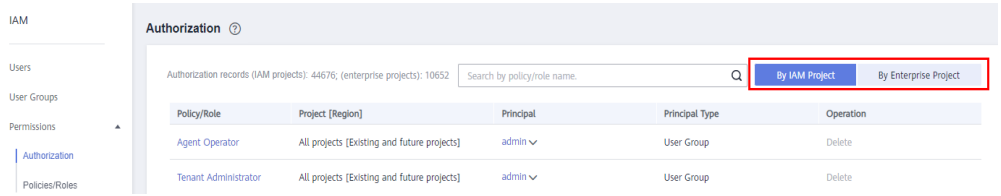
Servicio	Original	Actual
	VPC Viewer	VPC ReadOnlyAccess

5.5 Registros de autorización

Puede ver todos los registros de autorización de su cuenta en la página **Permissions** > **Authorization**. Puede filtrar registros por nombre de política/rol, nombre de usuario, nombre de grupo de usuarios, nombre de agencia, proyecto de IAM, proyecto de empresa (si está habilitado) y tipo principal (usuario, grupo de usuarios o delegación).

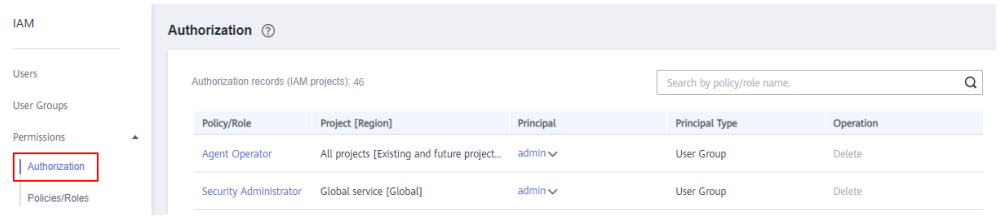
- Función de Proyecto empresarial habilitada: Ver registros de autorización por IAM o proyecto de empresa.

  Figura 5-6 Función de proyecto empresarial habilitada

- Función de Proyecto empresarial no habilitada: Ver registros de autorización por proyecto IAM. Para habilitar el proyecto empresarial, consulte **Habilitación de la función de Enterprise Project**.

  Figura 5-7 La función de proyecto empresarial no está habilitada

Viewing Authorization Records by IAM Project

Cuando vea los registros de autorización por proyecto IAM, seleccione las siguientes condiciones de filtro:

- **Policy/Role name**:

  Para ver los registros de autorización de una política o rol, seleccione **Policy/Role name** e introduzca un nombre. Para obtener más información sobre los permisos de todos los servicios en la nube, consulte **Permisos definidos por el sistema**.

- **Username/User group name/Agency name**:

  Para ver los permisos de proyecto de IAM asignados a un usuario, grupo de usuarios o agencia de IAM específicos, seleccione **Username**, **User group name**, or **Agency name** e introduzca un nombre.

NOTA

Para la autorización basada en proyectos de IAM, puede asignar permisos por grupo de usuarios. Si consulta los registros de autorización de un usuario específico, se muestran los registros de autorización del grupo al que pertenece el usuario.

- **IAM project**: El ámbito de aplicación de los permisos. Si desea ver los registros de autorización de un proyecto IAM, seleccione **IAM project** y cualquiera de las siguientes opciones:
  - **Global services**: Vea los registros de autorización de todos los servicios globales.
  - **All resources**: Vea los registros de autorización de todos los proyectos, es decir, los servicios globales y todos los proyectos específicos de la región (incluidos los proyectos creados posteriormente).
  - **Region-specific projects**: Ver los registros de autorización de un proyecto o subproyecto predeterminado (como)
- **Principal type**: El tipo de objetos que están autorizados. Hay tres tipos principales: usuario, grupo de usuarios y delegación. En la vista de proyecto de IAM, puede filtrar registros por grupo de usuarios o delegación. Si selecciona **User**, no se mostrará ningún registro.
- **Enterprise projects**: Nombre de un proyecto de empresa. Si selecciona **Enterprise project** e introduce un nombre de proyecto de empresa, se mostrará la **vista de proyecto de empresa**.

Consulta de Registros de Autorización por Proyecto empresarial

Al ver los registros de autorización por proyecto de empresa, seleccione las siguientes condiciones de filtro:

- **Policy/Role name**:

  Para ver los registros de autorización de una política o rol, seleccione **Policy/Role name** e introduzca un nombre. Para obtener más información sobre los permisos de servicio en la nube admitidos por proyectos empresariales, consulte **Permisos de servicio en la nube**.
- **Username/User group name/Agency name**:

  Para ver los permisos de proyecto de empresa asignados a un usuario o grupo de usuarios de IAM específico, seleccione **Username** o **User group name** e introduzca un nombre.

  NOTA

  - Para la autorización basada en proyectos de empresa, puede asignar permisos por usuario. Si consulta los registros de autorización de un usuario específico, se muestran los registros de autorización del usuario y el grupo de usuarios al que pertenece.
- **Enterprise project**: nombre de un proyecto de empresa, es decir, el ámbito de aplicación de los permisos. Para ver los registros de autorización de un proyecto de empresa específico, seleccione **Enterprise project** e introduzca un nombre de proyecto de empresa.
- **Principal type**: El tipo de objetos que están autorizados. Hay tres tipos principales: usuario, grupo de usuarios y delegación.
- **IAM project**: Nombre de un proyecto o región de IAM. Si selecciona un **IAM project** e introduce un nombre de proyecto, se mostrará la **vista de proyecto de IAM**.

5.6 Políticas personalizadas

5.6.1 Creación de una política personalizada

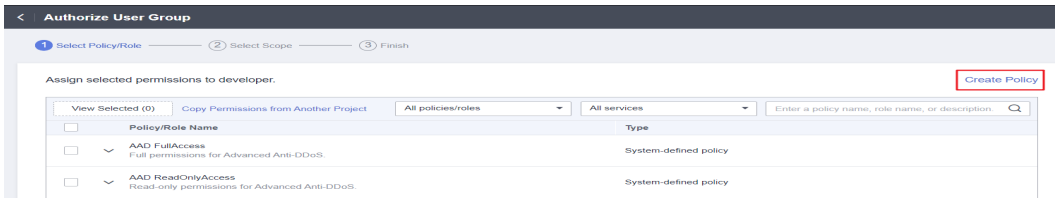
Puede crear políticas personalizadas para complementar las políticas definidas por el sistema e implementar un control de acceso más refinado.

Puede crear las políticas personalizadas de cualquiera de las siguientes maneras:

- Editor visual: Seleccionar servicios en la nube, acciones, recursos y condiciones de solicitud. Esto no requiere conocimiento de la sintaxis de políticas.
- JSON: Crear una política JSON o editar una existente.

En esta sección se describe cómo crear políticas personalizadas en la página **Permissions** > **Policies/Roles**. También puede crear políticas personalizadas durante la autorización (consulte **Figura 5-8**).

Figura 5-8 Creación de una política durante la autorización

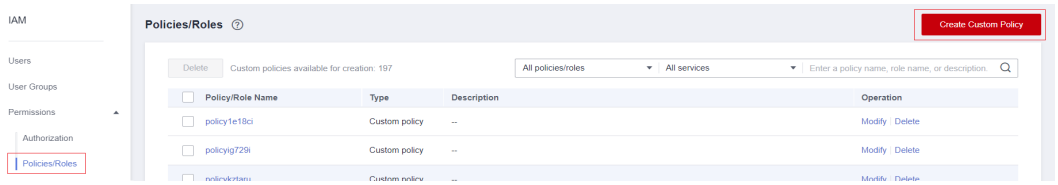


Creación de una política personalizada en el editor visual

Paso 1 Inicie sesión en la **consola de IAM**.

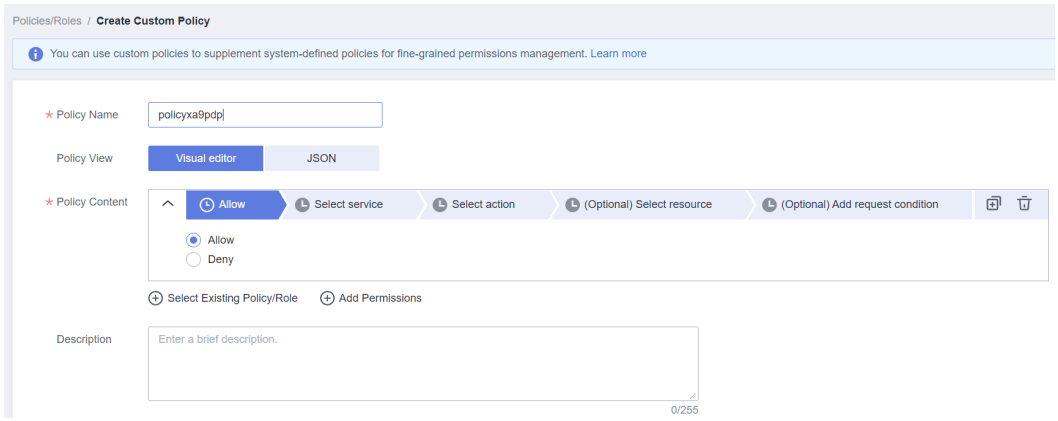
Paso 2 En la consola de IAM, seleccione **Permissions** > **Policies/Roles** en el panel de navegación y haga clic en **Create Custom Policy** en la esquina superior derecha.

Figura 5-9 Creación de una política personalizada



Paso 3 Introduzca un nombre de política.

Figura 5-10 Introducir un nombre de política



Paso 4 Seleccione **Visual editor** para **Policy View**.

Paso 5 Establezca el contenido de la política.

1. Seleccione **Allow** o **Deny**.
2. Seleccione un servicio en la nube.

   NOTA

   - Solo se puede seleccionar un servicio en la nube para cada bloque de permisos. Para configurar permisos para varios servicios en la nube, haga clic en **Add Permissions**, o cambie a la vista JSON (consulte **Creación de una política personalizada en la vista JSON**).
   - Una política personalizada puede contener permisos para servicios globales o a nivel de proyecto. Para definir los permisos necesarios para acceder a los servicios globales y a nivel de proyecto, incluya los permisos en dos directivas personalizadas independientes para la autorización refinada.
3. Seleccione acciones.
4. (Opcional) Seleccione todos los recursos o seleccione recursos específicos especificando sus rutas.

   Para obtener más información sobre los servicios en la nube que admiten la autorización a nivel de recursos, consulte **5.6.4 Servicios en la nube que admiten la autorización a nivel de recursos mediante IAM**.

Tabla 5-11 Tipo de recurso

Parámetro	Descripción
Specific	Permisos para recursos específicos. Por ejemplo, para definir permisos para buckets cuyos nombres comiencen por **TestBucket** especifique la ruta del recurso del bucket como **OBS:*:*:bucket:TestBucket***. **NOTA** – Especificación de recursos de bucket Formato: "OBS:*:*:bucket:*Bucket name*". Para los recursos del bucket, IAM genera automáticamente el prefijo de la ruta del recurso: **obs:*:*:bucket:**. Para la ruta de un bucket específico, agregue el *bucket name* al final. También puede utilizar un carácter comodín (*) para indicar cualquier bucket. Por ejemplo, **obs:*:*:bucket:*** indica cualquier bucket OBS. – Especificación de recursos de objeto Formato: "OBS:*:*:object:*Bucket name/object name*". Para los recursos de objetos, IAM genera automáticamente el prefijo de la ruta de recursos: **obs:*:*:object:**. Para la ruta de acceso de un objeto específico, agregue el *bucket name/object name* al final de la ruta de acceso del recurso. También puede utilizar un carácter comodín (*) para indicar cualquier objeto de un bucket. Por ejemplo, **obs:*:*:object:my-bucket/my-object/*** indica cualquier objeto en el directorio **my-object** del bucket de **my-bucket**.
All	Permisos para todos los recursos.

5. (Opcional) Agregue las condiciones de solicitud especificando claves de condición, operadores y valores.

Tabla 5-12 Parámetros de condición

Nombre	Descripción
Condition Key	Una clave en el elemento **Condition** de una sentencia. Hay claves de condición globales y específicas de servicio. **Las claves de condición globales** (comenzando con **g**:) están disponibles para las operaciones de todos los servicios, mientras que las claves de condición específicas de servicio (comenzando con un nombre de abreviatura de servicio como **obs:**) están disponibles sólo para las operaciones del servicio correspondiente. Para obtener más información, consulte la guía del usuario del servicio en la nube correspondiente, por ejemplo, consulte **Condiciones de solicitud de OBS**.
Operator	Se utiliza junto con una clave de condición y un valor de condición para formar una sentencia de condición completa.
Value	Se utiliza junto con una clave de condición y un operador que requiere una palabra clave, para formar una sentencia de condición completa.

Figura 5-11 Adición de una condición de solicitud

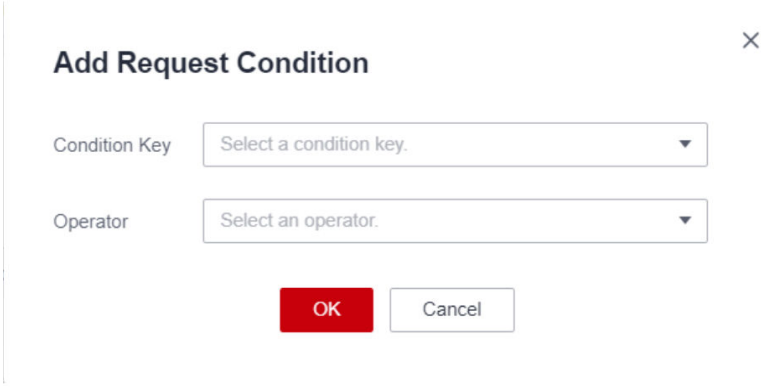


Tabla 5-13 Claves de condición globales

Clave de condición global	Tipo	Descripción
g:CurrentTime	Time	Tiempo en la que se recibe una solicitud de autenticación. La hora está en formato ISO 8601, por ejemplo **2012-11-11T23:59:59Z**.
g:DomainName	String	Nombre de cuenta.
g:MFAPresent	Boolean	Si se obtiene un token a través de la autenticación MFA.
g:MFAAge	Number	Período de validez de un token obtenido mediante autenticación MFA. Esta condición debe usarse junto con **g:MFAPresent**.
g:ProjectName	String	Nombre del proyecto.
g:ServiceName	String	Nombre del servicio.
g:UserId	String	ID de usuario de IAM.
g:UserName	String	Nombre de usuario de IAM.

Paso 6 (Opcional) Cambie a la vista JSON y modifique el contenido de la política en formato JSON.

NOTA

Si el contenido de la política modificada es incorrecto, vuelva a comprobarlo y modificarlo o haga clic en **Reset** para cancelar las modificaciones.

Paso 7 (Opcional) Para agregar otro bloque de permisos a la política, haga clic en **Add Permissions**. También puede hacer clic en el icono de (+) más a la derecha de un bloque de permisos existente para clonar sus permisos.

Paso 8 (Opcional) Introduzca una breve descripción de la política.

Paso 9 Haga clic en **OK**.

Paso 10 Adjunte la política a un grupo de usuarios. Los usuarios del grupo heredan los permisos definidos en esta política.

NOTA

Puede adjuntar políticas personalizadas a un grupo de usuarios del mismo modo que adjuntar políticas definidas por el sistema. Para obtener más información, véase **4.1 Creación de un grupo de usuarios y asignación de permisos**.

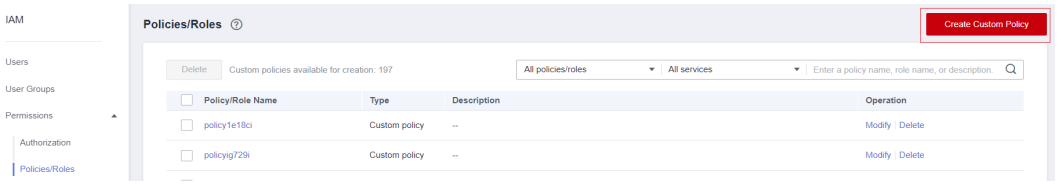
----Fin

Creación de una política personalizada en la vista JSON

Paso 1 Inicie sesión en la **consola de IAM**.

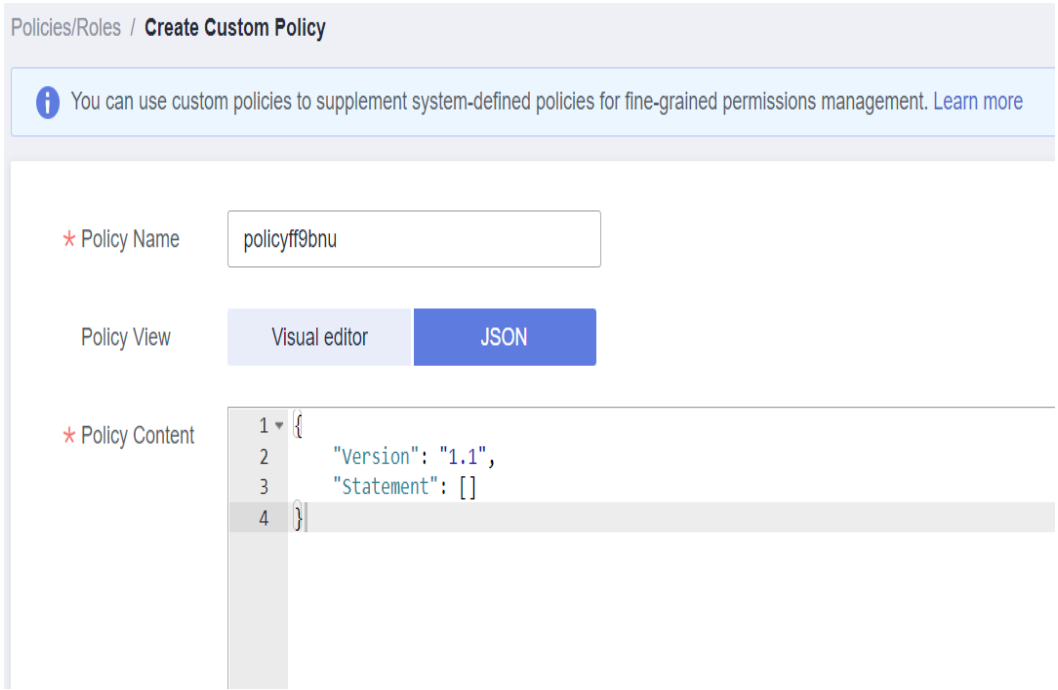
Paso 2 En la consola de IAM, seleccione **Permissions** > **Policies/Roles** en el panel de navegación y haga clic en **Create Custom Policy** en la esquina superior derecha.

Figura 5-12 Creación de una política personalizada



Paso 3 Introduzca un nombre de política.

Figura 5-13 Introducir un nombre de política



Paso 4 Seleccione **JSON** para **Policy View**.

Paso 5 (Opcional) Haga clic en **Select Existing Policy/Role** y seleccione una política o función para usarla como plantilla, por ejemplo, seleccione **EVS FullAccess**.

NOTA

Si selecciona varias políticas, todas deben tener el mismo ámbito, es decir, **Global services** o **Project-level services**. Para definir los permisos necesarios para acceder a los servicios globales y a nivel de proyecto, incluya los permisos en dos directivas personalizadas independientes para la autorización refinada.

Paso 6 Haga clic en **OK**.

Paso 7 Modifique la sentencia en la plantilla.

- **Effect**: Establezca como **Allow** o **Deny**.
- **Action**: Ingrese las acciones que aparecen en la tabla de acciones de la API (consulte **Figura 5-14**) del servicio EVS, por ejemplo, **evs:volumes:create**.

Figura 5-14 Acciones de API

Permission	API	Action
Listing IAM Users	GET /v3/users	iam:users:listUsers

NOTA

- La versión de cada política personalizada se fija en **1.1**.
- Para obtener más información sobre las acciones de la API admitidas por cada servicio, consulte **Permisos definidos por el sistema**.

Paso 8 (Opcional) Introduzca una breve descripción de la política.

Paso 9 Haga clic en **OK**. Si se muestra la lista de políticas, la política se crea correctamente. Si se muestra un mensaje que indica contenido de política incorrecto, modifique la política.

Paso 10 Adjunte la política a un grupo de usuarios. Los usuarios del grupo heredan los permisos definidos en esta política.

NOTA

Puede adjuntar políticas personalizadas a un grupo de usuarios del mismo modo que adjuntar políticas definidas por el sistema. Para obtener más información, véase **4.1 Creación de un grupo de usuarios y asignación de permisos**.

----Fin

5.6.2 Modificación o eliminación de una política personalizada

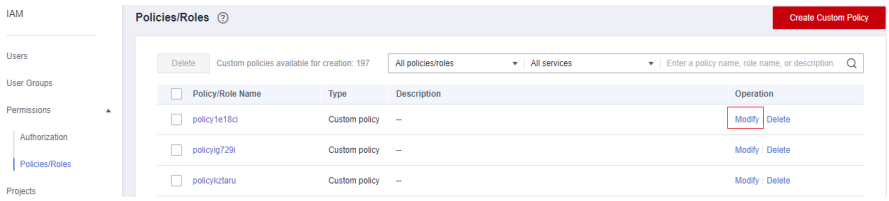
Puede modificar o eliminar políticas personalizadas.

Modificación de una política personalizada

Modifique el nombre, la descripción o el contenido de una política personalizada.

1. En el panel de navegación izquierdo de la **consola de IAM**, elija **Permissions** > **Policies/Roles**.
2. Busque la política personalizada que desea modificar y haga clic en **Modify** en la columna **Operation** o haga clic en el nombre de la política personalizada para ir a la página de detalles de la política.

Figura 5-15 Modificación del contenido de la política



3. Modifique el nombre o la descripción de la política según sea necesario.
4. Modifique el contenido de la política siguiendo las instrucciones proporcionadas en **Creación de una política personalizada en el Editor visual** según sea necesario.
5. Haga clic en **OK** para guardar las modificaciones.

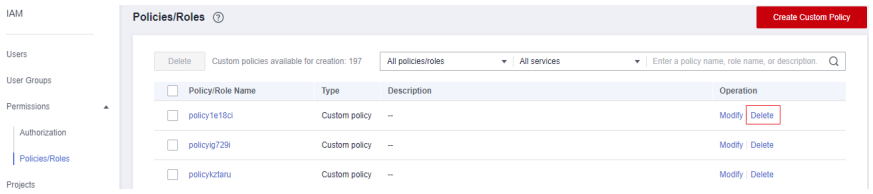
Eliminación de una política personalizada

NOTA

Solo se pueden eliminar las políticas personalizadas que no estén asociadas a ningún grupo de usuarios o delegaciones. Si se ha asociado una política personalizada a determinados grupos de usuarios o agencias, separe la política y, a continuación, elimínela.

1. En el panel de navegación izquierdo de la **consola de IAM**, elija **Permissions** > **Policies/Roles**.
2. En la fila que contiene la política personalizada que desea eliminar, haga clic en **Delete**.

Figura 5-16 Eliminación de una política personalizada



3. Haga clic en **Yes**.

5.6.3 Casos de uso de políticas personalizadas

Uso de una política personalizada junto con políticas definidas por el sistema de permiso completo

Si desea asignar permisos completos a un usuario pero no permitirle acceder a un servicio específico, como Cloud Trace Service (CTS), cree una política personalizada para denegar el acceso a CTS y, a continuación, adjunte esta política personalizada junto con la política **FullAccess** al usuario. Como un rechazo explícito en cualquier política anula cualquier permiso, el usuario puede realizar operaciones en todos los servicios excepto CTS.

Ejemplo de política que deniega el acceso solo a CTS:


```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                    "cts:*:*"
            ]
        }
    ]
}
```

NOTA

- **Action**: Operaciones a realizar. Cada acción debe definirse en el formato "*Service name*:*Resource type*:*Operation*".

  Por ejemplo, **cts:*:*** se refiere a los permisos para realizar todas las operaciones en todos los tipos de recursos de CTS.
- **Effect**: determina si se debe denegar o permitir la operación.

Uso de una política personalizada junto con una política definida por el sistema

- Si desea asignar permisos completos a un usuario pero no permitirle crear BMS, cree una política personalizada que deniegue la acción **bms:servers:create** y, a continuación, adjunte esta política personalizada junto con la política **BMS FullAccess** al usuario. Como un rechazo explícito en cualquier política anula cualquier permiso, el usuario puede realizar todas las operaciones en BMS excepto crear BMS.

  Ejemplo de política que deniega la creación de BMS:

  ```
  {
      "Version": "1.1",
      "Statement": [
          {
              "Effect": "Deny",
              "Action": [
                      "bms:servers:create"
              ]
          }
      ]
  }
  ```

- Si desea asignar permisos de solo lectura de OBS a todos los usuarios pero no permitir que ciertos usuarios vean recursos específicos, por ejemplo, no permitir que los usuarios cuyos nombres comiencen por **TestUser** vean depósitos cuyos nombres comiencen por **TestBucket** crear una política personalizada que deniegue dichas operaciones y adjuntar esta política personalizada junto con la política OBS ReadOnlyAccess a esos usuarios. Como un rechazo explícito en cualquier política anula cualquier permiso, ciertos usuarios no pueden ver depósitos cuyos nombres comienzan con **TestBucket**.

  Política de ejemplo que niega a los usuarios cuyos nombres comienzan por **TestUser** ver depósitos cuyos nombres comienzan por **TestBucket**:

  ```
  {
          "Version": "1.1",
          "Statement": [
                  {
                          "Effect": "Deny",
                          "Action": [
                                  "obs:bucket:ListAllMybuckets",
                                  "obs:bucket:HeadBucket",
                                  "obs:bucket:ListBucket",
                                  "obs:bucket:GetBucketLocation"
                          ],
                          "Resource": [
                              "obs:*:*:bucket:TestBucket*"
  ```



```
                        ],
                        "Condition": {
                            "StringStartWith": {
                                "g:UserName": [
                                    "TestUser"
                    ]
                }
            }
                }
        ]
}
```

NOTA

Actualmente, solo ciertos servicios en la nube (como OBS) admiten la autorización basada en recursos. Para los servicios que no admiten esta función, no puede crear políticas personalizadas que contengan tipos de recursos.

Usar solo una política personalizada

Puede crear una política personalizada y adjuntar solo la política personalizada al grupo al que pertenece el usuario.

- A continuación se muestra una política de ejemplo que permite el acceso solo a ECS, EVS, VPC, ELB y Application Operations Management (AOM).

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow"
                        "Action": [
                                "ecs:*:*",
                                "evs:*:*",
                                "vpc:*:*",
                                "elb:*:*",
                                "aom:*:*"
                        ]
                }
        ]
}
```

- A continuación se muestra una política de ejemplo que permite que solo los usuarios de IAM cuyos nombres comiencen por **TestUser** eliminen todos los objetos del directorio **my-object** del bucket **my-bucket**.

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                            "obs:object:DeleteObject"
                        ],
                        "Resource": [
                            "obs:*:*:object:my-bucket/my-object/*"
                        ],
                        "Condition": {
                            "StringStartWith": {
                                "g:UserName": [
                                    "TestUser"
                    ]
                }
        ]
}
```

- A continuación se muestra una política de ejemplo que permite el acceso a todos los servicios excepto ECS, EVS, VPC, ELB, AOM y APM.


```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Effect": "Allow",
                        "Action": [
                                "*:*:*"
                        ]
                },
                {
                        "Action": [
                                "ecs:*:*",
                "evs:*:*",
                "vpc:*:*",
                "elb:*:*",
                "aom:*:*",
                "apm:*:*"
                        ],
                        "Effect": "Deny"
                }
        ]
}
```

5.6.4 Servicios en la nube que admiten la autorización a nivel de recursos mediante IAM

Si desea conceder permisos de usuario de IAM para recursos específicos, **cree una política personalizada** que contenga permisos para los recursos y adjunte la política al usuario. El usuario solo tiene los permisos para los recursos especificados. Por ejemplo, para conceder permisos de usuario de IAM para buckets cuyos nombres comiencen por **TestBucket**, cree una política personalizada, especifique la ruta de acceso del recurso como **OBS:*:*:bucket:TestBucket***, y adjunte la política al usuario.

En la siguiente tabla se enumeran los servicios en la nube que admiten la autorización a nivel de recursos y los tipos de recursos admitidos.

Tabla 5-14 Servicios en la nube que admiten la autorización a nivel de recursos y los tipos de recursos admitidos

Servicio	Tipo de recurso	Nombre de recurso
Elastic Cloud Server (ECS)	instance	ECS
Elastic Volume Service (EVS)	volume	EVS disk
Object Storage Service (OBS)	bucket	Bucket
	object	Object
Virtual Private Cloud (VPC)	publicip	EIP
Software Repository for Container (SWR)	chart	Chart
	repository	Repository
	instance	Instance
Intelligent EdgeFabric (IEF)	product	Product
	node	Edge node

Servicio	Tipo de recurso	Nombre de recurso
	group	Edge node group
	deployment	Deployment
	batchjob	Batch job
	application	Application template
	appVersion	Application template version
	IEFInstance	IEF instance
	cluster	Cluster
Data Lake Insight (DLI)	queue	DLI queue
	database	DLI database
	table	DLI table
	column	DLI column
	datasourceauth	DLI security authentication information
	jobs	DLI job
	resource	Resource package
	elasticresourcepool	Elastic resource pool
	group	Resource package group
Graph Engine Service (GES)	graphName	GES graph name
	backupName	GES backup name
	metadataName	Metadata name
FunctionGraph	function	Function
	trigger	Trigger
Distributed Message Service (DMS)	rabbitmq	RabbitMQ instance
	kafka	Kafka instance
Distributed Cache Service (DCS)	instance	Instance
Document Database Service (DDS)	instanceName	Instance name
Resource Formation Service (RFS)	stack	Stack

Servicio	Tipo de recurso	Nombre de recurso
Data Encryption Workshop (DEW)	KeyId	Key ID
GaussDB(DWS)	cluster	Cluster
Cloud Bastion Host (CBH)	instanceId	Instance ID
ROMA Connect	graph	Service flowchart

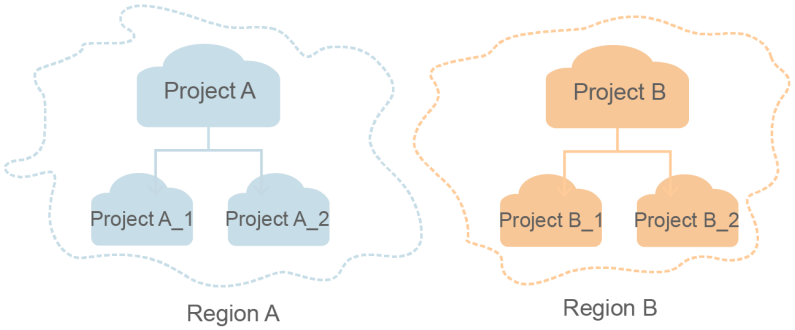
6 Proyectos

Los proyectos se utilizan para aislar los recursos (incluidos los recursos de cómputo, almacenamiento y red) entre las regiones físicas. Se proporciona un proyecto para cada región de forma predeterminada y los permisos se asignan en función de los proyectos.

Para un control de acceso más refinado, cree subproyectos bajo un proyecto y compre recursos en los subproyectos. A continuación, proporcione a los usuarios permisos para acceder a recursos en subproyectos específicos.

Los proyectos de IAM son diferentes de los proyectos empresariales. Para obtener más información sobre sus diferencias, consulte **¿Cuáles son las diferencias entre los proyectos de IAM y los proyectos empresariales?**

Figura 6-1 Aislamiento del proyecto



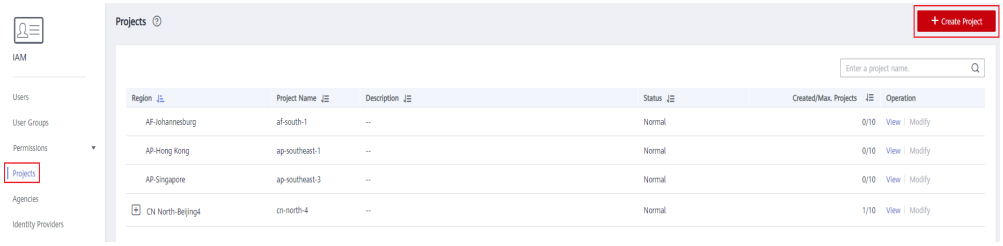
NOTA

- Los recursos no se pueden transferir a través de proyectos de IAM.
- No se pueden crear proyectos en IAM después de habilitar la función Proyecto empresarial.

Creación de un proyecto

Paso 1 En el panel de navegación izquierdo de la **consola de IAM**, elija Projects y haga clic en **Create Project**.

Figura 6-2 Creación de un proyecto



Paso 2 Seleccione una región en la que desee crear un subproyecto.

Paso 3 Ingrese el nombre de un proyecto.

NOTA

- El nombre del proyecto tendrá el formato "*Name of the default project for the selected region_Custom project name*". No se puede modificar el nombre de los proyectos por defecto.
- El nombre del proyecto solo puede contener letras, dígitos, guiones (-) y guiones bajos (_). La longitud total del nombre del proyecto no puede superar los 64 caracteres.

Paso 4 (Opcional) Introduzca una descripción para el proyecto.

Paso 5 Haga clic en **OK**.

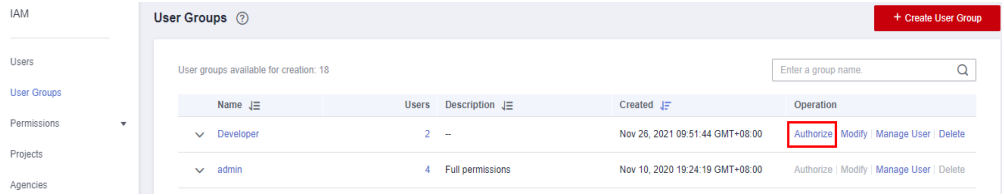
----Fin

Concesión de permisos de grupo de usuarios para un proyecto

Puede asignar permisos basados en proyectos para controlar el acceso a recursos en proyectos específicos.

Paso 1 En la lista de grupos de usuarios, haga clic en **Authorize** en la fila que contiene el grupo de usuarios de destino.

Figura 6-3 Gestión de permisos



Paso 2 En la página **Authorize User Group**, seleccione las políticas o roles que se adjuntarán al grupo de usuarios y haga clic en **Next**.

Paso 3 Especifique el ámbito de autorización. Si selecciona **Region-specific projects**, seleccione uno o más proyectos.

Paso 4 Haga clic en **OK**.

NOTA

Para obtener más información acerca de la autorización de grupo de usuarios, consulte **4.1 Creación de un grupo de usuarios y asignación de permisos**.

----Fin

Cambio de regiones o proyectos

Para los servicios a nivel de proyecto, cambie a una región o proyecto en el que se le haya autorizado a acceder a los servicios en la nube. No es necesario cambiar de regiones o proyectos para los servicios globales.

Paso 1 Inicie sesión en la consola de gestión de Huawei Cloud.

Paso 2 Vaya a una página de servicio en la nube a nivel de proyecto. Haga clic en el cuadro de lista desplegable en la esquina superior izquierda de la página y seleccione una región.

----Fin

7 Agencias

7.1 Delegación de cuenta

7.1.1 Delegación del acceso a recursos a otra cuenta

La función de delegación le permite delegar otra cuenta para implementar O&M en sus recursos en función de los permisos asignados.

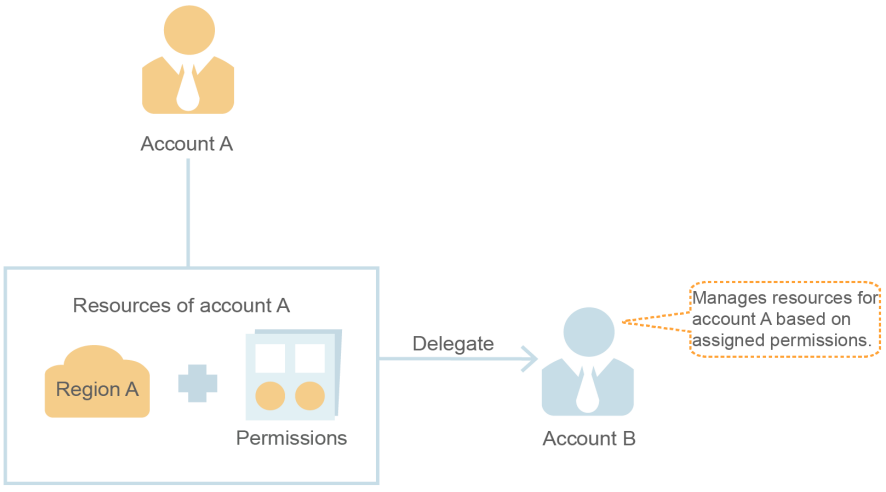
NOTA

Solo puede delegar el acceso a recursos en las cuentas. A continuación, las cuentas pueden delegar el acceso a los usuarios de IAM bajo ellas.

El siguiente es el procedimiento para delegar el acceso a recursos a otra cuenta. La cuenta A es la parte delegante y la cuenta B es la parte delegada.

Paso 1 Account A creates an agency in IAM to delegate resource access to account B.

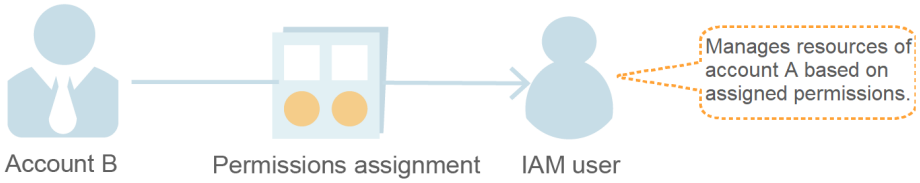
Figura 7-1 (Account A) Creating an agency



Paso 2 (Opcional) La cuenta B asigna permisos a un usuario de IAM para gestionar recursos específicos para la cuenta A.

1. Cree un grupo de usuarios y conceda los permisos necesarios para gestionar los recursos de la cuenta A.
2. Cree un usuario y agregue el usuario al grupo de usuarios.

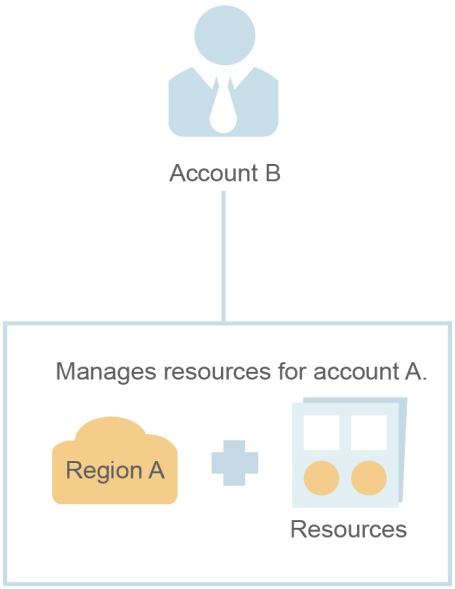
Figura 7-2 (Cuenta B) Autorizar a un usuario de IAM a gestionar recursos delegados



Paso 3 La cuenta B o el usuario autorizado gestiona los recursos de la cuenta A.

1. Inicie sesión en la cuenta de la cuenta B y cambie el rol a la cuenta A.
2. Cambie a la región A y administre los recursos de la cuenta A en esta región.

Figura 7-3 (Cuenta B) Cambiar el rol



----Fin

7.1.2 Creación de una delegación (por una Parte Delegada)

Al crear una delegación, puede compartir sus recursos con otra cuenta o delegar a un individuo o equipo para gestionar sus recursos. No es necesario que comparta sus credenciales de seguridad (la contraseña y las claves de acceso) con la parte delegada. En su lugar, la parte delegada puede iniciar sesión con sus propias credenciales de cuenta y, a continuación, cambiar el rol a su cuenta y gestionar sus recursos.

Prerrequisitos

Antes de crear una delegación, complete las siguientes operaciones:

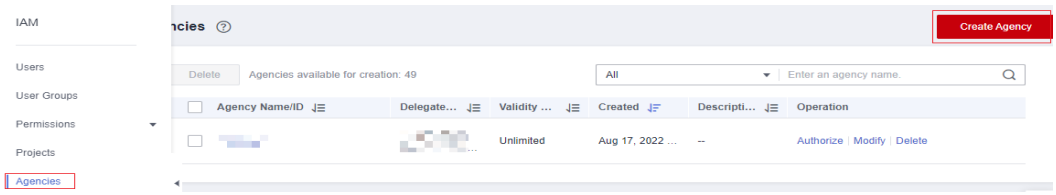
- Comprenda los **conceptos básicos** de permisos.
- Determine los **permisos definidos por el sistema** que se asignarán a la delegación, y compruebe si los permisos tienen dependencias. Para obtener más información, consulte **Asignación de funciones de dependencia**.

Procedimiento

Paso 1 Inicie sesión en la **consola de IAM**.

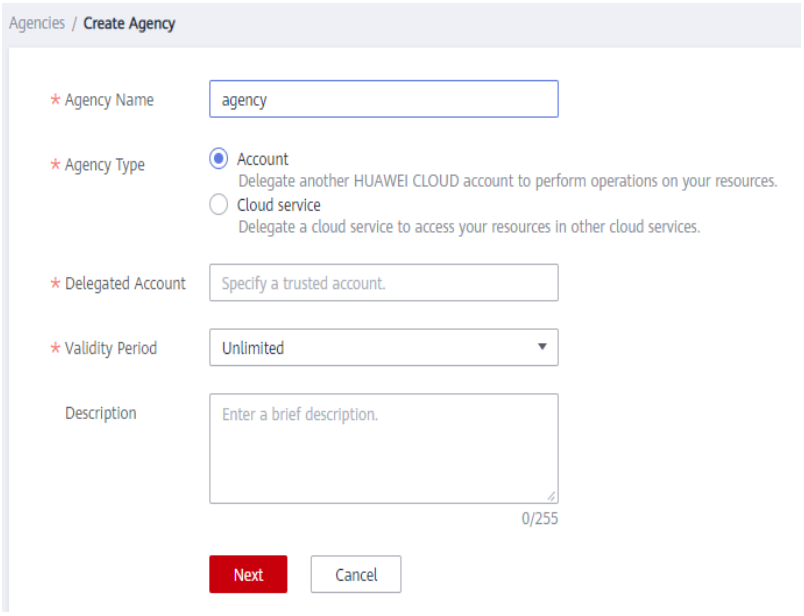
Paso 2 En la consola de IAM, seleccione **Agencies** en el panel de navegación y haga clic en **Create Agency** en la esquina superior derecha.

Figura 7-4 Creación de una delegación



Paso 3 Ingrese el nombre de una delegación.

Figura 7-5 Establecer el nombre de la delegación



Paso 4 Especifique el tipo de delegación como **Account** e introduzca el nombre de una cuenta delegada.

NOTA

- **Account**: Compartir recursos con otra cuenta o delegar a un individuo o equipo para gestionar sus recursos. La cuenta delegada solo puede ser una cuenta, en lugar de un usuario IAM o un usuario federado.
- **Cloud service**: Delegar un servicio específico para acceder a otros servicios. Para obtener más información, consulte **7.2 Delegación de servicios en la nube**.

Paso 5 Establezca el período de validez e introduzca una descripción para la delegación.

Paso 6 Haga clic en **Next**.

Paso 7 Seleccione las políticas o roles que se adjuntarán a la delegación, haga clic en **Next** y seleccione el ámbito de autorización.

NOTA

- La asignación de permisos a una agencia es similar a la asignación de permisos a un grupo de usuarios. Las dos operaciones difieren solo en el número de permisos disponibles. Para obtener más información sobre cómo asignar permisos a un grupo de usuarios, consulte **Asignación de permisos a un grupo de usuarios**.
- No se puede asignar a las agencias el rol de **Security Administrator**. Para garantizar la seguridad de la cuenta, conceda los permisos necesarios a las delegaciones en función del principio de privilegio mínimo.

Paso 8 Haga clic en **OK**.

NOTA

Después de crear una agencia, proporcione su nombre de dominio de cuenta, nombre de delegación, ID de delegación y permisos de delegación a la parte delegada. La parte delegada puede cambiar el rol a su cuenta y gestionar recursos específicos en función de los permisos asignados.

----Fin

7.1.3 (Opcional) Asignación de permisos a un usuario de IAM (por una parte delegada)

Cuando se establece una relación de confianza entre su cuenta y otra cuenta, usted se convierte en una parte delegada. De forma predeterminada, solo tu cuenta y los miembros del grupo de **admin** pueden gestionar los recursos del grupo de delegación. Para autorizar a los usuarios de IAM a gestionar estos recursos, asigne permisos a los usuarios.

Puede autorizar a un usuario de IAM a gestionar recursos para todas las partes delegadas, o autorizar al usuario a gestionar recursos para una parte delegada específica.

Prerrequisitos

- Se ha establecido una relación de confianza entre su cuenta y otra cuenta.
- Usted ha obtenido el nombre de la cuenta delegada y el nombre e ID de la agencia creada.

Procedimiento

Paso 1 Cree un grupo de usuarios y concédale permisos.

1. En la página **User Groups**, haga clic en **Create User Group**.

2. Ingrese un nombre de grupo de usuarios.
3. Haga clic en **OK**.
4. En la fila que contiene el grupo de usuarios, haga clic en **Authorize**.
5. Cree una política personalizada.

   NOTA

   Este paso se utiliza para crear una política que contiene los permisos necesarios para gestionar los recursos de una agencia específica. Si desea autorizar a un usuario de IAM a gestionar recursos para todas las delegaciones, vaya a **Paso 1.6**.

   a. En la página **Select Policy/Role**, haga clic en **Create Policy** en la esquina superior derecha de la lista de permisos.
   b. Introduzca un nombre de política.
   c. Seleccione **JSON** para **Policy View**.
   d. En el área **Policy Content**, introduzca el siguiente contenido:

```
{
        "Version": "1.1",
        "Statement": [
                {
                        "Action": [
                                "iam:agencies:assume"
                        ],
                        "Resource": {
                                "uri": [
                                        "/iam/agencies/
b36b1258b5dc41a4aa8255508xxx..."
                                ]
                        },
                        "Effect": "Allow"
                }
        ]
}
```

   NOTA

   - Reemplace *b36b1258b5dc41a4aa8255508xxx...* con la identificación de la delegación obtenida de una parte delegada. No haga ningún otro cambio.
   - Para obtener más información acerca de los permisos, consulte **5 Gestión de permisos**.

   e. Haga clic en **Next**.
6. Seleccione la política creada en el paso anterior o el rol de **Agent Operator** y haga clic en **Next**.
   - Política personalizada: permite a un usuario gestionar recursos solo para una delegación específica.
   - Rol de **Agent Operator**: Permite a un usuario gestionar recursos para todas las delegaciones.
7. Especifique el ámbito de autorización.
8. Haga clic en **OK**.

Paso 2 Cree un usuario de IAM y agregue el usuario al grupo de usuarios.

1. En la página **Users**, haga clic en **Create User**.
2. En la página **Create User**, introduzca un nombre de usuario.
3. Seleccione **Management console access** para **Access Type** y, a continuación, seleccione **Set by user** para **Credential Type**.

4. Habilite la protección de inicio de sesión y haga clic en **Next**.
5. Seleccione el grupo de usuarios creado en **Paso 1** y haga clic en **Create**.

NOTA

Una vez completada la autorización, el usuario de IAM puede cambiar a la cuenta de la parte delegada y gestionar recursos específicos bajo la cuenta.

----Fin

Operaciones relacionadas

La cuenta delegada o los usuarios de IAM autorizados pueden **cambiar sus roles** a la cuenta delegada para ver y usar sus recursos.

7.1.4 Cambio de roles (por una parte delegada)

Cuando una cuenta establece una relación de confianza con su cuenta, usted se convierte en una parte delegada. Los usuarios de IAM a los que se conceden permisos de delegación pueden cambiar a la cuenta de delegación y gestionar los recursos de la cuenta en función de los permisos concedidos.

Prerrequisitos

- Se ha establecido una relación de confianza entre su cuenta y otra cuenta.
- Usted ha obtenido el nombre de la cuenta delegada y el nombre de delegación.

Procedimiento

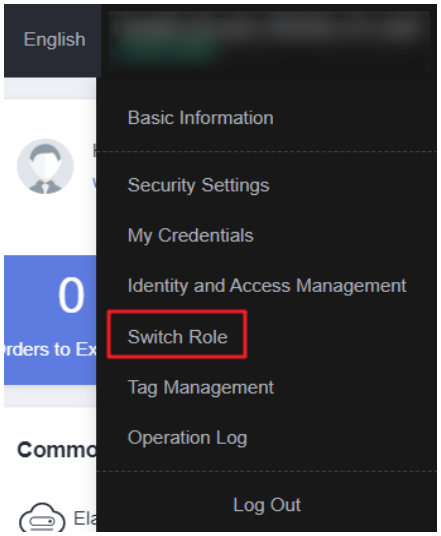
Paso 1 Inicie sesión en la consola de Huawei Cloud con su cuenta o inicie sesión como el usuario de IAM creado en **Paso 2**.

NOTA

El usuario de IAM creado en **Paso 2** de **7.1.3 (Opcional) Asignación de permisos a un usuario de IAM (por una parte delegada)** puede cambiar roles para gestionar recursos para la parte delegada.

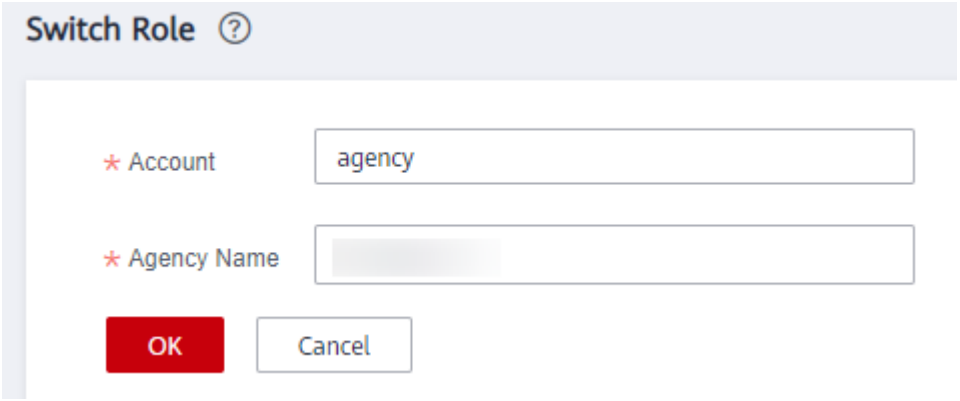
Paso 2 Pase el puntero del ratón sobre el nombre de usuario en la esquina superior derecha y elija **Switch Role**.

Figura 7-6 Cambiar el rol



Paso 3 En la página **Switch Role**, introduzca el nombre de cuenta de la parte delegada.

Figura 7-7 Introducir el nombre de la cuenta y el nombre de la delegación de la parte delegada



NOTA

Después de introducir el nombre de dominio de cuenta, las delegaciones creadas bajo esta cuenta se mostrarán automáticamente después de hacer clic en el cuadro de texto nombre de la delegación. Seleccione uno autorizado de la lista desplegable.

Paso 4 Haga clic en **OK** para cambiar a la cuenta de delegación.

----Fin

Acciones posteriores

Para volver a su propia cuenta, coloque el puntero del ratón sobre el nombre de usuario en la esquina superior derecha, elija **Switch Role** y seleccione su cuenta.

7.2 Delegación de servicios en la nube

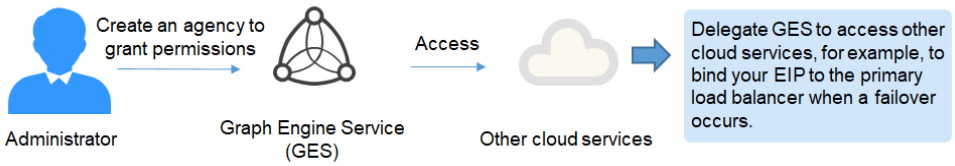
Los servicios de Huawei Cloud interactúan entre sí, y algunos servicios en la nube dependen de otros servicios. Para delegar un servicio en la nube para acceder a otros servicios y realizar O&M de recursos, cree una agencia para el servicio.

IAM proporciona dos métodos para crear una delegación de servicios en la nube:

1. **Creación de una delegación de servicios en la nube en la consola IAM**

   Por ejemplo, cree una delegación para Graph Engine Service (GES) y concédale permisos para vincular su EIP al balanceo de carga principal si se produce una conmutación por error.

Figura 7-8 Delegación de servicios en la nube



2. Creación automática de una agencia de servicios en la nube para utilizar ciertos recursos

   A continuación, se toma Scalable File Service (SFS) como ejemplo para describir el procedimiento para crear automáticamente una delegación de servicios en la nube:

   a. Vaya a la consola SFS.
   b. En la página **Create File System**, habilite encriptación de datos estáticos.
   c. Aparece un cuadro de diálogo en el que se le solicita que confirme la creación de una delegación SFS. Después de hacer clic en **OK**, el sistema crea automáticamente una delegación SFS con permisos **KMS CMKFullAccess** para el proyecto actual. Con la delegación, SFS puede obtener claves KMS para cifrar o descifrar sistemas de archivos.
   d. Puede ver la delegación en la lista de delegación en la consola IAM.

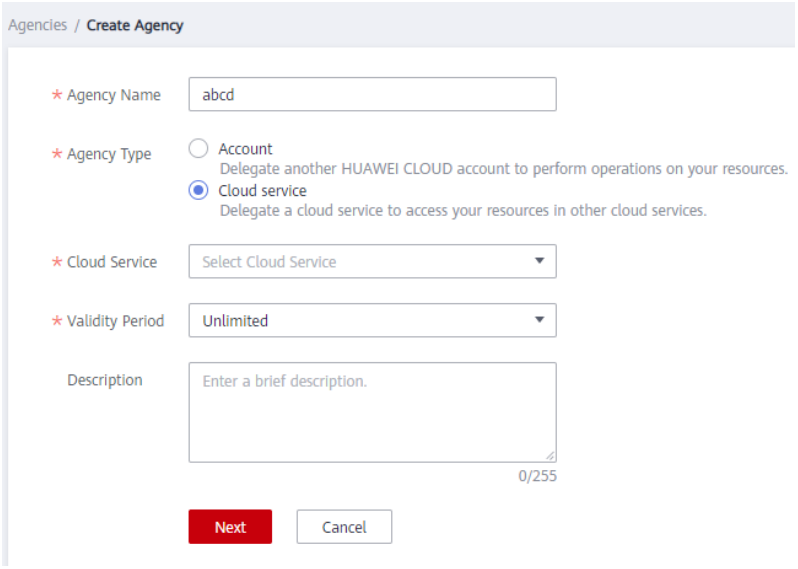
Creación de una delegación de servicios en la nube en la consola IAM

Paso 1 Inicie sesión en la **consola de IAM**.

Paso 2 En la consola de IAM, seleccione **Agencies** en el panel de navegación y haga clic en **Create Agency**.

Paso 3 Ingrese el nombre de una delegación.

Figura 7-9 Nombre de la delegación de servicios en la nube



Paso 4 Seleccione el tipo de delegación de **Cloud service** y, a continuación, seleccione un servicio.

Paso 5 Seleccione un período de validez.

Paso 6 (Opcional) Ingrese una descripción para la delegación para facilitar la identificación.

Paso 7 Haga clic en **Next**.

Paso 8 Seleccione los permisos que se asignarán a la agencia, haga clic en **Next** y especifique el ámbito de autorización.

Paso 9 Haga clic en **OK**.

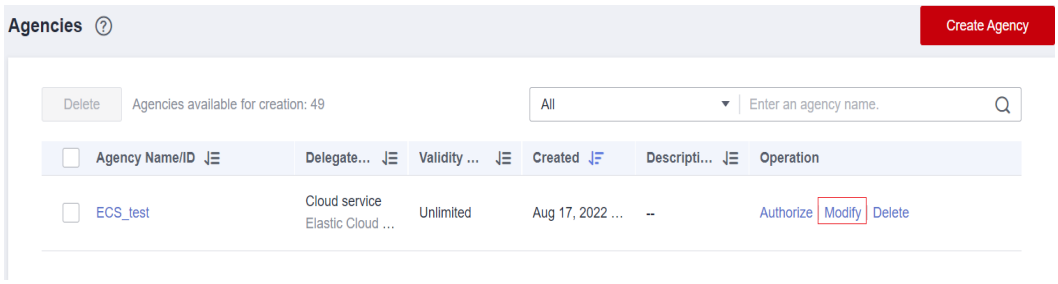
----Fin

7.3 Eliminación o modificación de delegaciones

Modificación de una delegación

Para modificar los permisos, el período de validez y la descripción de una agencia, haga clic en **Modify** en la fila que contiene la agencia que desea modificar.

Figura 7-10 Modificación de una delegación



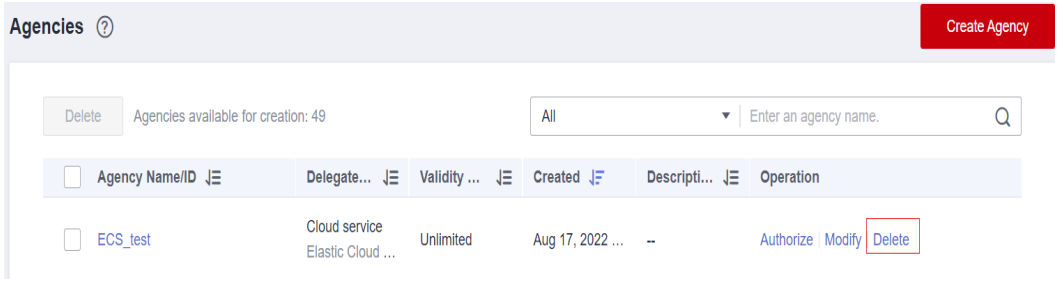
NOTA

- Puede cambiar el servicio en la nube, el período de validez, la descripción y los permisos de las agencias de servicios en la nube, pero no puede cambiar el nombre y el tipo de delegación.
- La modificación de los permisos de las agencias de servicios en la nube puede afectar el uso de ciertas funciones de los servicios en la nube. Tenga cuidado cuando realice esta operación.

Eliminación de una delegación

Para eliminar una agencia, haga clic en **Delete** en la fila que contiene la agencia que se va a eliminar y haga clic en **Yes**.

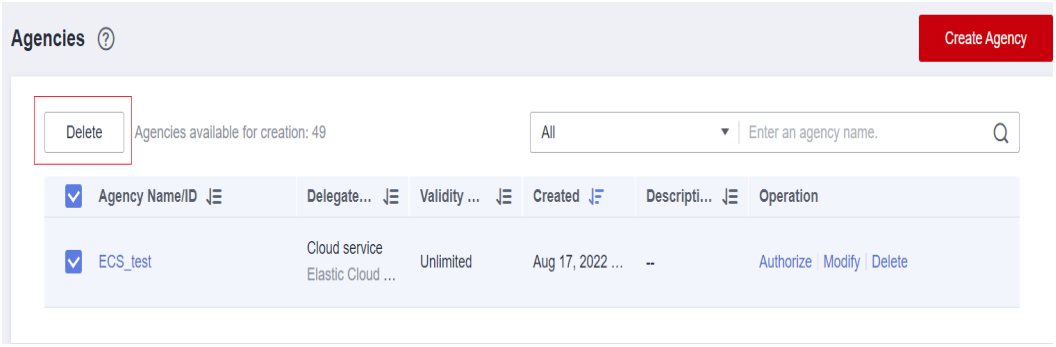
Figura 7-11 Eliminación de una delegación



Eliminación de delegaciones por lotes

Para eliminar varias agencias, seleccione las agencias que se van a eliminar en la lista y haga clic en **Delete** encima de la lista.

Figura 7-12 Eliminación de delegaciones por lotes



NOTA

Después de eliminar una delegación, se revocarán todos los permisos concedidos a las cuentas delegadas.

8 Configuraciones de seguridad

8.1 Descripción general de configuración de seguridad

Puede configurar la configuración de la cuenta, la protección de operaciones críticas, la política de autenticación de inicio de sesión, la política de contraseñas y la lista de control de acceso (ACL) en la página **Security Settings**. Para obtener más información, consulte **8.2 Información básica**, **8.3 Protección de operaciones críticas**, **8.4 Política de autenticación de inicio de sesión**, **8.5 Política de contraseñas** y **8.6 ACL**. En este capítulo se describe cómo acceder a la página **Security Settings** y quién es el público deseado.

Destinatarios

Tabla 8-1 enumera el público previsto de las diferentes funciones proporcionadas en la página **Security Settings** y sus permisos de acceso para las funciones.

Tabla 8-1 Destinatarios

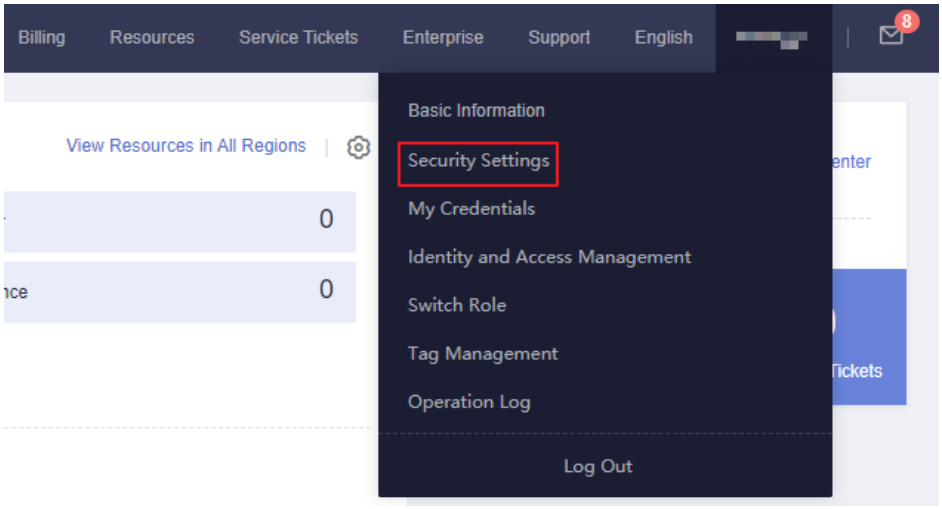
Función	Destinatarios
Información básica	● Usuarios de IAM: Full access ● Cuenta: Para cambiar la información básica, consulte **Gestión de información básica**.
Operaciones Críticas	● **Administrador**: Full access ● Usuarios de IAM: No access

Función	Destinatarios
Política de autenticación de inicio de sesión	● **Administrador**: Full access ● Usuarios de IAM: Read-only access
Política de Contraseña	● **Administrador**: Full access ● Usuarios de IAM: Read-only access
ACL	● **Administrador**: Full access ● Usuarios de IAM: No access

Acceso a la página Security Settings

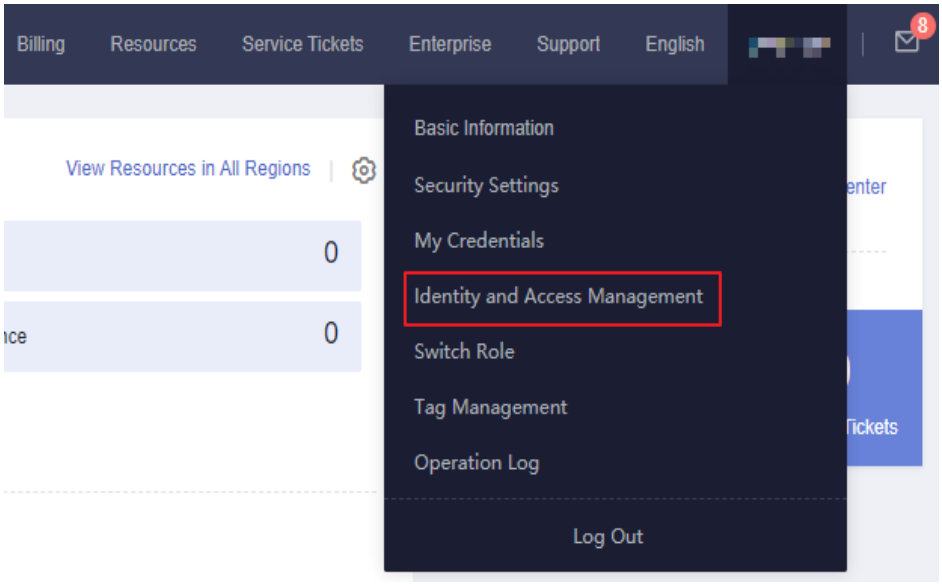
- Usted y todos los usuarios de IAM creados con su cuenta pueden acceder a la página **Security Settings** desde la consola de gestión.
  a. Inicie sesión en Huawei Cloud y haga clic en **Console** en la esquina superior derecha.
  b. En la consola de gestión, coloque el puntero del ratón sobre el nombre de usuario en la esquina superior derecha y elija **Security Settings** en la lista desplegable.

  Figura 8-1 Ir a la página de configuración de seguridad



- Como **administrador**, también puede acceder a la página **Security Settings** desde la consola de IAM.
  a. Inicie sesión en Huawei Cloud y haga clic en **Console** en la esquina superior derecha.
  b. En la consola de gestión, coloque el puntero del ratón sobre el nombre de usuario en la esquina superior derecha y elija **Identity and Access Management** en la lista desplegable.

Figura 8-2 Acceso al servicio IAM



c. En la consola de IAM, seleccione **Security Settings** en el panel de navegación.

8.2 Información básica

Como administrador de cuentas, tanto usted como sus usuarios de IAM pueden gestionar la información básica en esta página. También puede cambiar su contraseña de inicio de sesión, número de teléfono móvil y dirección de correo electrónico al referirse a **Gestión de información de ID de HUAWEI**.

NOTA

- Un número de teléfono móvil o una dirección de correo electrónico solo pueden vincularse a una cuenta o usuario de IAM.
- Solo un número de teléfono móvil, dirección de correo electrónico, y MFA virtual pueden vincularse a una cuenta o a un usuario de IAM.

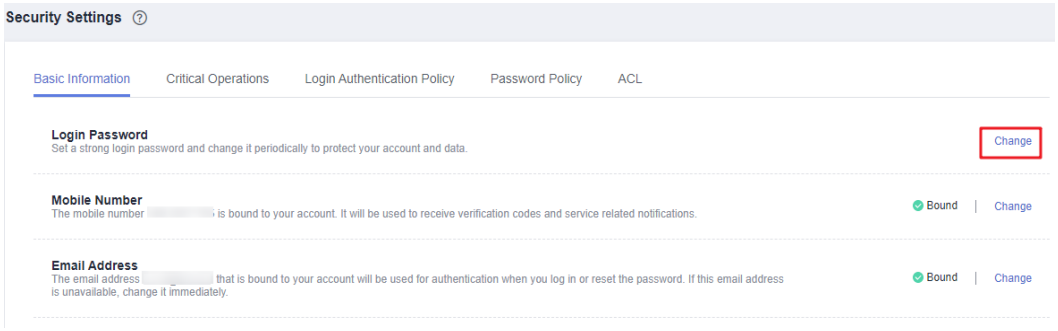
Cambiar la contraseña de inicio de sesión, el número de celular, o la dirección de correo electrónico

Los métodos para cambiar la contraseña de inicio de sesión, el número de celular, y la dirección de correo electrónico son similares. Para cambiar la contraseña de inicio de sesión, haga lo siguiente:

Paso 1 Vaya a la página **Security Settings**.

Paso 2 Haga clic en la pestaña **Basic Information** y haga clic en **Change** en la fila **Login Password**.

Figura 8-3 Cambio de la contraseña de inicio de sesión



Paso 3 (Opcional) Seleccione la dirección de correo electrónico o la verificación del número de teléfono móvil e introduzca el código de verificación.

NOTA

Si ni la dirección de correo electrónico ni el número de teléfono móvil están vinculados, no se requiere verificación.

Paso 4 Ingrese la contraseña antigua y la nueva contraseña, e ingrese la nueva contraseña de nuevo.

NOTA

- La contraseña no puede ser el nombre de usuario o el nombre de usuario escrito al revés. Por ejemplo, si el nombre de usuario es **A12345**, la contraseña no puede ser **A12345**, **a12345**, **54321A**, o **54321a**.
- Para evitar la grieta de la contraseña, el administrador puede configurar la política de contraseñas para definir los requisitos de contraseña, como la longitud mínima de la contraseña. Para obtener más información, véase **8.5 Política de contraseñas**.

Paso 5 Haga clic en **OK**.

----Fin

8.3 Protección de operaciones críticas

Solo un **administrador** puede configurar la protección de operaciones críticas y los usuarios de IAM solo pueden ver las configuraciones. Si un usuario de IAM necesita modificar las configuraciones, el usuario puede solicitar al administrador que realice la modificación o conceder los permisos necesarios.

NOTA

Los usuarios federados no necesitan verificar su identidad cuando realizan operaciones críticas.

Dispositivo MFA virtual

Un dispositivo MFA genera códigos de verificación de 6 dígitos de acuerdo con el algoritmo de contraseña de un solo uso basado en tiempo (TOTP). Los dispositivos MFA pueden estar basados en hardware o software. Actualmente, solo se admiten dispositivos MFA virtuales basados en software, y son programas de aplicación que se ejecutan en dispositivos inteligentes como teléfonos móviles.

Esta sección describe cómo vincular un dispositivo MFA virtual, por ejemplo, la aplicación de Huawei Cloud. Si ha instalado otra aplicación MFA, agregue un usuario siguiendo las

indicaciones en pantalla. Para obtener más información sobre cómo enlazar o quitar un dispositivo MFA virtual, consulte **11.2 Dispositivo MFA virtual**.

El método para vincular un dispositivo MFA virtual varía dependiendo de si su cuenta de Huawei Cloud se ha actualizado a un ID de HUAWEI.

NOTA

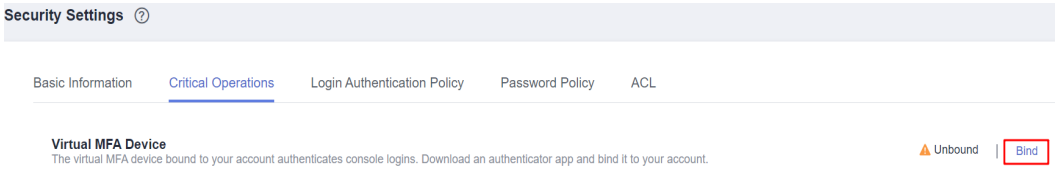
Antes de vincular un dispositivo MFA virtual, asegúrese de haber instalado una aplicación MFA (como una aplicación Authenticator) en su dispositivo móvil.

- **Cuenta de Huawei Cloud**

Paso 1 Vaya a la página **Configuración de seguridad**.

Paso 2 Haga clic en la pestaña **Critical Operations** y haga clic en **Bind** en la fila **Virtual MFA Device**.

Figura 8-4 Dispositivo MFA virtual



Paso 3 Configure la aplicación MFA escaneando el código QR o introduciendo manualmente la clave secreta.

Puede vincular un dispositivo MFA virtual a su cuenta escaneando el código QR o introduciendo la clave secreta.

- Escanear el código QR

  Abra la aplicación MFA en su teléfono móvil y utilice la aplicación para escanear el código QR que se muestra en la página **Bind Virtual MFA Device**. Su cuenta o usuario de IAM se agrega a la aplicación.

- Introducir manualmente la clave secreta

  Abra la aplicación MFA en su teléfono móvil e introduzca la clave secreta.

  NOTA

  El usuario solo se puede agregar manualmente utilizando contraseñas de un solo uso basadas en el tiempo (TOTP). Se recomienda activar la configuración automática de la hora en su teléfono móvil.

Paso 4 Vea los códigos de verificación en la aplicación MFA. El código se actualiza automáticamente cada 30 segundos.

Paso 5 En la página **Bind Virtual MFA Device**, introduzca dos códigos de verificación consecutivos y haga clic en **OK**.

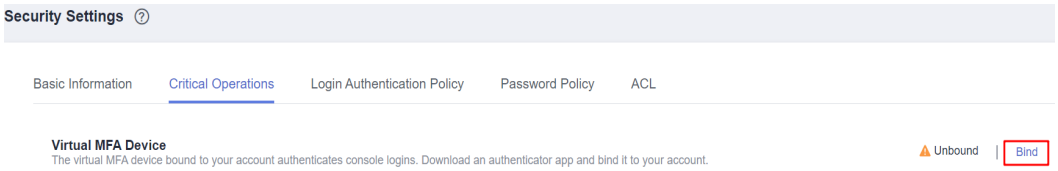
----Fin

- **HUAWEI ID**

Paso 1 Vaya a la página **Configuración de seguridad**.

Paso 2 Haga clic en la pestaña **Critical Operations** y haga clic en **Bind** en la fila **Virtual MFA Device**.

Figura 8-5 Vinculación de un dispositivo MFA virtual



Paso 3 En la página de **Account & security** del centro de cuentas de ID de HUAWEI, asocie un autenticador con su ID de HUAWEI según las instrucciones.

----Fin

Protección de inicio de sesión

Después de habilitar la protección de inicio de sesión, usted y los usuarios de IAM creados con su cuenta deberán ingresar un código de verificación además del nombre de usuario y la contraseña durante el inicio de sesión. Habilite esta función para la seguridad de la cuenta.

Para la cuenta, solo el administrador de la cuenta puede habilitar la protección de inicio de sesión para ella. Para los usuarios de IAM, tanto el administrador de la cuenta como otros administradores pueden habilitar esta función para los usuarios.

- **(Administrador) Habilitar la protección de inicio de sesión para un usuario de IAM**

  Para habilitar la protección de inicio de sesión para un usuario de IAM, vaya a la página **Users** y elija **More** > **Security Settings** en la fila que contiene el usuario de IAM. En el área **Login Protection** de sesión en la pestaña **Security Settings** mostrada, haga clic en

  junto a **Verification Method** y seleccione un método de verificación de SMS, correo electrónico o dispositivo MFA virtual.

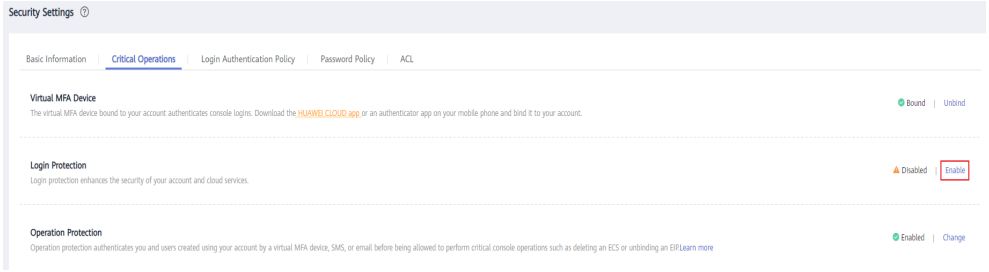
  NOTA

  Después de habilitar la protección de inicio de sesión, los usuarios de IAM deben realizar una verificación de identidad cuando acceden a Huawei Cloud mediante la consola de gestión. La configuración no se aplica si los usuarios de IAM usan acceso mediante programación.

- **Activar la protección de inicio de sesión para su cuenta de Huawei Cloud**

  Si su cuenta de Huawei Cloud no se ha actualizado a un ID de HUAWEI, puede habilitar la protección de inicio de sesión en la página **Security Settings**. Vaya a la página **Security Settings** y haga clic en la pestaña **Critical Operations**. Haga clic en **Enable** junto a **Login Protection**, seleccione un método de verificación, introduzca el código de verificación y haga clic en **OK**.

  Figura 8-6 Habilitación de la protección de inicio de sesión

- **Habilitar la protección de inicio de sesión para su ID de HUAWEI**

Si su cuenta de Huawei Cloud se ha actualizado a un ID de HUAWEI, habilite la protección de inicio de sesión en el centro de cuentas de ID de HUAWEI. Vaya al **centro de cuentas de ID de HUAWEI**, seleccione **Account & security**, busque **Two-step verification** en el área **Security verification**, haga clic en **ENABLE**, complete la verificación y haga clic en **OK**.

El sistema autentica tu identidad cuando inicias sesión con un ID de HUAWEI. Si utiliza un nuevo terminal para iniciar sesión, se autenticará con su número de teléfono de seguridad en el primer inicio de sesión. Si la verificación en dos pasos no está habilitada, haga clic en **Trust** para agregar su terminal a la lista de confianza. Entonces ya no necesitará realizar autenticación cuando inicie sesión con este terminal la próxima vez.

Protección de operaciones

- **Habilitación de la protección de la operación**

  Después de habilitar la protección de operaciones, usted y los usuarios de IAM creados con su cuenta deben introducir un código de verificación al realizar una **operación crítica**, como la eliminación de un ECS. Esta función está habilitada por defecto. Para garantizar la seguridad de los recursos, manténgala habilitada.

  La verificación es válida durante 15 minutos y no es necesario que se vuelva a verificar al realizar operaciones críticas dentro del período de validez.

Paso 1 Vaya a la página **Security Settings**.

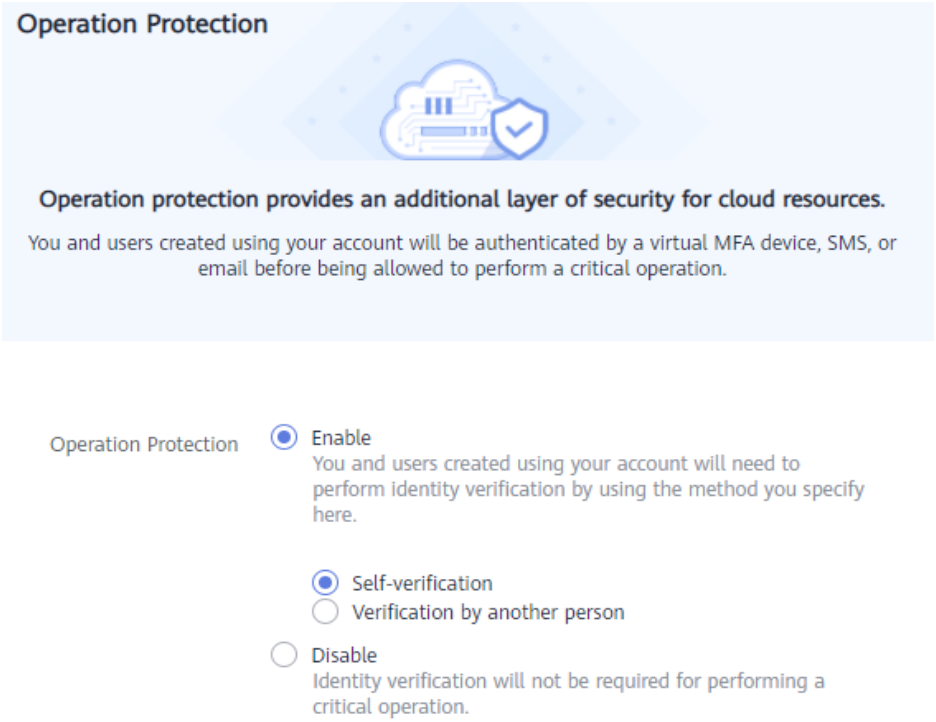
Paso 2 En la pestaña **Critical Operations**, busque la fila **Operation Protection** y haga clic en **Enable**.

Figura 8-7 Habilitación de la protección de la operación

Paso 3 Seleccione **Enable** y, a continuación, seleccione **Self-verification** o **Verification by another person**.

Si selecciona **Verification by another person**, se requiere una verificación de identidad para asegurarse de que este método de verificación está disponible.

Figura 8-8 Configuración de la protección de la operación



- **Self-verification**: Usted o los propios usuarios de IAM realizan la verificación cuando realizan una operación crítica.
- **Verification by another person**: La persona especificada completa la verificación cuando usted o los usuarios de IAM realizan una operación crítica. Solo se admite la verificación por SMS y correo electrónico.

Paso 4 Haga clic en **OK**.

----Fin

- **Deshabilitación de la protección de operación**

Si la protección de la operación está deshabilitada, usted y los usuarios de IAM creados con su cuenta no necesitan introducir un código de verificación al realizar una **operación crítica**.

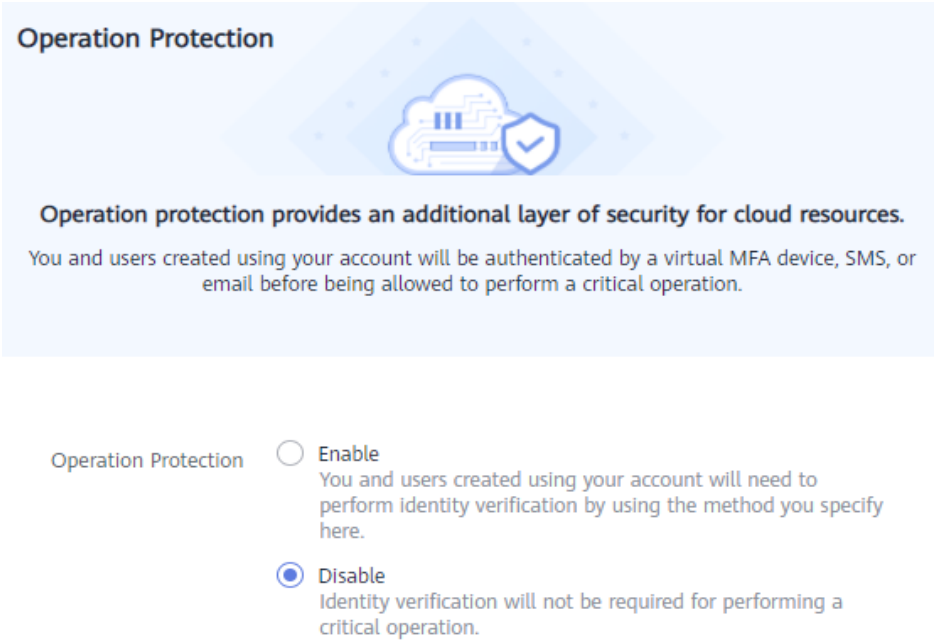
Paso 1 Vaya a la página **Security Settings**.

Paso 2 En la pestaña **Critical Operations**, busque la fila **Operation Protection** y haga clic en **Change**.

Figura 8-9 Deshabilitación de la protección de operaciones

Paso 3 Seleccione **Disable** y haga clic en **OK**.

Figura 8-10 Deshabilitación de la protección de operaciones



Paso 4 Ingrese un código de verificación.

- **Self-verification**: El administrador que desea deshabilitar la protección de operación completa la verificación. Se admite la verificación de SMS, correo electrónico y MFA virtual.
- **Verification by another person**: La persona especificada completa la verificación. Solo se admite la verificación por SMS y correo electrónico.

Paso 5 Haga clic en **OK**.

----Fin

NOTA

- Cada servicio en la nube define sus propias operaciones críticas.
- Cuando los usuarios de IAM creados con su cuenta realizan una operación crítica, se les pedirá que elijan un método de verificación de correo electrónico, SMS y dispositivo MFA virtual.
  - Si un usuario solo está asociado con un número de móvil, sólo está disponible la verificación por SMS.
  - Si un usuario solo está asociado con una dirección de correo electrónico, solo está disponible la verificación por correo electrónico.
  - Si un usuario no está asociado con una dirección de correo electrónico, número móvil o dispositivo MFA virtual, el usuario necesitará asociar al menos uno de ellos antes de que el usuario pueda realizar cualquier operación crítica.
- Es posible que no pueda recibir códigos de verificación de correo electrónico o SMS debido a errores de comunicación. En este caso, se recomienda utilizar un dispositivo MFA virtual para la verificación.
- **Puede cambiar el número de celular o la dirección de correo electrónico en My Account y cambiar el dispositivo virtual MFA en la página de Security Settings de la consola de IAM.**
- Si la protección de operación está habilitada, los usuarios de IAM deben introducir códigos de verificación cuando realizan una operación crítica. Los códigos de verificación se envían al número móvil o a la dirección de correo electrónico vinculada a los usuarios de IAM.

Gestión de claves de acceso

- **Habilitación de la gestión de claves de acceso**

  Después de habilitar la gestión de claves de acceso, solo el administrador puede crear, habilitar, deshabilitar o eliminar claves de acceso de los usuarios de IAM. Esta función está deshabilitada por defecto. Para garantizar la seguridad de los recursos, habilite esta función.

  Para habilitar la gestión de claves de acceso, haga clic en la pestaña **Critical Operations** de la página **Security Settings** y haga clic en  en la fila **Access Key Management**.

- **Deshabilitación de la gestión de claves de acceso**

  Después de deshabilitar la gestión de claves de acceso, todos los usuarios de IAM pueden crear, habilitar, deshabilitar o eliminar sus propias claves de acceso.

  Para habilitar la gestión de claves de acceso, haga clic en la pestaña **Critical Operations** de la página **Security Settings** y haga clic en  en la fila **Access Key Management**.

Autogestión de la información

- **Habilitación de la autogestión de la información**

  De forma predeterminada, la autogestión de la información está habilitada, lo que indica que todos los usuarios de IAM pueden gestionar su propia **información básica** (contraseña de inicio de sesión, número de teléfono móvil y dirección de correo electrónico). Determinar si permitir que los usuarios de IAM gestionen su propia información y qué información pueden modificar.

  Para habilitar la autogestión de la información, haga clic en la pestaña **Critical Operations** de la página **Configuración de seguridad**, y haga clic en **Enable** junto a **Information Self-Management**. Seleccione **Enable**, seleccione los tipos de información que los usuarios de IAM pueden modificar y haga clic en **OK**.

- **Deshabilitación de la autogestión de la información**

  Después de deshabilitar la autogestión de la información, solo los administradores pueden gestionar su propia **información básica**. Si los usuarios de IAM necesitan modificar su contraseña de inicio de sesión, número de teléfono móvil o dirección de correo electrónico, pueden ponerse en contacto con el administrador. Para obtener más información, véase **3.4 Consulta o modificación de información de usuario de IAM**.

  Para deshabilitar la autogestión de información, haga clic en la pestaña **Operaciones críticas** de la página **Configuración de seguridad** y haga clic en **Change** en la fila **Information Self-Management**. En el panel mostrado, seleccione **Disable** y haga clic en **OK**.

Operaciones críticas

En las siguientes tablas se enumeran las operaciones críticas definidas por cada servicio en la nube.

Tabla 8-2 Operaciones críticas definidas por los servicios en la nube

Categoría de servicio	Servicio	Operación crítica
Cómputo	Elastic Cloud Server (ECS)	● Detener, reiniciar o eliminar un ECS ● Restablecimiento de la contraseña del inicio de sesión de un ECS ● Separación de un disco ● Desvinculación de una EIP
	Bare Metal Server (BMS)	● Detener o reiniciar un BMS ● Restablecimiento de la contraseña del BMS ● Separación de un disco ● Desvinculación de una EIP
	Auto Scaling (AS)	Eliminación de un grupo de AS
Almacenamiento	Object Storage Service (OBS)	● Eliminación de un bucket ● Creación, edición o eliminación de una política de bucket ● Configuración de una política de objeto ● Creación, edición o eliminación de una ACL de bucket ● Configuración del registro de acceso ● Configuración de la validación de URL ● Creación o edición de un inventario de buckets
	Elastic Volume Service (EVS)	Eliminación de un disco EVS
	Cloud Backup and Recovery (CBR)	● Eliminación de un almacén ● Eliminación de una copia de respaldo ● Restauración de una copia de respaldo ● Eliminación de una política ● Disociación de un recurso ● Aceptación de una copia de respaldo
CDN y Intelligent Edge	Content Delivery Network (CDN)	Configuración de la política de terminación del servicio
Contenedores	Cloud Container Engine (CCE)	Eliminación de un clúster
	Application Orchestration Service (AOS)	Eliminación de una pila

Categoría de servicio	Servicio	Operación crítica
Red	Domain Name Service (DNS)	● Modificación, deshabilitación o eliminación de un conjunto de registros ● Modificación o eliminación de un registro PTR ● Eliminación de una línea personalizada
	Virtual Private Cloud (VPC)	● Liberación o desvinculación de una EIP ● Eliminación de una interconexión de VPC ● Operaciones de grupo de seguridad – Eliminación de una regla entrante o saliente – Modificación de una regla entrante o saliente – Eliminación de reglas entrantes o salientes
	Elastic Load Balance (ELB)	● Balanceador de carga compartidos – Eliminación de un balanceador de carga – Eliminación de un oyente – Eliminación de un certificado – Eliminación de un servidor backend – Desvinculación de una EIP – Desvinculación de una dirección IPv4 pública o privada ● Balanceadores de carga dedicados – Eliminación de un balanceador de carga – Eliminación de un oyente – Eliminación de un certificado – Eliminación de un servidor backend – Desvinculación de una EIP – Desvinculación de una dirección IPv4 pública o privada – Desvinculación de una dirección IPv6 – Eliminación del ancho de banda compartido IPv6
	Elastic IP (EIP)	● Eliminación de un ancho de banda compartido ● Liberación o desvinculación de una EIP ● Liberación o desvinculación de las EIP
Red	Virtual Private Network (VPN)	● Eliminación de una conexión VPN ● Cancelación de la suscripción de un gateway de VPN anual/mensual

Categoría de servicio	Servicio	Operación crítica
Seguridad & Cumplimiento	SSL Certificate Manager (SCM)	● Eliminación de un certificado ● Revocación de un certificado
Gestión & Gobernanza	Identity and Access Management (IAM)	● Deshabilitación de la protección de operaciones ● Deshabilitación de la protección de inicio de sesión ● Cambio del número de teléfono móvil ● Cambio de la dirección de correo electrónico ● Cambio de la contraseña de inicio de sesión ● Cambio del método de autenticación de inicio de sesión ● Eliminación de un usuario de IAM ● Deshabilitación de un usuario de IAM ● Eliminación de una delegación ● Eliminación de un grupo de usuarios ● Eliminación de una política ● Eliminación de permisos ● Creación de una clave de acceso ● Eliminación de una clave de acceso ● Desactivación de una clave de acceso ● Eliminación del proyecto ● Modificación del estado de la gestión de claves de acceso
Gestión & Gobernanza	Cloud Trace Service (CTS)	Deshabilitación de un rastreador del sistema
Gestión & Gobernanza	Log Tank Service (LTS)	● Eliminación de un flujo de registro o grupo de registro ● Desinstalación del ICAgent
Aplicación	Distributed Cache Service (DCS)	● Restablecimiento de la contraseña de una instancia DCS ● Eliminación de una instancia de DCS ● Eliminación de datos de instancia de DCS
Nube dedicada	Dedicated Distributed Storage Service (DSS)	Eliminación de un disco

Categoría de servicio	Servicio	Operación crítica
Base de datos	RDS for MySQL	● Restablecimiento de la contraseña del administrador ● Eliminación de una instancia de base de datos ● Eliminación de una copia de respaldo de base de datos ● Restauración de una instancia de base de datos existente desde un archivo de copia de respaldo ● Restauración de una instancia de base de datos existente a un punto en el tiempo ● Cambio entre instancias de base de datos primarias y en espera ● Cambio del puerto de la base de datos ● Eliminación de cuenta de base de datos ● Eliminación de una base de datos ● Cambio de una dirección IP flotante ● Desvinculación de una EIP ● Descarga de una copia de respaldo completa
Base de datos	RDS for PostgreSQL	● Restablecimiento de la contraseña del administrador ● Eliminación de una instancia de base de datos ● Eliminación de una copia de respaldo de base de datos ● Cambio entre instancias de base de datos primarias y en espera ● Cambio del puerto de la base de datos ● Cambio de una dirección IP flotante ● Desvinculación de una EIP ● Descarga de una copia de respaldo completa

Categoría de servicio	Servicio	Operación crítica
Base de datos	GaussDB(for MySQL)	● Eliminación de una instancia de base de datos ● Reinicio de una instancia de base de datos ● Reinicio de un nodo ● Eliminación de una réplica de lectura ● Desvinculación de una EIP ● Eliminación de una base de datos ● Restablecimiento de una contraseña para una cuenta de base de datos ● Eliminación de cuenta de base de datos ● Restablecimiento de la contraseña del administrador ● Cambio de un nombre de dominio privado ● Cambio de una dirección IP privada ● Restauración de datos a un punto específico en el tiempo
Bases de datos	Document Database Service (DDS)	● Restablecimiento de la contraseña ● Reinicio o eliminación de una instancia de base de datos ● Reinicio de un nodo ● Cambio de los nodos primario y secundario de un conjunto de réplicas ● Eliminación de una regla de grupo de seguridad ● Habilitación de direcciones IP de nodos shard y config ● Restauración de la instancia de base de datos actual desde una copia de respaldo ● Restauración de una instancia de base de datos existente a partir de una copia de respaldo ● Cambio de una instancia anual/mensual a pago por uso
Inteligencia empresarial	Data Warehouse Service (DWS)	● Escalamiento o cambio del tamaño de un clúster ● Reinicio de un clúster ● Reparación de un nodo ● Restablecimiento de la contraseña

Categoría de servicio	Servicio	Operación crítica
	MapReduce Service (MRS)	● Clústeres – Eliminación de un clúster – Cambio de un clúster de pago por uso a facturación anual/mensual – Detener todos los componentes – Sincronización de configuraciones de clúster ● Nodos – Detener todos los roles – Aislamiento de un host – Cancelación del aislamiento de un host ● Componentes – Deshabilitación de un servicio – Reinicio de un servicio – Realización de un reinicio de servicio continuo – Detener una instancia de rol – Reinicio de una instancia de rol – Realización de un reinicio continuo de instancia – Reiniciación de una instancia de rol – Retiración del servicio de una instancia de rol – Guardar configuraciones de servicio ● Parches – Instalación de un parche – Desinstalación de un parche – Retroceder un parche
Comunicaciones en la nube	Message&SMS	● Eliminación de una firma ● Eliminación de una plantilla ● Obtención de una app_secret ● Vinculación de un número de teléfono móvil o una dirección de correo electrónico a su cuenta de Huawei Cloud ● Configuración de una lista blanca de direcciones IP ● Renovación de un paquete

Categoría de servicio	Servicio	Operación crítica
Desarrollo de software DevCloud	Gestión de proyecto (ProjectMan)	• Eliminación de un proyecto • Eliminación de un miembro del proyecto • Modificación de la información del miembro • Modificación o eliminación de permisos • Modificación de la información básica del proyecto • Eliminación de un elemento de trabajo
Soporte para el usuario	Centro de facturación	• Pago por un pedido • Darse de baja de un pedido • Liberación de recursos

8.4 Política de autenticación de inicio de sesión

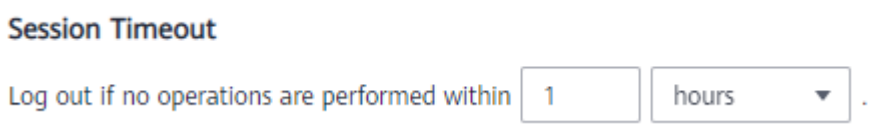
La pestaña **Login Authentication Policy** de la página **Configuración de seguridad** proporciona la **Tiempo de espera de la sesión**, **Bloqueo de la cuenta**, **Deshabilitación de la cuenta**, **Información de inicio de sesión reciente**, y **Información personalizada** configuración. Esta configuración tiene efecto tanto para su cuenta como para los usuarios de IAM creados con la cuenta.

Solo el **administrador** puede configurar la política de autenticación de inicio de sesión y los usuarios de IAM sólo pueden ver las configuraciones. Si un usuario de IAM necesita modificar las configuraciones, el usuario puede solicitar al administrador que realice la modificación o conceder los permisos necesarios.

Tiempo de espera de la sesión

Establezca el tiempo de espera de sesión que se aplicará si usted o los usuarios creados con su cuenta no realizan ninguna operación dentro de un período específico.

Figura 8-11 Tiempo de espera de la sesión

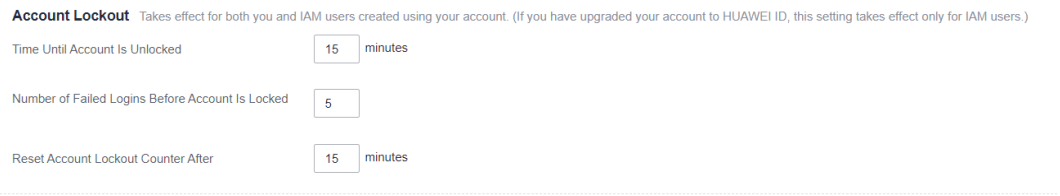


El tiempo de espera varía de 15 minutos a 24 horas, y el tiempo de espera predeterminado es 1 hora.

Bloqueo de la cuenta

Establezca una duración para bloquear a los usuarios si se ha alcanzado un número específico de intentos de inicio de sesión fallidos dentro de un período determinado. No puede desbloquear su propia cuenta o la de un usuario de IAM. Espere hasta que expire el tiempo de bloqueo.

Figura 8-12 Bloqueo de la cuenta



El administrador puede establecer la duración del bloqueo de la cuenta, el número máximo de intentos de inicio de sesión sin éxito antes de bloquear la cuenta y el tiempo para restablecer el contador de bloqueo de la cuenta.

- Duración del bloqueo: El valor oscila entre 15 y 30 minutos y el valor predeterminado es **15 minutes**.
- Número máximo de intentos de inicio de sesión fallidos: el valor varía de 3 a 10, y el valor predeterminado es **5**.
- Tiempo para restablecer el contador de bloqueo de cuenta: El valor varía entre 15 y 60 minutos y el valor predeterminado es **15 minutes**.

Deshabilitación de la cuenta

Establezca un período de validez para deshabilitar a los usuarios de IAM si no han accedido a Huawei Cloud mediante la consola o las API dentro de un período determinado.

Esta opción está deshabilitada de forma predeterminada. El período de validez oscila entre 1 y 240 días.

Si habilita esta opción, la configuración solo tendrá efecto para los usuarios de IAM creados con su cuenta. Si un usuario de IAM está deshabilitado, el usuario puede solicitar al administrador que vuelva a habilitar su cuenta.

Información de inicio de sesión reciente

Configure si desea que el sistema muestre la información de inicio de sesión anterior después de iniciar sesión. Si se muestra información de inicio de sesión incorrecta en la página **Login Verification**, cambie su contraseña inmediatamente.

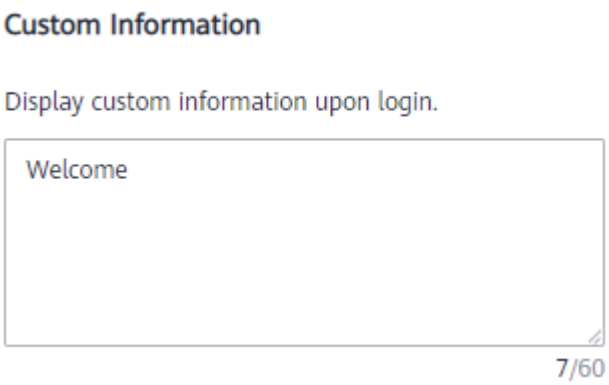
Esta opción está deshabilitada por defecto y puede ser habilitada por el administrador.

Información personalizada

Establezca información personalizada que se mostrará al iniciar sesión correctamente. Por ejemplo, introduzca la palabra **Welcome**.

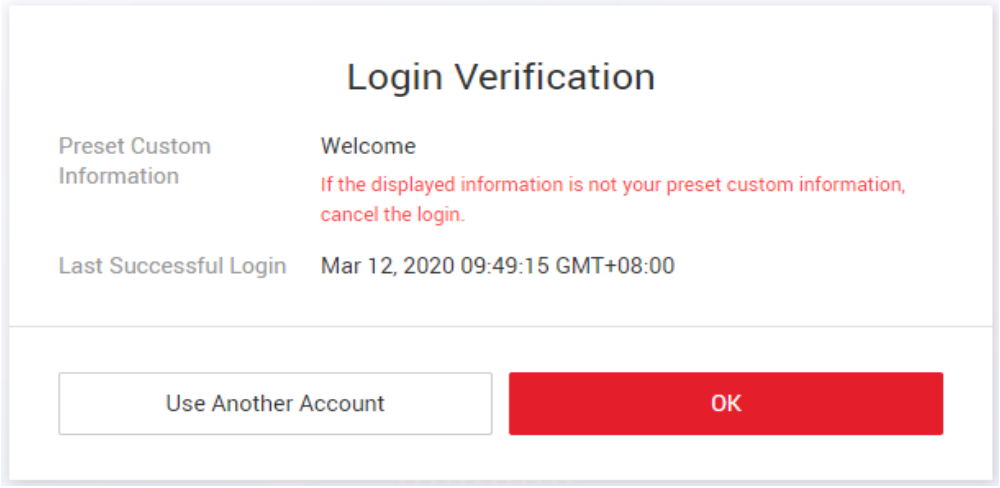
De forma predeterminada, no se muestra ninguna información y el administrador puede establecer la información personalizada que se mostrará.

Figura 8-13 Información personalizada



Usted y todos los usuarios de IAM creados con su cuenta verán la misma información al iniciar sesión correctamente.

Figura 8-14 Verificación de inicio de sesión



8.5 Política de contraseñas

La pestaña **Password Policy** de la página **Security Settings** proporciona la configuración de **Composición de contraseña & Reutilizar**, **Expiración de la contraseña**, y **Período de duración mínimo de la contraseña**.

Solo el **administrador** puede configurar la política de contraseñas y los usuarios de IAM sólo pueden ver las configuraciones. Si un usuario de IAM necesita modificar las configuraciones, el usuario puede solicitar al administrador que realice la modificación o conceder los permisos necesarios.

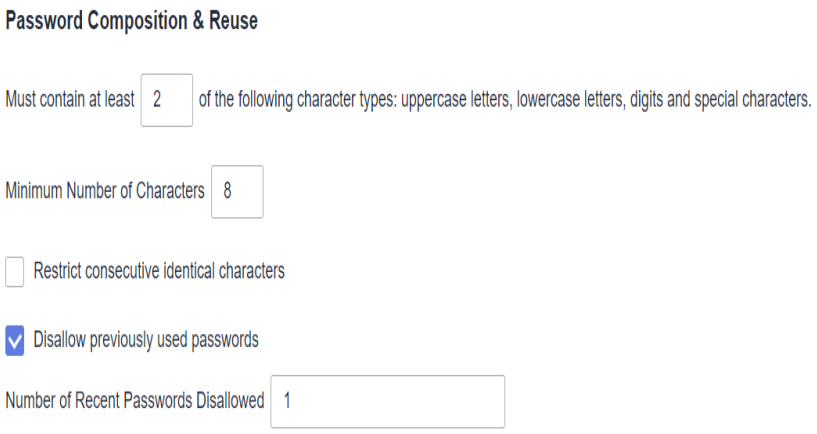
Puede configurar la política de contraseñas para asegurarse de que los usuarios de IAM crean contraseñas seguras y las rotan periódicamente. En la política de contraseñas, puede definir los requisitos de contraseña, como la longitud mínima de la contraseña, si se deben permitir caracteres idénticos consecutivos en una contraseña y si se deben permitir las contraseñas utilizadas anteriormente.

NOTA

Si su cuenta de Huawei Cloud ya se ha actualizado a un ID de HUAWEI, la política de contraseñas no entrará en vigor para el ID.

Composición de contraseña & Reutilizar

Figura 8-15 Composición de contraseña & Reutilizar



- Asegúrese de que la contraseña contiene de 2 a 4 de los siguientes tipos de caracteres: letras mayúsculas, minúsculas, dígitos y caracteres especiales. De forma predeterminada, la contraseña debe contener al menos 2 de estos tipos de caracteres.
- Establezca el número mínimo de caracteres que debe contener una contraseña. El valor predeterminado es 8 y el rango de valores es de 8 to 32.
- (Opcional) Active la opción **Restrict consecutive identical characters** y establezca el número máximo de veces que se permite que un carácter esté presente consecutivamente en una contraseña. Por ejemplo, el valor **1** indica que no se permiten caracteres idénticos consecutivos en una contraseña.
- (Opcional) Habilite la opción **Disallow previously used passwords** y establezca el número de contraseñas usadas anteriormente que no están permitidas. Por ejemplo, el valor **3** indica que el usuario no puede establecer las tres últimas contraseñas que el usuario ha utilizado anteriormente al establecer una nueva contraseña.

Los cambios en la política de contraseñas entrarán en vigor la próxima vez que usted o sus usuarios de IAM cambien las contraseñas. La nueva política de contraseñas también se aplicará a los usuarios de IAM creados posteriormente.

Expiración de la contraseña

Establezca un período de validez de las contraseñas para que los usuarios deban cambiar sus contraseñas periódicamente. Se pedirá a los usuarios que cambien sus contraseñas 15 días antes del vencimiento de la contraseña. Las contraseñas caducadas no se pueden usar para iniciar sesión en la Huawei Cloud.

Esta opción está deshabilitada de forma predeterminada. El período de validez oscila entre 1 y 180 días.

Los cambios entrarán en vigor inmediatamente para su cuenta y para todos los usuarios de IAM bajo su cuenta.

NOTA

Después de que la contraseña caduca, los usuarios deben establecer una nueva contraseña a través de la URL enviada por correo electrónico. La contraseña nueva debe ser diferente a la contraseña anterior.

Período de duración mínimo de la contraseña

Para evitar la pérdida de contraseñas debido a cambios frecuentes de contraseña, puede establecer un período mínimo después del cual se permite a los usuarios realizar un cambio de contraseña.

Esta opción está deshabilitada de forma predeterminada. Si habilita esta opción, puede establecer un período de 0 a 1440 minutos.

Los cambios entrarán en vigor inmediatamente para su cuenta y para todos los usuarios de IAM bajo su cuenta.

8.6 ACL

La pestaña **ACL** de la página **Security Settings** proporciona la configuración y las configuraciones **Rangos de direcciones IP**, **Bloques CIDR IPv4**, y **Puntos de conexión de la VPC** para permitir el acceso del usuario solo desde intervalos de direcciones IP especificados, bloques CIDR IPv4 o puntos de conexión de VPC.

Solo el **administrador** puede configurar la ACL. Si un usuario de IAM necesita configurar la ACL, el usuario puede solicitar al administrador que realice la configuración o que otorgue los permisos necesarios.

Tipo de acceso:

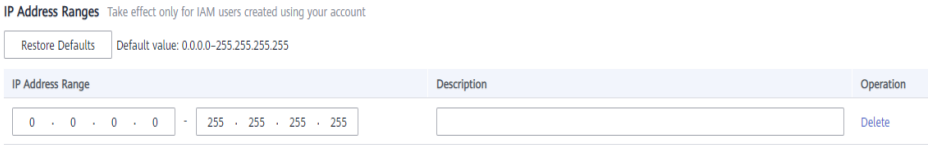
- **Console Access** (recomendado): La ACL solo tiene efecto para los usuarios de IAM y los usuarios federados que se crean con su cuenta y tienen acceso a la consola.
- **API Access**: La ACL controla el acceso a la API de los usuarios a través de API Gateway y solo tiene efecto para usuarios de IAM y usuarios federadosdos horas después de completar la configuración.

NOTA

- Puede configurar un máximo de 200 elementos de control de acceso.
- Si un usuario de IAM o un usuario federado accede a Huawei Cloud a través de un servidor proxy, configure las direcciones IP, los intervalos de direcciones o los bloques CIDR permitidos según la dirección IP del proxy. Si un usuario de IAM o un usuario federado accede a Huawei Cloud a través de una red pública, ajuste en función de la dirección IP pública.

Rangos de direcciones IP

Figura 8-16 Rangos de direcciones IP



Especifique rangos de direcciones IP de 0.0.0.0 a 255.255.255.255 para permitir el acceso a Huawei Cloud. El valor por defecto es **0.0.0.0–255.255.255.255**. Si este parámetro se deja en

blanco o se utiliza el valor predeterminado, los usuarios de IAM pueden acceder a la consola de Huawei Cloud desde cualquier lugar.

Bloques CIDR IPv4

Especifique los bloques CIDR IPv4 para permitir el acceso a Huawei Cloud. Por ejemplo, establezca **IPv4 CIDR block** en **10.10.10.10/32**.

Puntos de conexión de la VPC

Especifique puntos de conexión de VPC, como **0ccad098-b8f4-495a-9b10-613e2a5exxxx**, para permitir el acceso basado en API a Huawei Cloud. Si el control de acceso no está configurado, puede acceder a las API desde todos los puntos finales de VPC de forma predeterminada.

NOTA

- Se permite el acceso del usuario si se cumple cualquiera de **IP Address Ranges**, **IPv4 CIDR Blocks**, y **VPC Endpoints**.
- Para restaurar **IP Address Ranges** a la configuración predeterminada (0.0.0.0–255.255.255.255) y borrar la configuración en **IPv4 CIDR Blocks** y **VPC Endpoints**, haga clic en **Restore Defaults**.

9 Proveedores de identidades

9.1 Introducción

Huawei Cloud proporciona federación de identidades basada en lenguaje de marcado de aserción de seguridad (SAML) o OpenID Connect. Esta función permite a los usuarios de su sistema de gestión empresarial acceder a Huawei Cloud a través del inicio de sesión único (SSO).

Conceptos básicos

Tabla 9-1 Conceptos básicos

Concepto	Descripción
Proveedor de identidad (IdP)	Un IdP recopila y almacena información de identidad del usuario, como nombres de usuario y contraseñas, y autentica a los usuarios durante el inicio de sesión. Para la federación de identidades entre una empresa y Huawei Cloud, el sistema de autenticación de identidad de la empresa es un proveedor de identidad y también se llama "empresa IdP". Las IdPs de terceros más populares incluyen los servicios de Microsoft Active Directory Federation (AD FS) y Shibboleth.

Concepto	Descripción
Proveedor de servicios (SP)	Un proveedor de servicios establece una relación de confianza con un IdP y proporciona servicios basados en la información de usuario proporcionada por el IdP. Para la federación de identidades entre una empresa y Huawei Cloud, Huawei Cloud es un proveedor de servicios.
Federación de identidades	La federación de identidades es el proceso de **establecer una relación de confianza** entre un IdP y SP para implementar SSO.
Inicio de sesión único (SSO)	El inicio de sesión único SSO permite a los usuarios acceder a un SP de confianza después de iniciar sesión en el IdP de la empresa. Por ejemplo, después de establecer una relación de confianza entre un sistema de gestión empresarial y Huawei Cloud, los usuarios en el sistema de gestión empresarial pueden usar sus cuentas y contraseñas existentes para acceder a Huawei Cloud a través del enlace de inicio de sesión en el sistema de gestión empresarial. La nube de Huawei admite dos tipos de SSO: SSO de usuario virtual y SSO de usuario IAM.
SAML 2.0	SAML 2.0 es un protocolo basado en XML que utiliza securityTokens que contienen aserciones para pasar información sobre un usuario final entre un IdP y un SP. Es un estándar abierto ratificado por la Organización para el Avance de Estándares de Información Estructurada (OASIS) y está siendo utilizado por muchos IdP. Para obtener más información acerca de este estándar, consulte **Descripción técnica de SAML 2.0**. Huawei Cloud implementa la federación de identidades de acuerdo con SAML 2.0. Para federar con éxito a sus usuarios empresariales con Huawei Cloud, asegúrese de que su IdP empresarial sea compatible con este protocolo.
OpenID Connect	OpenID Connect es una capa de identidad simple en la parte superior del protocolo Open Authorization 2.0 (OAuth 2.0). IAM implementa la federación de identidad de acuerdo con OpenID Connect 1.0. Para federar con éxito a sus usuarios empresariales con Huawei Cloud, asegúrese de que su IdP empresarial sea compatible con este protocolo. Para obtener más información acerca de OpenID Connect, vea **Introducción a OpenID Connect**.
OAuth 2.0	OAuth 2.0 es un protocolo de autorización abierto. El marco de autorización de este protocolo permite que las aplicaciones de terceros obtengan permisos de acceso.

Ventajas de la Federación de Identidad

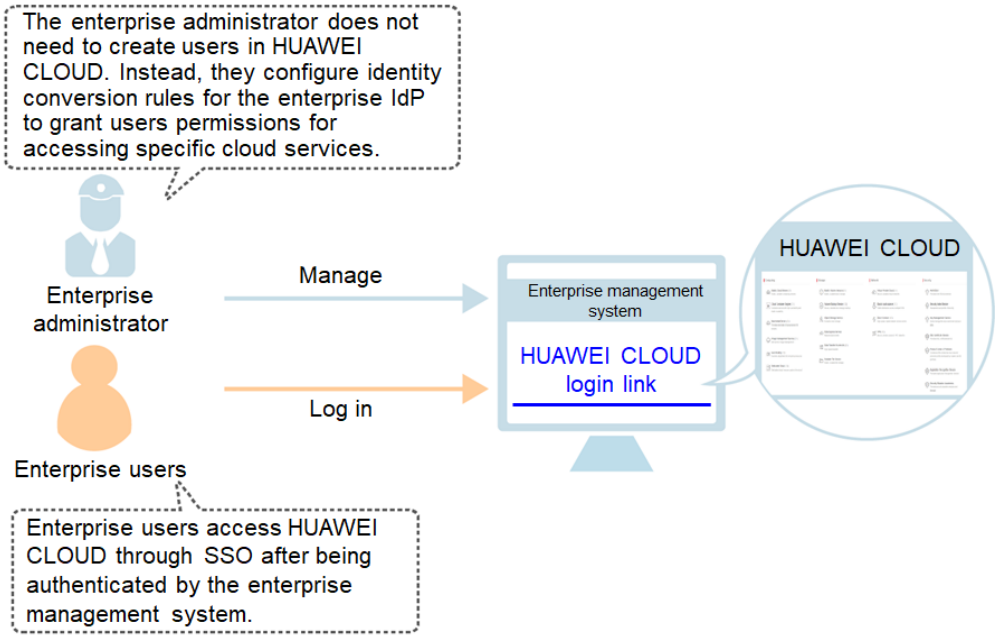
- Fácil gestión de identidades

  Con un proveedor de identidades, el administrador puede gestionar las identidades de la fuerza laboral fuera de Huawei Cloud y otorgar a estas identidades de fuerza laboral externas permisos para usar los recursos en Huawei Cloud.

- Operaciones simplificadas

  Los usuarios de la fuerza laboral pueden usar sus cuentas existentes en la empresa para acceder a Huawei Cloud a través de SSO.

Figura 9-1 Ventajas de la federación de identidad



Tipo de SSO

IAM admite dos tipos de SSO: SSO de usuario virtual y SSO de usuario de IAM. Para obtener más información sobre cómo elegir un tipo de inicio de sesión único, consulte **9.2 Escenarios de aplicación de SSO de usuario virtual y SSO de usuario de IAM**.

- SSO de usuario virtual

  Después de que un usuario federado inicie sesión en Huawei Cloud, el sistema crea automáticamente un usuario virtual y otorga permisos de acceso al usuario virtual basándose en las reglas de conversión de identidad configuradas.

- Inicio de sesión único del usuario de IAM

  Después de que un usuario federado inicie sesión en Huawei Cloud, el sistema asigna automáticamente el **ID de identidad externo** a un usuario de IAM para que el usuario federado tenga los permisos del usuario de IAM asignado.

Actualmente, IAM admite dos métodos de inicio de sesión federados: SSO basado en navegador (SSO web) y SSO a través de invocaciones de API.

- Web SSO: Los navegadores se utilizan como medio de comunicación. Este tipo de autenticación permite a los usuarios comunes acceder a Huawei Cloud mediante navegadores. Puede iniciar el inicio de sesión único web desde el lado del IdP o del SP.
  - SSO iniciado por IdP: **Configurar un enlace de inicio de sesión en el sistema de gestión empresarial**. Los empleados de su empresa pueden usar el enlace para iniciar sesión en Huawei Cloud desde el sistema de gestión empresarial.
  - SSO iniciado por SP: Huawei Cloud proporciona la entrada de **inicio de sesión del usuario federado**. Los empleados de su empresa pueden ingresar una cuenta de

Huawei Cloud y elegir el IdP de la empresa en la página de inicio de sesión para acceder a Huawei Cloud.

- SSO vía invocación de API: Los empleados de la empresa invocan a las API usando herramientas de desarrollo (como el cliente OpenStack y el cliente ShibbolethECP) para acceder a Huawei Cloud.

Tabla 9-2 Inicios de sesión federados

Tipo de SSO	Protocolos admitidos	Web SSO	Invocación a las API	Iniciado por IdP	Iniciado por SP	Múltiples IdP
Usuario virtual	SAML 2.0 y OpenID Connect	Admitido	Admitido	Admitido	Admitido	Admitido
Usuario de IAM	SAML 2.0	Admitido	Admitido	Admitido	Admitido	No admitido

Este capítulo describe cómo acceder a Huawei Cloud a través del inicio de sesión SSO web. Para obtener más información sobre cómo acceder a Huawei Cloud invocando a las API, consulta **Gestión de federación de identidades**.

Precauciones

- Asegúrese de que su servidor IdP empresarial y Huawei Cloud utilizan la hora del meridiano de Greenwich (GMT) en la misma zona horaria.
- La información de identidad (como la dirección de correo electrónico o el número de teléfono móvil) de los usuarios federados se almacena en el IdP de la empresa. Los usuarios federados se asignan a Huawei Cloud como identidades virtuales, por lo que su acceso a Huawei Cloud tiene las siguientes restricciones:
  - Los usuarios federados no necesitan realizar una verificación en 2 pasos cuando realizan operaciones críticas aunque **protección de operación crítica** (protección de inicio de sesión o protección de operación) esté habilitada.
  - Los usuarios federados no pueden crear claves de acceso con validez ilimitada, pero pueden obtener credenciales de acceso temporales (claves de acceso y tokens de seguridad) utilizando tokens de usuario o delegación. Para obtener más información, consulte **Obtención de una clave de acceso temporal y un token de seguridad a través de un token**.

    Si un usuario federado necesita una clave de acceso con validez ilimitada, puede ponerse en contacto con el administrador de la cuenta o con un usuario de IAM para crear una. Una clave de acceso contiene los permisos concedidos a un usuario, por lo que se recomienda que el usuario federado solicite a un usuario IAM del mismo grupo que cree una clave de acceso.

9.2 Escenarios de aplicación de SSO de usuario virtual y SSO de usuario de IAM

IAM admite dos tipos de SSO: SSO de usuario virtual y SSO de usuario de IAM. Esta sección describe los dos tipos de SSO y sus diferencias, lo que le ayuda a elegir un tipo adecuado para su negocio.

SSO de usuario virtual

Después de que un usuario federado inicie sesión en Huawei Cloud, el sistema crea automáticamente un usuario virtual y asigna permisos al usuario según las reglas de conversión de identidad. Se recomienda el inicio de sesión único del usuario virtual si:

- Para reducir los costos de gestión, no desea crear y gestionar usuarios de IAM en la plataforma en la nube.
- Desea asignar permisos para los recursos de la nube en función de los grupos de usuarios o atributos en su IdP de empresa local. Los cambios de permisos en el IdP empresarial local se pueden sincronizar con la plataforma en la nube ajustando los grupos de usuarios o atributos localmente.
- Su empresa tiene sucursales y puede requerir múltiples IdPs empresariales. Estos IdPs tienen que acceder a la misma cuenta de Huawei Cloud. Necesita configurar múltiples IdPs en Huawei Cloud para la federación de identidades.

Inicio de sesión único del usuario de IAM

Después de que un usuario federado inicie sesión en Huawei Cloud, el sistema asigna automáticamente el ID de identidad externo a un usuario de IAM para que el usuario federado tenga los permisos del usuario de IAM asignado. Se recomienda el inicio de sesión único del usuario de IAM si:

- Los productos en la nube que utiliza (como **CodeArts**) no admiten el inicio de sesión único del usuario virtual.
- No necesita SSO de usuario virtual y desea simplificar la configuración de IdP.

Diferencias entre SSO de usuario virtual y SSO de usuario de IAM

Las diferencias entre el SSO de usuario virtual y el SSO de usuario de IAM se describen a continuación:

1. Conversión de identidad: El SSO de usuario virtual utiliza **reglas de conversión de identidad**, mientras que el SSO de usuario de IAM utiliza ID de identidad externos para la conversión de identidad. Un usuario IdP se asignará a un usuario IAM si el valor **IAM_SAML_Attributes_xUserId** del usuario IdP es el mismo que el **ID de identidad externo** del usuario IAM. Cuando utilice el inicio de sesión único del usuario de IAM, asegúrese de haber establecido **IAM_SAML_Attributes_xUserId** en el IdP y **External Identity ID** en el SP en el mismo valor.

2. Identidad de usuario en IAM: En el SSO de usuario virtual, el usuario IdP no tiene un usuario IAM correspondiente en la lista de usuarios IAM. Después de que el usuario IdP inicie sesión, el sistema crea automáticamente un usuario virtual para él. En el SSO del

usuario de IAM, el usuario de IdP tiene un usuario de IAM asignado por ID de identidad externa en la consola de IAM.

3. Asignación de permisos en IAM: en el inicio de sesión único del usuario virtual, los permisos del usuario IdP se definen mediante la regla de conversión de identidad. En el SSO del usuario de IAM, el usuario de IdP hereda los permisos del grupo de usuarios al que pertenece el usuario de IAM asignado.

9.3 SSO de usuario virtual a través de SAML

9.3.1 Descripción general del inicio de sesión único del usuario virtual a través de SAML

Huawei Cloud admite la federación de identidades con SAML (Security Assertion Markup Language), que es un estándar abierto que utilizan muchos proveedores de identidades (IdP). Durante la federación de identidades, Huawei Cloud funciona como un proveedor de servicios (SP) y las empresas funcionan como IdPs. Esta sección describe cómo configurar la federación de identidades y cómo funciona la federación de identidades.

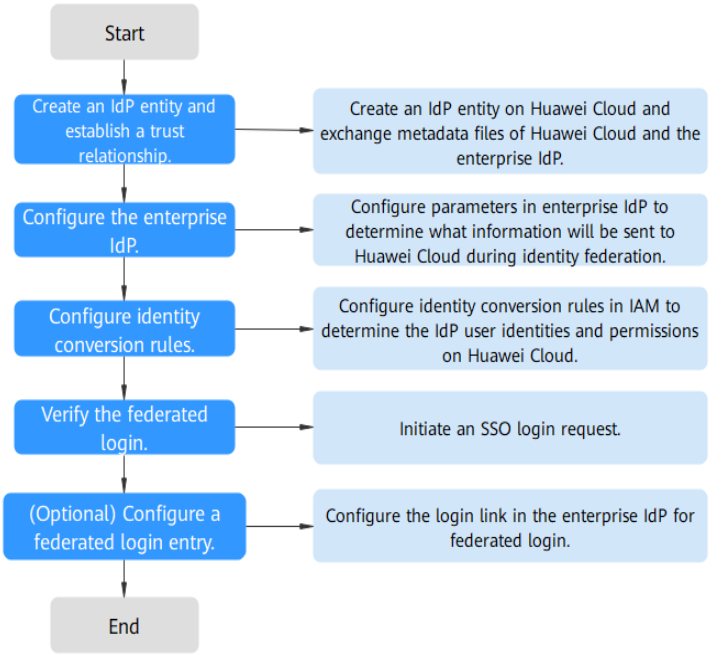
⚠ ATENCIÓN

Asegúrese de que su IdP empresarial sea compatible con SAML 2.0.

Configuración de la federación de identidades

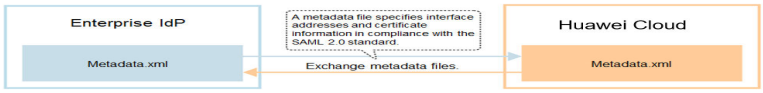
A continuación se describe cómo configurar su IdP empresarial y Huawei Cloud para que confíen entre sí.

Figura 9-2 Configuración de SSO de usuario virtual a través de SAML



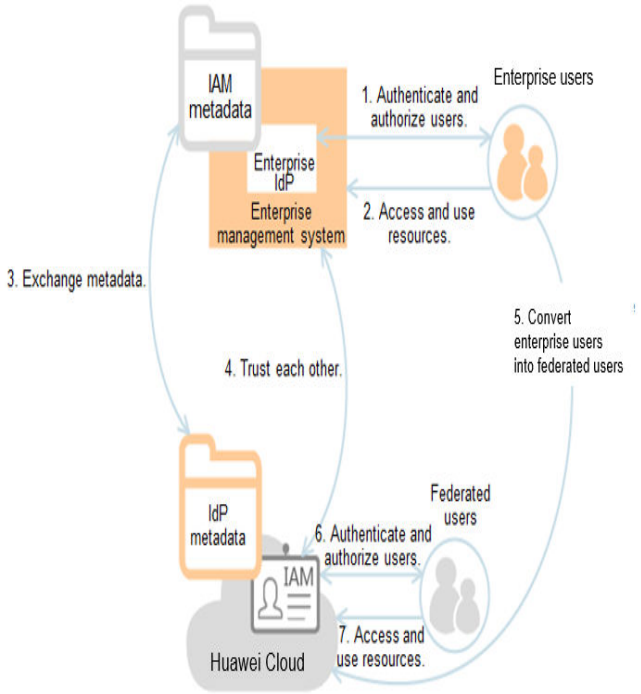
1. **Crear una entidad IdP y establecer una relación de confianza**: Cree una entidad IdP para su empresa en Huawei Cloud. A continuación, cargue el archivo de metadatos de Huawei Cloud en el IdP empresarial y cargue el archivo de metadatos del IdP empresarial en Huawei Cloud.

   Figura 9-3 Intercambio de archivos de metadatos



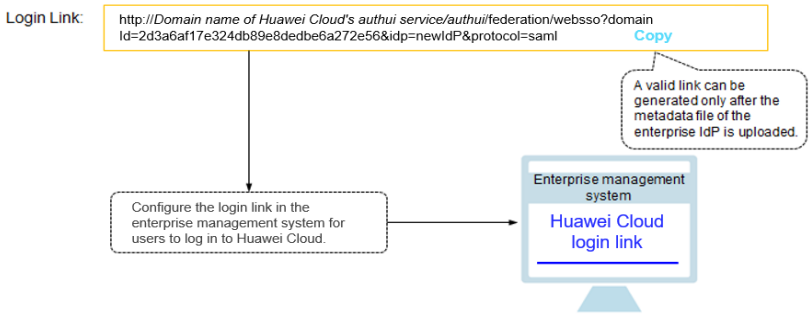
2. **Configurar el IdP empresarial**: Configure los parámetros del IdP empresarial para determinar qué información se puede enviar a Huawei Cloud.
3. **Configurar reglas de conversión de identidad**: Configure reglas de conversión de identidad para determinar las identidades de usuario IdP y los permisos en Huawei Cloud.

   Figura 9-4 Asignación de identidades externas a usuarios virtuales



4. **Verificar el inicio de sesión federado**: Compruebe si el usuario empresarial puede iniciar sesión en Huawei Cloud a través de SSO.
5. **(Opcional) Configurar una entrada de inicio de sesión federada**: Configure el enlace de inicio de sesión (consulte **Figura 9-5**) en el IdP empresarial para permitir que los usuarios empresariales sean redirigidos a Huawei Cloud desde su sistema de gestión empresarial.

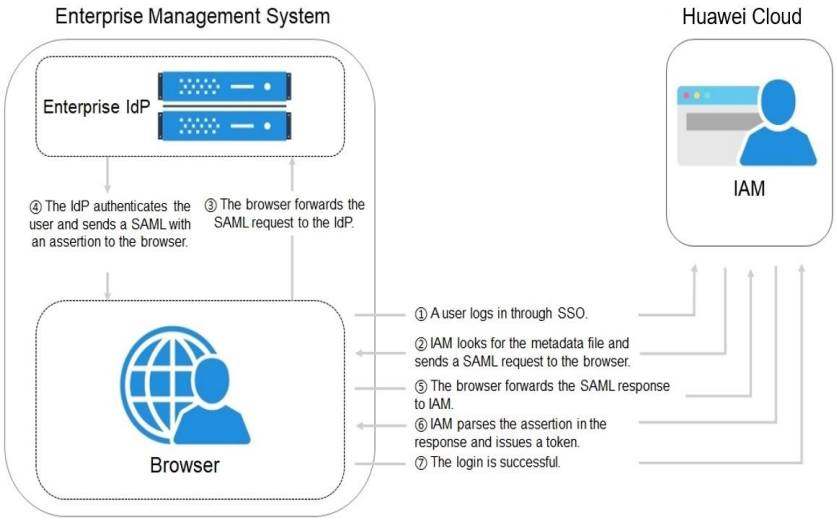
Figura 9-5 Modelo de inicio de sesión SSO



Cómo funciona la federación de identidades

Figura 9-6 muestra el proceso de federación de identidades entre un sistema de gestión empresarial y Huawei Cloud.

Figura 9-6 Cómo funciona la federación de identidades



NOTA

Para ver las solicitudes y afirmaciones interactivas con una mejor experiencia, se recomienda utilizar Google Chrome e instalar SAML Message Decoder.

Como se muestra en **Figura 9-6**, el proceso de federación de identidad es el siguiente:

1. Un usuario abre el enlace de inicio de sesión generado después de la creación del IdP en el navegador. El navegador envía una solicitud de inicio de sesión único a Huawei Cloud.
2. Huawei Cloud autentica al usuario contra el archivo de metadatos del IdP empresarial y crea una solicitud SAML al navegador.
3. El navegador reenvía la solicitud SAML al IdP de empresa.
4. El usuario introduce su nombre de usuario y contraseña en la página de inicio de sesión. Después de que el IdP de empresa autentica la identidad del usuario, construye una

aserción SAML que contiene los detalles del usuario y envía la aserción al navegador como una respuesta SAML.

5. El navegador responde y reenvía la respuesta SAML a Huawei Cloud.
6. Huawei Cloud analiza la afirmación en la respuesta SAML, identifica el grupo de usuarios de IAM que se asigna al usuario según las reglas de conversión de identidad y emite un token al usuario.
7. El inicio de sesión SSO se realiza correctamente.

NOTA

La aserción debe llevar una firma; de lo contrario, el inicio de sesión fallará.

9.3.2 Paso 1: Crear una entidad IdP

Para establecer una relación de confianza entre un IdP empresarial y Huawei Cloud, cargue el archivo de metadatos de Huawei Cloud al IdP empresarial, y, a continuación, cree una entidad IdP y cargue el archivo de metadatos del IdP empresarial en la consola IAM.

Prerrequisitos

Ha leído la documentación del IdP de empresa o ha entendido cómo utilizar el IdP de empresa. Las configuraciones de diferentes IdPs empresariales difieren mucho, por lo que no se describen en este documento. Para obtener detalles sobre cómo obtener el archivo de metadatos del IdP empresarial y cómo cargar el archivo de metadatos de Huawei Cloud al IdP empresarial, consulte la documentación de ayuda del IdP.

Establecer una relación de confianza entre el IdP empresarial y Huawei Cloud

El archivo de metadatos de Huawei Cloud debe configurarse en el IdP empresarial para establecer una relación de confianza entre los dos sistemas.

Paso 1 Descargue el archivo de metadatos de Huawei Cloud.

Visite **https://auth-intl.huaweicloud.com/authui/saml/metadata.xml** (Se recomienda Google Chrome). Descargue el archivo de metadatos de Huawei Cloud y establezca el nombre del archivo, por ejemplo, **SP-metadata.xml**.

Paso 2 Cargue el archivo de metadatos al servidor IdP empresarial. Para obtener más información, consulte la documentación de ayuda del IdP empresarial.

Paso 3 Obtenga el archivo de metadatos del IdP de empresa. Para obtener más información, consulte la documentación de ayuda del IdP empresarial.

----Fin

Creación de una entidad IdP en Huawei Cloud

Para crear una entidad IdP en la consola IAM, haga lo siguiente:

Paso 1 Inicie sesión en la **consola de IAM**, elija **Identity Providers** en el panel de navegación y haga clic en **Create Identity Provider** en la esquina superior derecha.

Paso 2 Especifique el nombre, el protocolo, el tipo de inicio de sesión único, el estado y la descripción de la entidad IdP.

Tabla 9-3 Parámetros básicos de un IdP

Parámetro	Descripción
Name	Nombre IdP, que debe ser único a nivel mundial. Se recomienda utilizar el nombre de dominio.
Protocol	Protocolo IdP. Huawei Cloud es compatible con los protocolos SAML y OpenID Connect. Para obtener más información sobre la federación de identidades basada en OpenID Connect, consulte **9.5 SSO de usuario virtual a través de OpenID Connect**.
SSO Type	Tipo de IdP. Una cuenta solo puede tener un tipo de IdP. A continuación se describe el tipo de usuario virtual. SSO de usuario virtual: después de que un usuario federado inicie sesión en Huawei Cloud, el sistema crea automáticamente un usuario virtual para el usuario federado. Una cuenta puede tener varias IdPs del tipo de usuario virtual.
Status	Estado de IdP. El valor predeterminado es **Enabled**.

Paso 3 Haga clic en **OK**.

----Fin

Configuración del archivo de metadatos del IdP empresarial en Huawei Cloud

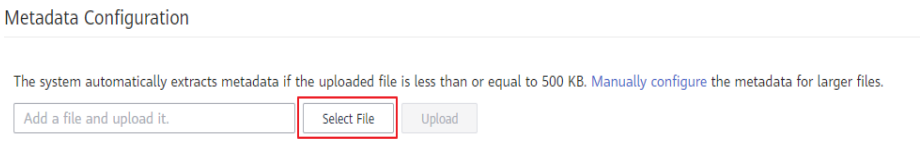
Para configurar el archivo de metadatos del IdP empresarial en Huawei Cloud, puede cargar el archivo de metadatos o editar manualmente los metadatos en la consola de IAM. Para un archivo de metadatos de más de 500 KB, configure manualmente los metadatos. Si se han cambiado los metadatos, cargue el último archivo de metadatos o edite los metadatos existentes para garantizar que los usuarios federados puedan iniciar sesión en Huawei Cloud con éxito.

NOTA

Para obtener más información sobre cómo obtener el archivo de metadatos de un IdP de empresa, consulte la documentación de ayuda del IdP de empresa.

- **Cargar un archivo de metadatos.**
  a. Haga clic en **Modify** en la fila que contiene el IdP.
  b. Haga clic en **Select File** y seleccione el archivo de metadatos del IdP de empresa.

  Figura 9-7 Carga de un archivo de metadatos

  c. Haga clic en **Upload**. Se muestran los metadatos extraídos del archivo cargado. Haga clic en **OK**.
     - Si el archivo de metadatos cargado contiene varios IdP, seleccione el IdP que desea usar en la lista desplegable **Entity ID**.

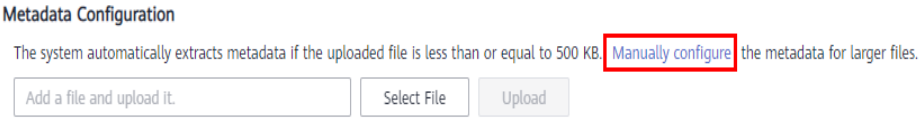
- Si aparece un mensaje que indica que no se ha especificado ningún ID de entidad o que el certificado de firma ha caducado, compruebe el archivo de metadatos y cárguelo de nuevo o configure los metadatos manualmente.

d. Haga clic en **OK**.

- **Configurar manualmente los metadatos.**

a. Haga clic en **Manually configure**.

Figura 9-8 Configuración manual de metadatos



b. En el cuadro de diálogo **Configure Metadata**, establezca los parámetros de metadatos, como **Entity ID**, **Signing Certificate** y **SingleSignOnService**.

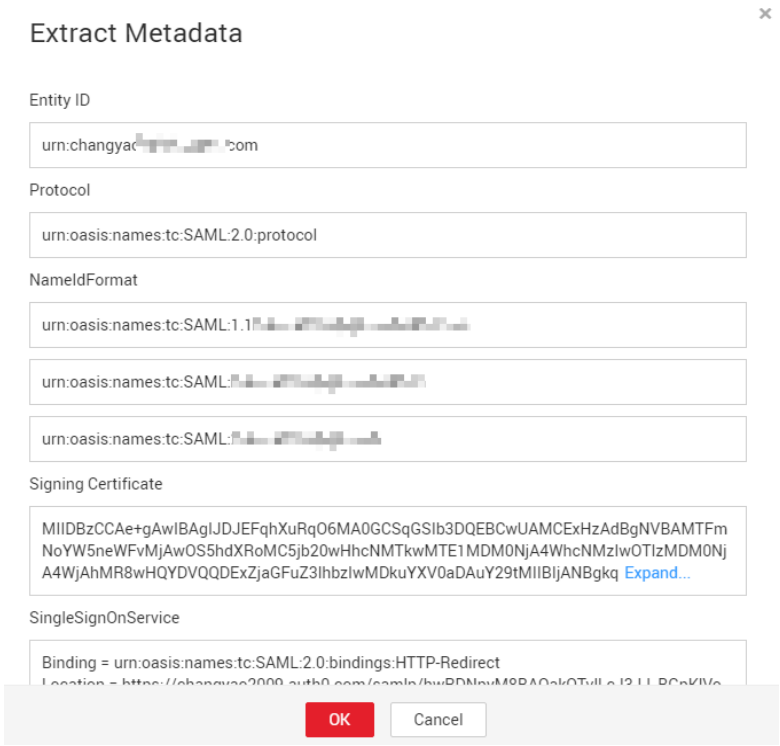
Parámetro	Obligatorio	Descripción
Entity ID	Sí	El identificador único de un IdP. Introduzca el valor del **entityID** que se muestra en el archivo de metadatos del IdP de empresa. Si el archivo de metadatos contiene varios IdP, elija la que desee usar.
Protocol	Sí	Protocolo utilizado para la federación de identidades entre un IdP de empresa y un SP. El protocolo está seleccionado de forma predeterminada.
NameIdFormat	No	Introduzca el valor de **NameIdFormat** que se muestra en el archivo de metadatos IdP. Especifica el formato de identificador de nombre de usuario soportado por el IdP, que se utiliza para la comunicación entre el IdP y el usuario federado. Si configura varios valores, Huawei Cloud utiliza el primer valor de forma predeterminada.

Parámetro	Obligatorio	Descripción
Signing Certificate	Sí	Introduzca el valor de **<X509Certificate>** que se muestra en el archivo de metadatos IdP. Un certificado de firma es un certificado de clave pública utilizado para la verificación de firma. Por motivos de seguridad, introduzca una clave pública que contenga al menos 2,048 bits. El certificado de firma se utiliza durante la federación de identidad para garantizar que las afirmaciones sean creíbles y completas. Si configura varios valores, Huawei Cloud utiliza el primer valor de forma predeterminada.
SingleSignOnService	Sí	Introduzca el valor de **SingleSignOnService** que se muestra en el archivo de metadatos IdP. Este parámetro define cómo se envían las solicitudes SAML durante el inicio de sesión único. Debe ser compatible con HTTP Redirect o HTTP POST. Si configura varios valores, Huawei Cloud utiliza el primer valor de forma predeterminada.
SingleLogoutService	No	Introduzca el valor de **SingleLogoutService** que se muestra en el archivo de metadatos IdP. Este parámetro indica la dirección a la que los usuarios federados serán redirigidos después de cerrar sus sesiones. Debe ser compatible con HTTP Redirect o HTTP POST. Si configura varios valores, Huawei Cloud utiliza el primer valor de forma predeterminada.

En el ejemplo siguiente se muestra el archivo de metadatos de un IdP de empresa y los metadatos configurados manualmente.

Figura 9-9 Archivo de metadatos de un IdP de empresa

Figura 9-10 Configuración manual de metadatos



c. Haga clic en **OK**.

Operaciones relacionadas

- Consulta de información de IdP: En la lista IdP, haga clic en **View** en la fila que contiene el IdP y vea su información básica, configuración de metadatos y reglas de conversión de identidad.

  NOTA

  Para modificar la configuración de un IdP, haga clic en **Modify** en la parte inferior de la página de detalles.

- Modificación de un IdP: En la lista IdP, haga clic en **Modify** en la fila que contiene el IdP y, a continuación, cambie su estado o modifique la descripción, metadatos o reglas de conversión de identidad.
- Eliminación de un IdP: En la lista IdP, haga clic en **Delete** en la fila que contiene el IdP y haga clic en **Yes** en el cuadro de diálogo mostrado.

Acciones posteriores

- Configurar el IdP empresarial: Configure los parámetros del IdP empresarial para determinar qué información se puede enviar a Huawei Cloud.
- Configurar reglas de conversión de identidad: en el área **Identity Conversion Rules**, configure reglas de conversión de identidad para establecer una asignación entre usuarios de empresa y grupos de usuarios de IAM. De esta manera, los usuarios empresariales pueden obtener los permisos correspondientes en Huawei Cloud. Para obtener más información, véase **9.3.4 Paso 3: Configurar reglas de conversión de identidad**.
- Verificar el inicio de sesión federado: Compruebe si el usuario empresarial puede iniciar sesión en Huawei Cloud a través de SSO. Para obtener más información, véase **9.3.5 Paso 4: Verificar el inicio de sesión federado**.

9.3.3 Paso 2: Configurar el IdP de la empresa

Puede configurar parámetros en el IdP empresarial para determinar qué información se enviará a Huawei Cloud. Huawei Cloud autentica la identidad federada y asigna permisos basados en la información recibida y las reglas de conversión de identidad.

Parámetros comunes en un IdP de empresa

Tabla 9-4 Parámetros comunes en un IdP de empresa

Parámetro	Descripción	Escenario
IAM_SAML_Attributes_redirect_url	URL de destino a la que se redirigirá el usuario federado	Durante el inicio de sesión SSO, el usuario federado será redirigido a una página en Huawei Cloud, por ejemplo, la página de inicio de Cloud Eye en la región CN-Hong Kong.
IAM_SAML_Attributes_domain_id	ID de cuenta de Huawei Cloud se federará con el IdP empresarial	Este parámetro es obligatorio en la federación iniciada por IdP de empresa.
IAM_SAML_Attributes_idp_id	Nombre de la entidad IdP creada en Huawei Cloud	Este parámetro es obligatorio en la federación iniciada por IdP de empresa.

9.3.4 Paso 3: Configurar reglas de conversión de identidad

Después de que un usuario de IdP empresarial inicie sesión en Huawei Cloud, Huawei Cloud autentica la identidad y asigna permisos al usuario según las reglas de conversión de identidad. Puede personalizar las reglas de conversión de identidad en función de sus requisitos de servicio. Si no configura reglas de conversión de identidad, el nombre de usuario del usuario federado en Huawei Cloud es **FederationUser** de forma predeterminada, y el usuario federado solo puede acceder a Huawei Cloud de forma predeterminada.

Puede configurar los siguientes parámetros para usuarios federados:

- Nombre de usuario: Nombres de usuario de usuarios federados en Huawei Cloud.

- Permisos de usuario: Permisos asignados a usuarios federados en Huawei Cloud. Debe asignar los usuarios federados a los grupos de usuarios de IAM. De esta manera, los usuarios federados pueden obtener los permisos de los grupos de usuarios para usar los recursos de Huawei Cloud. Asegúrese de que se han creado grupos de usuarios. Para obtener más información acerca de cómo crear un grupo de usuarios, consulte **4.1 Creación de un grupo de usuarios y asignación de permisos**.

  NOTA

  - Las modificaciones a las reglas de conversión de identidad entrarán en vigor la próxima vez que los usuarios federados inicien sesión.
  - Para modificar los permisos de un usuario, modifique los permisos del grupo de usuarios al que pertenece el usuario. A continuación, reinicie el IdP de empresa para que las modificaciones surtan efecto.

Prerrequisitos

- El administrador de la empresa ha creado una cuenta en Huawei Cloud, y ha creado grupos de usuarios y asignado permisos al grupo en IAM. Para más detalles, consulte **4.1 Creación de un grupo de usuarios y asignación de permisos**.
- Se ha creado un IdP en Huawei Cloud. Para obtener más información, véase **9.3.2 Paso 1: Crear una entidad IdP**.

Procedimiento

Si configura las reglas de conversión de identidad haciendo clic en **Create Rule**, IAM convertirá los parámetros especificados al formato JSON. Alternativamente, puede hacer clic en **Edit Rule** para configurar directamente las reglas en formato JSON. Para obtener más información, véase **9.6 Sintaxis de las reglas de conversión de identidad**.

- **Creación de reglas**

  a. Inicie sesión en la **consola de IAM** como administrador. En el panel de navegación, elija **Identity Providers**.

  b. En la lista IdP, haga clic en **Modify** en la fila que contiene el IdP.

  c. En el área **Identity Conversion Rules**, haga clic en **Create Rule**. A continuación, configure las reglas en el cuadro de diálogo **Create Rule**.

  Figura 9-11 Hacer clic en Create Rule

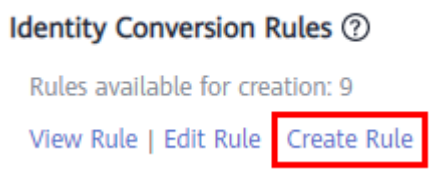
  

Figura 9-12 Creación de reglas

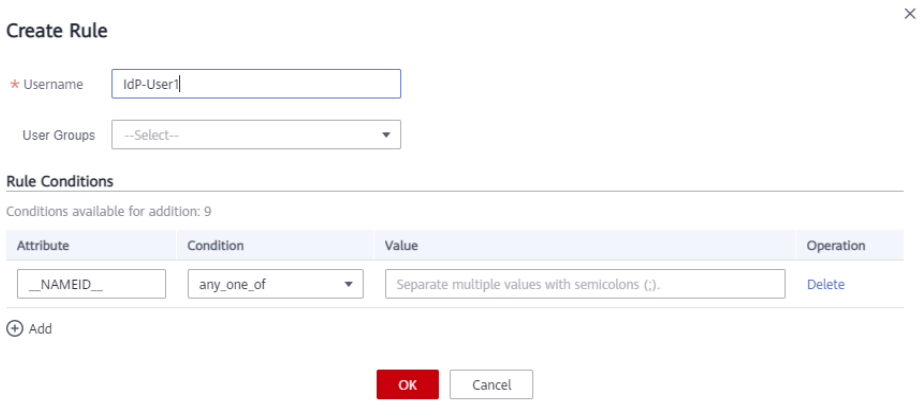


Tabla 9-5 Descripción del parámetro

Parámetro	Descripción	Observaciones
Username	Nombre de usuario de los usuarios federados en Huawei Cloud.	Para distinguir a los usuarios federados de los usuarios de Huawei Cloud, se recomienda que establezca el nombre de usuario en **FederationUser-***IdP_XXX*. *IdP* indica un nombre de IdP, por ejemplo, AD FS o Shibboleth. *XXX* indica un nombre personalizado. **AVISO** ● El nombre de usuario de cada usuario federado debe ser único en el mismo IdP. Los usuarios federados con los mismos nombres de usuario en el mismo IdP se asignarán al mismo usuario IAM en Huawei Cloud. ● El nombre de usuario solo puede contener letras, dígitos, espacios, guiones (-) guiones bajos (_) y puntos (.). No puede comenzar con un dígito y no puede contener el siguiente characters: ", \", \\, \n, \r
User Groups	Grupos de usuarios a los que pertenecen los usuarios federados en Huawei Cloud.	Los usuarios federados heredarán permisos de los grupos a los que pertenecen. Puede seleccionar un grupo de usuarios que ya se haya creado.

Parámetro	Descripción	Observaciones
Rule Conditions	Condiciones que debe cumplir un usuario federado para obtener permisos de los grupos de usuarios seleccionados.	Los usuarios federados que no cumplan estas condiciones no pueden acceder a Huawei Cloud. Puede crear un máximo de 10 condiciones para una regla de conversión de identidad. Los parámetros **Attribute** y **Value** se utilizan para que el IdP empresarial transfiera información del usuario a Huawei Cloud mediante aserciones SAML. El parámetro **Condition** se puede establecer en **empty**, **any_one_of**, o **not_any_of**. Para obtener más información sobre estos parámetros, consulte **Sintaxis de reglas de conversión de identidad**. **NOTA** ● Una regla de conversión de identidad puede tener varias condiciones. Solo tiene efecto si se cumplen todas las condiciones. ● Un IdP puede tener varias reglas de conversión de identidad. Si un usuario federado no cumple con ninguna de las condiciones, se le denegará el acceso a Huawei Cloud.

Por ejemplo, establezca una regla de conversión de identidad para los administradores del sistema de gestión empresarial.

- Nombre de usuario: **FederationUser-IdP_admin**
- Grupo de usuarios: **admin**
- Condición de regla: **_NAMEID_** (atributo), **any_one_of** (condición) y **000000001** (valor).

  Solo el usuario con ID 000000001 se asigna al usuario de IAM **FederationUser-IdP_admin** y hereda los permisos del grupo de usuarios **admin**.

d. En el cuadro de diálogo **Create Rule**, haga clic en **OK**.

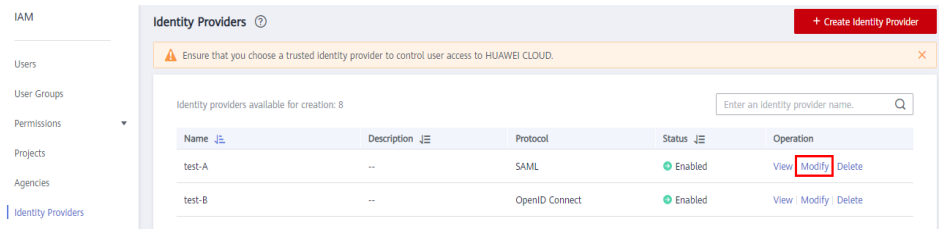
e. En la página **Modify Identity Provider**, haga clic en **OK**.

- **Edición de reglas**

a. Inicie sesión en la **consola de IAM** como administrador. En el panel de navegación, elija **Identity Providers**.

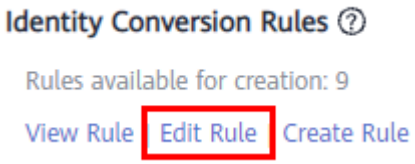
b. En la lista IdP, haga clic en **Modify** en la fila que contiene el IdP.

Figura 9-13 Modificación de un IdP



c. En el área **Identity Conversion Rules**, haga clic en **Edit Rule**.

Figura 9-14 Edición de reglas de conversión de identidad



d. Edite las reglas de conversión de identidad en formato JSON. Para obtener más información, véase **9.6 Sintaxis de las reglas de conversión de identidad**.

e. Haga clic en **Validate** para verificar la sintaxis de las reglas.

f. Si la regla es correcta, haga clic en **OK** en el cuadro de diálogo **Edit Rule** y haga clic en **OK** en la página **Modify Identity Provider**.

Si aparece un mensaje que indica que el archivo JSON está incompleto, modifique las instrucciones o haga clic en **Cancel** para cancelar las modificaciones.

Operaciones relacionadas

Ver reglas de conversión de identidad: haga clic en **View Rule** en la página **Modify Identity Provider**. Las reglas de conversión de identidad se muestran en formato JSON. Para obtener más información sobre el formato JSON, consulte **Sintaxis de reglas de conversión de identidad**.

9.3.5 Paso 4: Verificar el inicio de sesión federado

Verificación del inicio de sesión federado

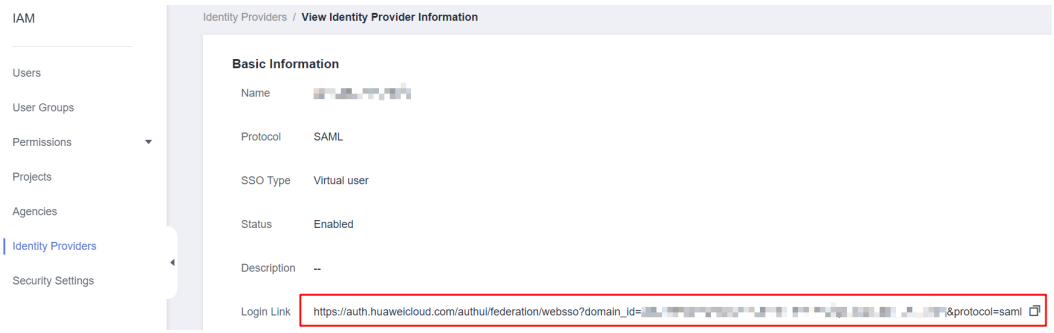
Los usuarios federados pueden iniciar un inicio de sesión desde el IdP o el SP.

- Iniciar un inicio de sesión desde un IdP, por ejemplo, Microsoft Active Directory Federation Services (AD FS) o Shibboleth.
- Iniciar un inicio de sesión desde el SP. Puede obtener el enlace de inicio de sesión en la página de detalles del IdP en la consola de IAM.

El método de inicio de sesión iniciado por IdP depende del IdP. Para obtener más información, consulte la documentación de ayuda del IdP. Esta sección describe cómo iniciar un inicio de sesión desde el SP.

Paso 1 Inicie sesión como usuario federado.

En la página **Identity Providers** de la consola de IAM, haga clic en **View** en la fila que contiene el IdP. Haga clic en para copiar el enlace de inicio de sesión que se muestra en el área **Basic Information** y abra el enlace con un explorador y, a continuación, introduzca el nombre de usuario y la contraseña utilizados en el sistema de gestión empresarial.



Paso 2 Compruebe que el usuario federado tiene los permisos asignados a su grupo de usuarios.

----Fin

Redirección a una Región o Servicio Especificado

Puede especificar la página de destino a la que el usuario federado será redirigido después de iniciar sesión, por ejemplo, la página de inicio de Cloud Eye en la región CN-Hong Kong.

- Configuración del enlace de inicio de sesión en el SP

  Combine el enlace de inicio de sesión obtenido de la consola con la URL especificada usando el formato **Login link&service=Specified URL**. Por ejemplo, si el enlace de inicio de sesión obtenido es **https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml** y la dirección URL especificada es **https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1**, el enlace de inicio de sesión configurado en el SP es **https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml&service=https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1**
- Configuración del enlace de inicio de sesión en el IdP

  Configure **IAM_SAML_Attributes_redirect_url** (la dirección URL a la que se redirigirá) en la afirmación SAML del IdP de empresa.

9.3.6 (Opcional) Paso 5: Configurar una entrada de inicio de sesión federada en el IdP de empresa

Configure una entrada de inicio de sesión federada en el IdP empresarial para que los usuarios empresariales puedan usar el enlace de inicio de sesión para acceder a Huawei Cloud.

NOTA

Si no se ha configurado ningún enlace de inicio de sesión en su sistema de gestión empresarial, los usuarios federados de su empresa pueden iniciar sesión en Huawei Cloud a través de la página de inicio de sesión de Huawei Cloud. Para obtener más información, véase **Inicio de sesión como usuario federado**.

Prerrequisitos

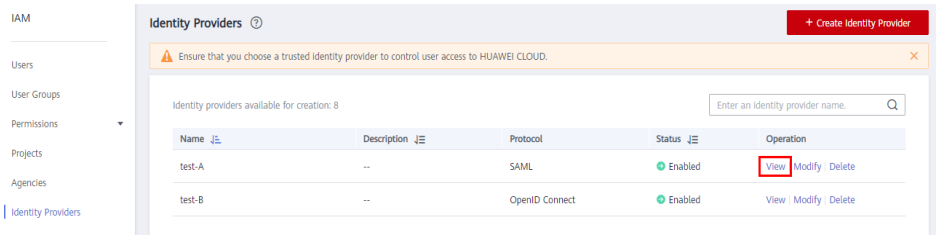
- Se ha creado una entidad IdP en Huawei Cloud. Para obtener más información acerca de cómo crear una entidad IdP, consulte **9.3.2 Paso 1: Crear una entidad IdP**.
- La entrada de inicio de sesión para iniciar sesión en Huawei Cloud se ha configurado en el sistema de gestión empresarial.

Procedimiento

Paso 1 Inicie sesión en la **consola de IAM**. En el panel de navegación, elija **Identity Providers**.

Paso 2 Haga clic en **View** en la fila que contiene el IdP.

Figura 9-15 Consulta de los detalles del IdP



Paso 3 Copie el enlace de inicio de sesión haciendo clic en en la fila **Login Link**.

Figura 9-16 Copia del enlace de inicio de sesión

Paso 4 Agregue la siguiente instrucción al archivo de página del sistema de gestión empresarial:

```
<a href="<Login link>"> Huawei Cloud login entry </a>
```

Paso 5 Inicie sesión en el sistema de gestión empresarial con su cuenta empresarial y haga clic en el enlace de inicio de sesión configurado para acceder a Huawei Cloud.

----Fin

9.4 SSO de usuario de IAM a través de SAML

9.4.1 Descripción general del inicio de sesión único del usuario de IAM a través de SAML

Huawei Cloud admite la federación de identidades con SAML (Security Assertion Markup Language), que es un estándar abierto que utilizan muchos proveedores de identidades (IdP). Durante la federación de identidades, Huawei Cloud funciona como un proveedor de servicios (SP) y las empresas funcionan como IdPs. La federación basada en SAML permite el inicio de sesión único (SSO), por lo que los empleados de su empresa pueden iniciar sesión en Huawei Cloud como usuarios de IAM.

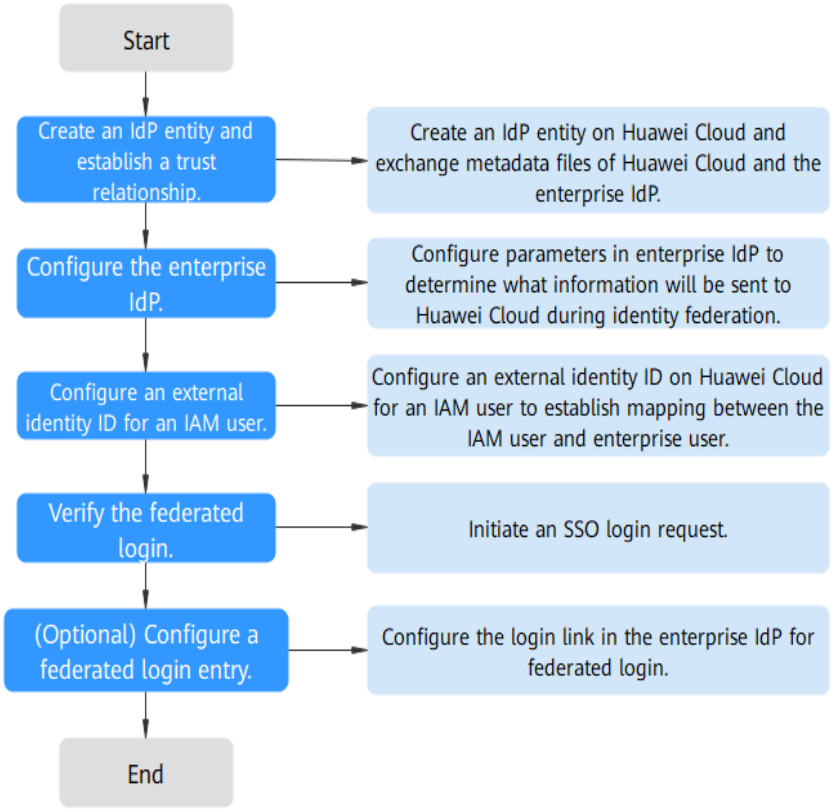
Esta sección describe cómo configurar la federación de identidades y cómo funciona la federación de identidades.

> **ATENCIÓN**
>
> Asegúrese de que su IdP empresarial sea compatible con SAML 2.0.

Configuración de la federación de identidades

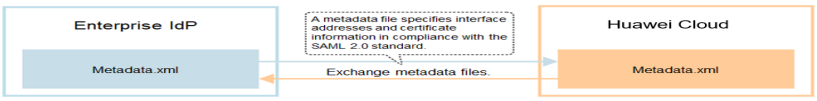
A continuación se describe cómo configurar su IdP empresarial y Huawei Cloud para que confíen entre sí.

Figura 9-17 Configuración del inicio de sesión único del usuario de IAM a través de SAML



1. **Crear una entidad IdP y establecer una relación de confianza**: Cree una entidad IdP para su empresa en Huawei Cloud. A continuación, cargue el archivo de metadatos de Huawei Cloud en el IdP empresarial y cargue el archivo de metadatos del IdP empresarial en Huawei Cloud.

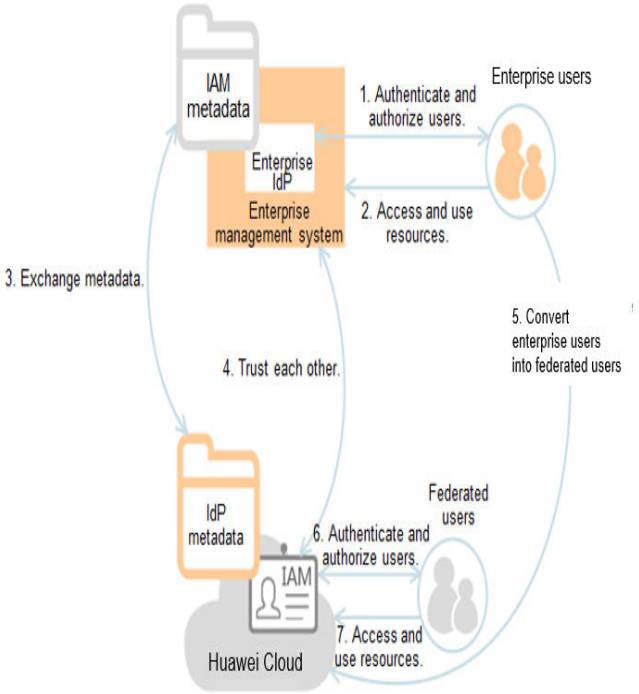
   Figura 9-18 Intercambio de archivos de metadatos

2. **Configurar el IdP empresarial**: Configure los parámetros del IdP empresarial para determinar qué información se puede enviar a Huawei Cloud.

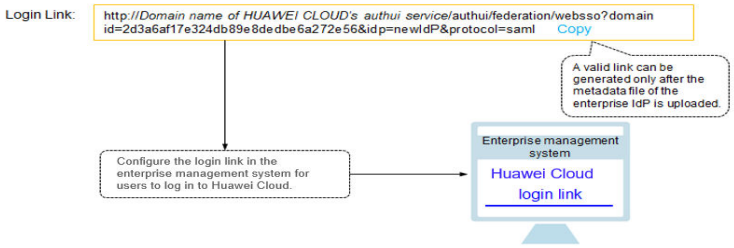
3. **Configurar un ID de identidad externo**: Establezca una asignación entre un usuario de IAM y un usuario de empresa. Cuando su IdP empresarial establece el acceso SSO a Huawei Cloud, el usuario empresarial puede iniciar sesión en Huawei Cloud como el usuario IAM con el ID de identidad externo especificado. Por ejemplo, si un usuario de empresa **IdP_Test_User** se asigna al usuario de IAM **Alice**, el usuario de empresa **IdP_Test_User** iniciará sesión en Huawei Cloud como el usuario de IAM **Alice**.

   Figura 9-19 Asignación de identidades externas a usuarios de IAM



4. **Verificar el inicio de sesión federado**: Compruebe si el usuario empresarial puede iniciar sesión en Huawei Cloud a través de SSO.
5. **(Opcional) Configurar una entrada de inicio de sesión federada**: Configure el enlace de inicio de sesión (consulte **Figura 9-20**) en el IdP empresarial para permitir que los usuarios empresariales sean redirigidos a Huawei Cloud desde su sistema de gestión empresarial.

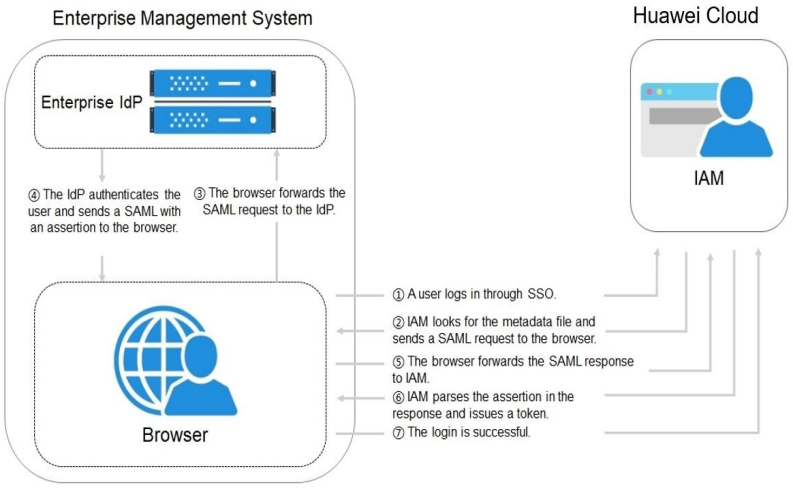
Figura 9-20 Modelo de inicio de sesión SSO



Cómo funciona la federación de identidades

Figura 9-21 muestra el proceso de federación de identidades entre un sistema de gestión empresarial y Huawei Cloud.

Figura 9-21 Cómo funciona la federación de identidades



NOTA

Para ver las solicitudes y afirmaciones interactivas con una mejor experiencia, se recomienda utilizar Google Chrome e instalar SAML Message Decoder.

Como se muestra en **Figura 9-21**, el proceso de federación de identidad es el siguiente:

1. Un usuario abre el enlace de inicio de sesión generado después de la creación del IdP en el navegador. El navegador envía una solicitud de inicio de sesión único a Huawei Cloud.
2. Huawei Cloud autentica al usuario contra el archivo de metadatos del IdP empresarial y crea una solicitud SAML al navegador.
3. El navegador reenvía la solicitud SAML al IdP de empresa.
4. El usuario introduce su nombre de usuario y contraseña en la página de inicio de sesión. Después de que el IdP de empresa autentica la identidad del usuario, construye una

aserción SAML que contiene los detalles del usuario y envía la aserción al navegador como una respuesta SAML.

5. El navegador responde y reenvía la respuesta SAML a Huawei Cloud.
6. Huawei Cloud analiza la afirmación en la respuesta SAML, identifica el grupo de usuarios de IAM que se asigna al usuario según las reglas de conversión de identidad y emite un token al usuario.
7. El inicio de sesión SSO se realiza correctamente.

NOTA

La aserción debe llevar una firma; de lo contrario, el inicio de sesión fallará.

9.4.2 Paso 1: Crear una entidad IdP

Para establecer una relación de confianza entre un IdP empresarial y Huawei Cloud, cargue el archivo de metadatos de Huawei Cloud al IdP empresarial, y, a continuación, cree una entidad IdP y cargue el archivo de metadatos del IdP empresarial en la consola IAM.

Establecer una relación de confianza entre el IdP empresarial y Huawei Cloud

Configure el archivo de metadatos de Huawei Cloud en el IdP empresarial para establecer una confianza.

Paso 1 Descargue el archivo de metadatos de Huawei Cloud.

Visite **https://auth-intl.huaweicloud.com/authui/saml/metadata.xml** (Se recomienda Google Chrome). Descargue el archivo de metadatos de Huawei Cloud y establezca el nombre del archivo, por ejemplo, **SP-metadata.xml**.

Paso 2 Cargue el archivo de metadatos al servidor IdP empresarial. Para obtener más información, consulte la documentación de ayuda del IdP empresarial.

Paso 3 Obtenga el archivo de metadatos del IdP de empresa. Para obtener más información, consulte la documentación de ayuda del IdP empresarial.

----Fin

Creación de una entidad IdP en Huawei Cloud

Para crear una entidad IdP en la consola IAM, haga lo siguiente:

Paso 1 Inicie sesión en la **consola de IAM**, elija **Identity Providers** en el panel de navegación y haga clic en **Create Identity Provider** en la esquina superior derecha.

Paso 2 Especifique el nombre, el protocolo, el tipo de inicio de sesión único, el estado y la descripción de la entidad IdP.

Tabla 9-6 Parámetros básicos de un IdP

Parámetro	Descripción
Name	Nombre IdP, que debe ser único a nivel mundial. Se recomienda utilizar el nombre de dominio.

Parámetro	Descripción
Protocol	Protocolo IdP. Huawei Cloud es compatible con los protocolos SAML y OpenID Connect. Para obtener más información sobre la federación de identidades basada en OpenID Connect, consulte **9.5 SSO de usuario virtual a través de OpenID Connect**.
SSO Type	Tipo de IdP. Una cuenta solo puede tener un tipo de IdP. A continuación se describe el tipo de usuario de IAM. SSO del usuario de IAM: después de que un usuario federado inicie sesión en Huawei Cloud, el sistema asigna automáticamente el **ID de identidad externo** a un usuario de IAM para que el usuario federado tenga los permisos del usuario de IAM asignado. Una cuenta solo puede tener un IdP del tipo de usuario IAM. Si selecciona el inicio de sesión único del usuario de IAM, asegúrese de que ha creado un usuario de IAM y establezca el ID de identidad externo. Para obtener más información, véase **3.1 Creación de un usuario de IAM**.
Status	Estado de IdP. El valor predeterminado es **Enabled**.

Paso 3 Haga clic en **OK**.

----Fin

Configuración del archivo de metadatos del IdP empresarial en Huawei Cloud

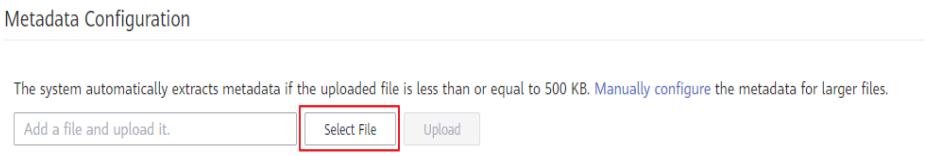
Puede cargar el archivo de metadatos o editar manualmente los metadatos en la consola de IAM. Para un archivo de metadatos de más de 500 KB, configure manualmente los metadatos. Si se han cambiado los metadatos, cargue el último archivo de metadatos o edite los metadatos existentes para garantizar que los usuarios federados puedan iniciar sesión en Huawei Cloud con éxito.

NOTA

Para obtener más información sobre cómo obtener el archivo de metadatos de un IdP de empresa, consulte la documentación de ayuda del IdP de empresa.

- **Cargar un archivo de metadatos.**
  a. Haga clic en **Modify** en la fila que contiene el IdP.
  b. Haga clic en **Select File** y seleccione el archivo de metadatos del IdP de empresa.

  Figura 9-22 Carga de un archivo de metadatos

  c. Haga clic en **Upload**. Se muestran los metadatos extraídos del archivo cargado. Haga clic en **OK**.
     - Si el archivo de metadatos cargado contiene varios IdP, seleccione el IdP que desea usar en la lista desplegable **Entity ID**.

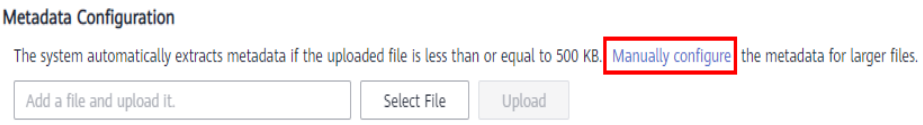
- Si aparece un mensaje que indica que no se ha especificado ningún ID de entidad o que el certificado de firma ha caducado, compruebe el archivo de metadatos y cárguelo de nuevo o configure los metadatos manualmente.

d. Haga clic en **OK** para guardar la configuración.

- **Configurar manualmente los metadatos.**

a. Haga clic en **Manually configure**.

Figura 9-23 Configuración manual de metadatos



b. En el cuadro de diálogo **Configure Metadata**, establezca los parámetros de metadatos, como **Entity ID**, **Signing Certificate** y **SingleSignOnService**.

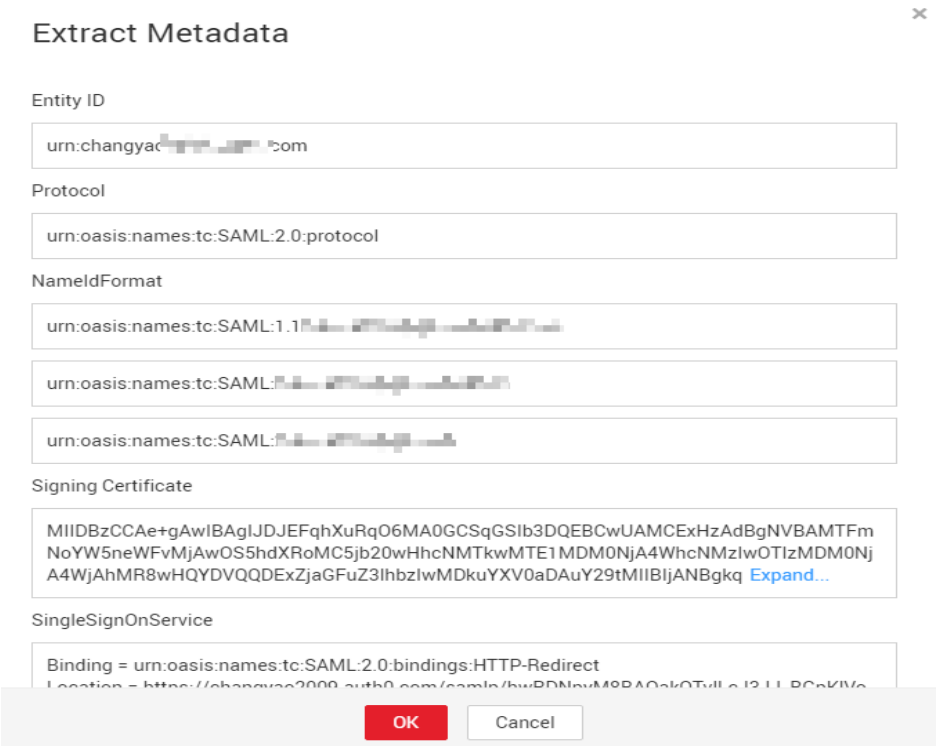
Parámetro	Obligatorio	Descripción
Entity ID	Sí	El identificador único de un IdP. Introduzca el valor del **entityID** que se muestra en el archivo de metadatos del IdP de empresa. Si el archivo de metadatos contiene varios IdP, elija la que desee usar.
Protocol	Sí	Protocolo utilizado para la federación de identidades entre un IdP de empresa y un SP. El protocolo está seleccionado de forma predeterminada.
NameIdFormat	No	Introduzca el valor de **NameIdFormat** que se muestra en el archivo de metadatos IdP. Especifica el formato de identificador de nombre de usuario soportado por el IdP, que se utiliza para la comunicación entre el IdP y el usuario federado. Si configura varios valores, Huawei Cloud utiliza el primer valor de forma predeterminada.

Parámetro	Obligatorio	Descripción
Signing Certificate	Sí	Introduzca el valor de **<X509Certificate>** que se muestra en el archivo de metadatos IdP. Un certificado de firma es un certificado de clave pública utilizado para la verificación de firma. Por motivos de seguridad, introduzca una clave pública que contenga al menos 2,048 bits. El certificado de firma se utiliza durante la federación de identidad para garantizar que las afirmaciones sean creíbles y completas. Si configura varios valores, Huawei Cloud utiliza el primer valor de forma predeterminada.
SingleSignOnService	Sí	Introduzca el valor de **SingleSignOnService** que se muestra en el archivo de metadatos IdP. Este parámetro define cómo se envían las solicitudes SAML durante el inicio de sesión único. Debe ser compatible con HTTP Redirect o HTTP POST. Si configura varios valores, Huawei Cloud utiliza el primer valor de forma predeterminada.
SingleLogoutService	No	Introduzca el valor de **SingleLogoutService** que se muestra en el archivo de metadatos IdP. Este parámetro indica la dirección a la que los usuarios federados serán redirigidos después de cerrar sus sesiones. Debe ser compatible con HTTP Redirect o HTTP POST. Si configura varios valores, Huawei Cloud utiliza el primer valor de forma predeterminada.

En el ejemplo siguiente se muestra el archivo de metadatos de un IdP de empresa y los metadatos configurados manualmente.

Figura 9-24 Archivo de metadatos de un IdP de empresa

Figura 9-25 Configuración manual de metadatos



c. Haga clic en **OK** para guardar la configuración.

9.4.3 Paso 2: Configurar el IdP de la empresa

Puede configurar parámetros en el IdP empresarial para determinar qué información se enviará a Huawei Cloud. Huawei Cloud autentica la identidad federada y asigna permisos basados en la información recibida.

NOTA

Si el tipo de SSO es usuario de IAM, el IdP de empresa debe tener la aserción **IAM_SAML_Attributes_xUserId** configurada.

Parámetros comunes en un IdP de empresa

Tabla 9-7 Parámetros comunes en un IdP de empresa

Parámetro	Descripción	Escenario
IAM_SAML_Attributes_xUserId	ID de un usuario IdP de empresa (usuario federado)	Este parámetro es obligatorio cuando el tipo de SSO es usuario IAM. Cada usuario federado se asigna a un usuario IAM. El **IAM_SAML_Attributes_xUserId** del usuario federado es el mismo que el ID de identidad externo del usuario IAM correspondiente.

Parámetro	Descripción	Escenario
IAM_SAML_Attributes_redirect_url	URL de destino a la que se redirigirá el usuario federado	Durante el inicio de sesión SSO, el usuario federado será redirigido a una página en Huawei Cloud, por ejemplo, la página de inicio de Cloud Eye en la región CN-Hong Kong.
IAM_SAML_Attributes_domain_id	ID de cuenta de Huawei Cloud se federará con el IdP empresarial	Este parámetro es obligatorio en la federación iniciada por IdP de empresa.
IAM_SAML_Attributes_idp_id	Nombre de la entidad IdP creada en Huawei Cloud	Este parámetro es obligatorio en la federación iniciada por IdP de empresa.

9.4.4 Paso 3: Configurar un ID de identidad externo

Para el tipo SSO de usuario de IAM, debe configurar un ID de identidad externo para el usuario de IAM al que el usuario federado asigna en Huawei Cloud. El ID de identidad externo debe ser el mismo que el valor **IAM_SAML_Attributes_xUserId** del usuario IdP de empresa (usuario federado). Puede crear un usuario de IAM y configurar un ID de identidad externo para él, o cambiar el ID de identidad externo de un usuario de IAM existente.

- **Creación de un usuario de IAM y configuración de un ID de identidad externo**
- **Cambio del ID de identidad externo de un usuario de IAM existente**

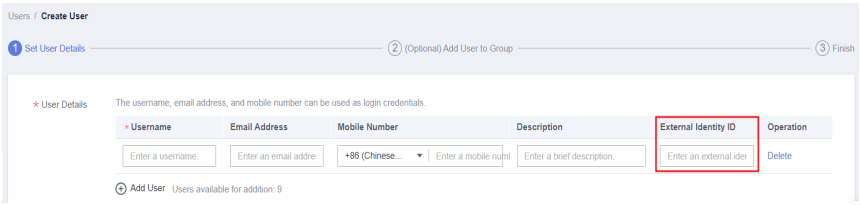
Creación de un usuario de IAM y configuración de un ID de identidad externo

Paso 1 Inicie sesión en la consola de IAM como administrador.

Paso 2 En la consola de IAM, seleccione **Users** en el panel de navegación y haga clic en **Create User** en la esquina superior derecha.

Paso 3 En el área **User Details**, configure un ID de identidad externo. Para obtener más información sobre otras configuraciones, consulte **3.1 Creación de un usuario de IAM**.

Figura 9-26 Configuración de un ID de identidad externo

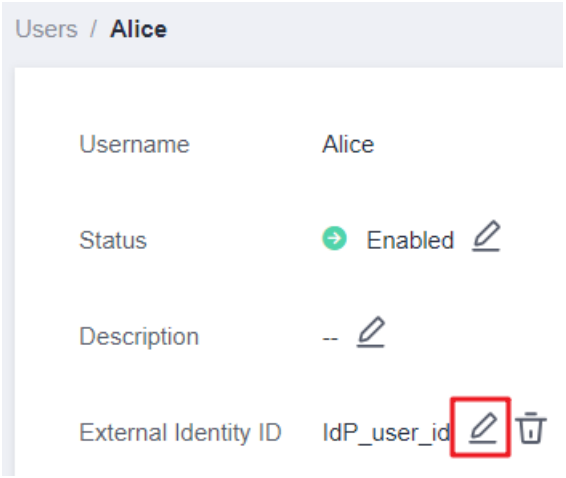


----Fin

Cambio del ID de identidad externo de un usuario de IAM existente

En la lista de usuarios de IAM, haga clic en un nombre de usuario o elija **More** > **Security Settings** en la fila que contiene el usuario y cambie el ID de identidad externo.

Figura 9-27 Cambio del ID de identidad externo de un usuario de IAM existente



9.4.5 Paso 4: Verificar el inicio de sesión federado

Verificación del inicio de sesión federado

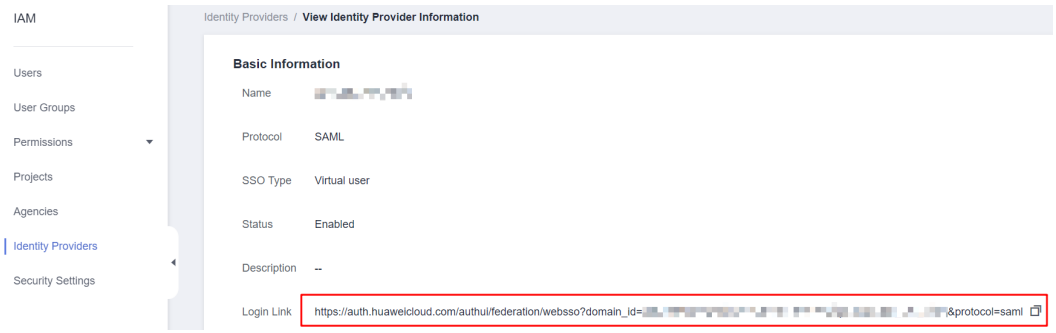
Los usuarios federados pueden iniciar un inicio de sesión desde el IdP o el SP.

- Iniciar un inicio de sesión desde un IdP, por ejemplo, Microsoft Active Directory Federation Services (AD FS) o Shibboleth.
- Iniciar un inicio de sesión desde el SP (). Puede obtener el enlace de inicio de sesión en la página de detalles del IdP en la consola de IAM.

El método de inicio de sesión iniciado por IdP depende del IdP. Para obtener más información, consulte la documentación de ayuda del IdP. Esta sección describe cómo iniciar un inicio de sesión desde el SP.

Paso 1 Inicie sesión como usuario federado.

En la página **Identity Providers** de la consola de IAM, haga clic en **View** en la fila que contiene el IdP. Haga clic en para copiar el vínculo de inicio de sesión que se muestra en el área **Basic Information** y abra el vínculo con un explorador y, a continuación, introduzca el nombre de usuario y la contraseña utilizados en el sistema de gestión empresarial.



Paso 2 Compruebe si el usuario federado está iniciando sesión como usuario IAM.

----Fin

Redirección a una Región o Servicio Especificado

Puede especificar la página de destino a la que el usuario federado será redirigido después de iniciar sesión, por ejemplo, la página de inicio de Cloud Eye en la región CN-Hong Kong.

- Configuración del enlace de inicio de sesión en el SP

  Combine el enlace de inicio de sesión obtenido de la consola con la URL especificada usando el formato **Login link&service=Specified URL**. Por ejemplo, si el enlace de inicio de sesión obtenido es **https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml** y la dirección URL especificada es **https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1**, el enlace de inicio de sesión configurado en el SP es **https://auth.huaweicloud.com/authui/federation/websso?domain_id=XXX&idp=XXX&protocol=saml&service=https://console-intl.huaweicloud.com/ces/?region=ap-southeast-1**
- Configuración del enlace de inicio de sesión en el IdP

  Configure **IAM_SAML_Attributes_redirect_url** (la dirección URL a la que se redirigirá) en la afirmación SAML del IdP de empresa.

9.4.6 (Opcional) Paso 5: Configurar una entrada de inicio de sesión federada en el IdP de empresa

Configure una entrada de inicio de sesión federada en el IdP empresarial para que los usuarios empresariales puedan usar el enlace de inicio de sesión para acceder a Huawei Cloud.

NOTA

Si no desea configurar la entrada de inicio de sesión en su sistema de gestión empresarial, omita esta sección. Huawei Cloud proporciona una entrada de inicio de sesión para usuarios federados. Para obtener más información sobre el inicio de sesión, consulte **Inicio de sesión como usuario federado**.

Prerrequisitos

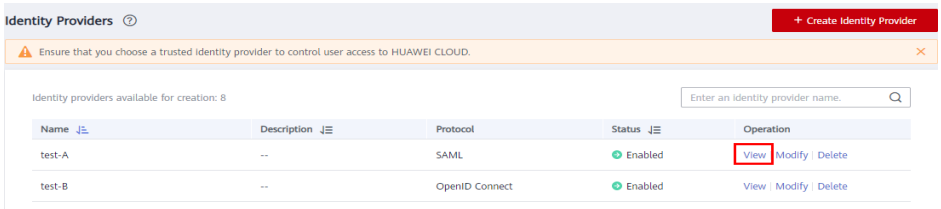
- Se ha creado una entidad IdP en Huawei Cloud, y el enlace de inicio de sesión para el IdP está disponible. Para obtener más información, véase **9.4.2 Paso 1: Crear una entidad IdP**.
- La entrada de inicio de sesión para iniciar sesión en Huawei Cloud se ha configurado en el sistema de gestión empresarial.

Procedimiento

Paso 1 Inicie sesión en la **consola de IAM**. En el panel de navegación, elija **Identity Providers**.

Paso 2 Haga clic en **View** en la fila que contiene el IdP.

Figura 9-28 Consulta de los detalles del IdP



Paso 3 Copie el enlace de inicio de sesión haciendo clic en en la fila **Login Link**.

Figura 9-29 Copia del enlace de inicio de sesión

Paso 4 Agregue la siguiente instrucción al archivo de página del sistema de gestión empresarial:

```
<a href="<Login link>"> Huawei Cloud login entry </a>
```

Paso 5 Inicie sesión en el sistema de gestión empresarial con su cuenta empresarial y haga clic en el enlace de inicio de sesión configurado para acceder a Huawei Cloud.

----Fin

9.5 SSO de usuario virtual a través de OpenID Connect

9.5.1 Descripción general del inicio de sesión único del usuario virtual mediante OpenID Connect

Esta sección describe cómo configurar la federación de identidades y cómo funciona la federación de identidades.

Configuración de la federación de identidades

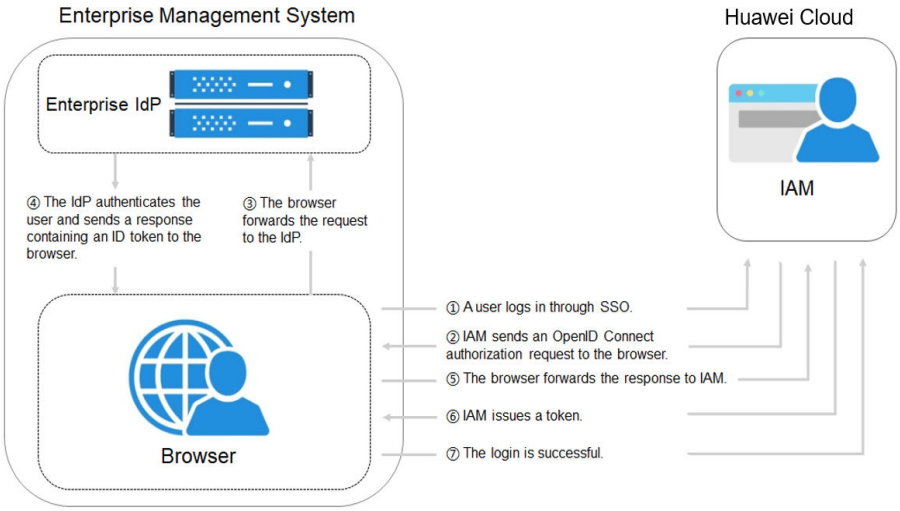
A continuación se describe cómo configurar su IdP empresarial y Huawei Cloud para que confíen entre sí.

1. **Crear una entidad IdP y establecer una relación de confianza**: Cree credenciales OAuth 2.0 en el IdP de empresa. En Huawei Cloud, cree una entidad IdP y establezca una relación de confianza entre los dos sistemas.
2. **Configurar reglas de conversión de identidad**: Configure reglas de conversión de identidad en Huawei Cloud para asignar los usuarios, grupos de usuarios y permisos en el IdP empresarial a Huawei Cloud.
3. **Configurar una entrada de inicio de sesión federada**: Configure el enlace de inicio de sesión en el IdP empresarial para permitir que los usuarios empresariales sean redirigidos a Huawei Cloud desde su sistema de gestión empresarial.

Cómo funciona la federación de identidades

Figura 9-30 muestra el proceso de federación de identidades entre un sistema de gestión empresarial y Huawei Cloud.

Figura 9-30 Cómo funciona la federación de identidades



El proceso de federación de identidades es el siguiente:

1. Un usuario abre el enlace de inicio de sesión obtenido de la consola IAM en el navegador. El navegador envía una solicitud de inicio de sesión único a Huawei Cloud.
2. Huawei Cloud autentica al usuario contra la configuración del IdP empresarial y crea una solicitud OpenID Connect al navegador.
3. El navegador reenvía la solicitud OpenID Connect al IdP de empresa.
4. El usuario introduce su nombre de usuario y contraseña en la página de inicio de sesión que se muestra en el IdP de empresa. Después de que el IdP de empresa autentica la identidad del usuario, construye un token de ID que contiene la información del usuario y envía el token de ID al navegador como respuesta de autorización de OpenID Connect.
5. El navegador responde y reenvía la respuesta de OpenID Connect a Huawei Cloud.
6. Huawei Cloud analiza el token de ID en la respuesta de OpenID Connect, identifica el grupo de usuarios de IAM asignado al usuario según las reglas de conversión de identidad y emite un token al usuario.
7. El inicio de sesión SSO se realiza correctamente.

9.5.2 Paso 1: Crear una entidad IdP

Para establecer una relación de confianza entre un IdP empresarial y Huawei Cloud, establezca las URL de redirección del usuario y cree credenciales de OAuth 2.0 en el IdP empresarial. En la consola IAM, cree una entidad IdP y configure la información de autorización.

Prerrequisitos

- El administrador de la empresa ha creado una cuenta en Huawei Cloud, y ha creado grupos de usuarios y les ha asignado permisos en IAM. Para más detalles, consulte **4.1 Creación de un grupo de usuarios y asignación de permisos**. Los grupos de usuarios creados en IAM se asignarán a los usuarios federados para que los usuarios federados puedan obtener los permisos de los grupos de usuarios para usar los recursos de Huawei Cloud.

- El administrador de la empresa ha leído la documentación de ayuda del IdP de la empresa o ha entendido cómo utilizar el IdP de la empresa. Las configuraciones de diferentes IdPs empresariales difieren mucho, por lo que no se describen en este documento. Para obtener detalles sobre cómo obtener las credenciales de OAuth 2.0 de un IdP empresarial, consulte la documentación de ayuda de IdP.

Creación de credenciales de OAuth 2.0 en el IdP empresarial

Paso 1 Establezca las URL de redirección **https:///authui/oidc/redirect** y **https:///authui/oidc/post** en el IdP empresarial para que los usuarios puedan ser redirigidos al IdP de OpenID Connect en Huawei Cloud.

Paso 2 Obtenga las credenciales de OAuth 2.0 del IdP empresarial.

----Fin

Creación de una entidad IdP en Huawei Cloud

Crear una entidad IdP y configurar la información de autorización en IAM para establecer una relación de confianza entre el IdP de la empresa y el IAM

Paso 1 Inicie sesión en la **consola de IAM**, elija **Identity Providers** en el panel de navegación y haga clic en **Create Identity Provider** en la esquina superior derecha.

Paso 2 Escriba un nombre de IdP, seleccione **OpenID Connect** y **Enabled** y haga clic en **OK**.

NOTA

El nombre IdP debe ser único en su cuenta. Se recomienda utilizar el nombre de dominio.

----Fin

Configuración de la información de autorización en Huawei Cloud

Paso 1 Haga clic en **Modify** en la columna **Operation** de la fila que contiene el IdP que desea modificar.

Paso 2 Seleccione un tipo de acceso.

Tabla 9-8 Descripción del tipo de acceso

Tipo de acceso	Descripción
Acceso programático y acceso a la consola de gestión	● Acceso programático: Los usuarios federados pueden utilizar herramientas de desarrollo (incluidas API, CLI y SDK) que admiten la autenticación clave para acceder a Huawei Cloud. ● Acceso a la consola de administración: los usuarios federados pueden iniciar sesión en Huawei Cloud con sus propios nombres de usuario y contraseñas. Seleccione este tipo de acceso si desea que los usuarios accedan a Huawei Cloud a través de SSO.

Tipo de acceso	Descripción
Acceso programático	Los usuarios federados solo pueden usar herramientas de desarrollo (incluidas API, CLI y SDK) que admitan autenticación clave para acceder a Huawei Cloud.

Paso 3 Especifique la información de configuración.

Tabla 9-9 Información de configuración

Parámetro	Descripción
Identity Provider URL	URL del IdP de OpenID Connect. Establezca el valor de **issuer** en el **Openid-configuration**. **NOTA** **Openid-configuration** indica una dirección URL definida en OpenID Connect, que contiene configuraciones de un IdP de empresa. El formato de URL es de **https://***{base URL}***/.well-known/openid-configuration**, donde la *base URL* es definida por el IdP de la empresa. Por ejemplo, la **Openid-configuration** de Google es de **https://accounts.google.com/.well-known/openid-configuration**.
Client ID	ID de un cliente registrado con el IdP de OpenID Connect. El ID de cliente es **una credencial de OAuth 2.0 creada en el IdP de empresa**.
Authorization Endpoint	Punto de conexión de autorización del IdP de OpenID Connect. Establezca el valor de **authorization_endpoint** en **Openid-configuration**. Este parámetro solo es necesario si se establece **Access Type** en **Programmatic access and management console access**.
Scopes	Ámbitos de las solicitudes de autorización. **openid** está seleccionado por defecto. Este parámetro solo es necesario si se establece **Access Type** en **Programmatic access and management console access**. Valores enumerados: ● openid ● email ● profile
Response Type	Tipo de respuesta de solicitudes de autorización. El valor predeterminado es **id_token**. Este parámetro solo es necesario si se establece **Access Type** en **Programmatic access and management console access**.

Parámetro	Descripción
Response Mode	Modo de respuesta de solicitudes de autorización. Las opciones incluyen **form_post** y **fragment**. **form_post** es recomendado. ● **form_post**: Si se selecciona este modo, configure la URL de redirección a **https:///authui/oidc/post** en el IdP de empresa. ● **fragment**: si se selecciona este modo, establezca la URL de redirección a **https:///authui/oidc/redirect** en el IdP de empresa. Este parámetro solo es necesario si se establece **Access Type** en **Programmatic access and management console access**.
Signing Key	Clave pública utilizada para firmar el token de ID del IdP de OpenID Connect. Por motivos de seguridad de la cuenta, cambie la clave de firma periódicamente.

Paso 4 Haga clic en **OK**.

----Fin

Verificación del inicio de sesión federado

Paso 1 Haga clic en el enlace de inicio de sesión que se muestra en la página de detalles del IdP y compruebe si se muestra la página de inicio de sesión del servidor IdP empresarial.

1. En la página **Identity Providers**, haga clic en **Modify** en la columna **Operation** del proveedor de identidad.
2. Copie el enlace de inicio de sesión que se muestra en la página **Modify Identity Provider** y visite el enlace usando un navegador.
3. Si no se muestra la página de inicio de sesión de IdP de empresa, compruebe las configuraciones del IdP y del servidor IdP de empresa.

Paso 2 Introduzca el nombre de usuario y la contraseña de un usuario creado en el sistema de gestión empresarial.

- Si el inicio de sesión se realiza correctamente, agregue el enlace de inicio de sesión al sistema de gestión empresarial.
- Si el inicio de sesión falla, compruebe el nombre de usuario y la contraseña.

NOTA

Los usuarios federados solo pueden acceder a Huawei Cloud de forma predeterminada. Para asignar permisos a usuarios federados, configure las reglas de conversión de identidad para el IdP. Para obtener más información, véase **9.5.3 Paso 2: Configurar reglas de conversión de identidad**.

----Fin

Operaciones relacionadas

- Consulta de información de IdP: En la lista IdP, haga clic en **View** en la fila que contiene el IdP y vea su información básica, configuración de metadatos y reglas de conversión de identidad.

> NOTA
>
> Para modificar la configuración de un IdP, haga clic en **Modify** en la parte inferior de la página de detalles.

- Modificación de un IdP: En la lista IdP, haga clic en **Modify** en la fila que contiene el IdP y, a continuación, cambie su estado o modifique la descripción, metadatos o reglas de conversión de identidad.
- Eliminación de un IdP: En la lista IdP, haga clic en **Delete** en la fila que contiene el IdP y haga clic en **Yes** en el cuadro de diálogo mostrado.

Acciones posteriores

- Configure reglas de conversión de identidad para asignar usuarios de IdP de empresa a grupos de usuarios de IAM y asignar permisos a los usuarios. Para obtener más información, véase **9.5.3 Paso 2: Configurar reglas de conversión de identidad**.
- Configure el sistema de gestión empresarial para permitir a los usuarios acceder a Huawei Cloud a través de SSO. Para obtener más información, véase **9.5.4 (Opcional) Paso 3: Configurar el enlace de inicio de sesión en el sistema de gestión empresarial**.

9.5.3 Paso 2: Configurar reglas de conversión de identidad

Los usuarios federados reciben el nombre de **FederationUser** de forma predeterminada en Huawei Cloud. Estos usuarios solo pueden iniciar sesión en Huawei Cloud y no tienen ningún otro permiso. Puede configurar reglas de conversión de identidad en la consola de IAM para lograr lo siguiente:

- Mostrar usuarios empresariales con diferentes nombres en Huawei Cloud.
- Asigne permisos a los usuarios empresariales para usar recursos de Huawei Cloud asignando estos usuarios a grupos de usuarios de IAM. Asegurarse de que ha creado los grupos de usuarios necesarios. Para obtener más información, véase **4.1 Creación de un grupo de usuarios y asignación de permisos**.

> NOTA
>
> - Las modificaciones a las reglas de conversión de identidad solo tendrán efecto después de que los usuarios federados vuelvan a iniciar sesión.
> - Para modificar los permisos de un usuario, modifique los permisos del grupo de usuarios al que pertenece el usuario. A continuación, reinicie el IdP de empresa para que las modificaciones surtan efecto.

Prerrequisitos

Se ha creado una entidad IdP y se puede acceder al enlace de inicio de sesión del IdP. (Para obtener más información sobre cómo crear y verificar una entidad IdP, consulte **9.5.2 Paso 1: Crear una entidad IdP**.)

Procedimiento

Si configura reglas de conversión de identidad haciendo clic en **Create Rule**, IAM convierte los parámetros de regla al formato JSON. Alternativamente, puede hacer clic en **Edit Rule** para configurar reglas en formato JSON. Para obtener más información, véase **9.6 Sintaxis de las reglas de conversión de identidad**.

- **Creación de reglas**

a. Inicie sesión en la **consola de IAM** como administrador. En el panel de navegación, elija **Identity Providers**.

b. En la lista IdP, haga clic en **Modify** en la fila que contiene el IdP.

c. En el área **Identity Conversion Rules**, haga clic en **Create Rule**. A continuación, configure las reglas en el cuadro de diálogo **Create Rule**.

Figura 9-31 Creación de reglas

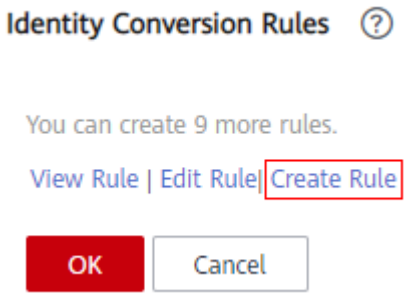


Figura 9-32 Configuración de parámetros

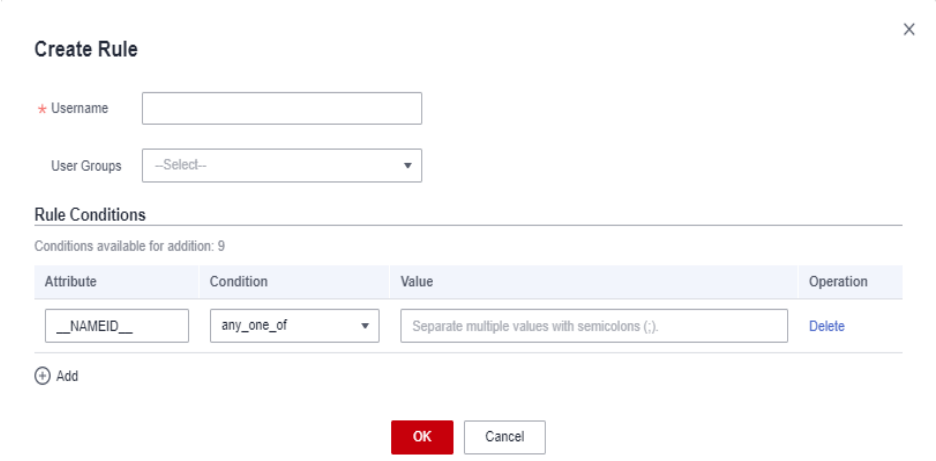


Tabla 9-10 Descripción del parámetro

Parámetro	Descripción	Observaciones
Username	Nombre de usuario de los usuarios federados en Huawei Cloud.	Para distinguir a los usuarios federados de los usuarios de Huawei Cloud, se recomienda que establezca el nombre de usuario en **FederationUser-***IdP_XXX*. *IdP* indica un nombre de IdP, por ejemplo, AD FS o Shibboleth. *XXX* indica un nombre personalizado. **AVISO** ● El nombre de usuario de cada usuario federado debe ser único en el mismo IdP. Los usuarios federados con los mismos nombres de usuario en el mismo IdP se asignarán al mismo usuario IAM en Huawei Cloud. ● El nombre de usuario solo puede contener letras, dígitos, espacios, guiones (-) guiones bajos (_) y puntos (.). No puede comenzar con un dígito y no puede contener el siguiente characters: ", \", \\, \n, \r
User Groups	Grupos de usuarios a los que pertenecen los usuarios federados en Huawei Cloud.	Los usuarios federados heredarán permisos de sus grupos de usuarios. Puede seleccionar un grupo de usuarios que ya se haya creado.
Rule Conditions	Condiciones que debe cumplir un usuario federado para obtener permisos de los grupos de usuarios seleccionados.	Los usuarios federados que no cumplan estas condiciones no pueden acceder a Huawei Cloud. Puede crear un máximo de 10 condiciones para una regla de conversión de identidad. **NOTA** ● Una regla de conversión de identidad puede tener varias condiciones. Solo tiene efecto si se cumplen todas las condiciones. ● Un IdP puede tener varias reglas de conversión de identidad. Si un usuario federado no cumple con ninguna de las condiciones, se le denegará el acceso a Huawei Cloud.

Por ejemplo, establezca una regla de conversión de identidad para los administradores del sistema de gestión empresarial.

- Nombre de usuario: **FederationUser-IdP_admin**
- Grupo de usuarios: **admin**
- Condición de regla: **_NAMEID_** (atributo), **any_one_of** (condición) y **000000001** (valor).

  Solo el usuario con ID 000000001 se asigna al usuario de IAM **FederationUser-IdP_admin** y hereda los permisos del grupo de usuarios **admin**.

d. En el cuadro de diálogo **Create Rule**, haga clic en **OK**.

e. En la página **Modify Identity Provider**, haga clic en **OK**.

- **Edición de reglas**

a. Inicie sesión en la **consola de IAM** como administrador. En el panel de navegación, elija **Identity Providers**.

b. En la lista IdP, haga clic en **Modify** en la fila que contiene el IdP.

c. En el área **Identity Conversion Rules**, haga clic en **Edit Rule**.

d. Edite las reglas de conversión de identidad en formato JSON. Para obtener más información, véase **9.6 Sintaxis de las reglas de conversión de identidad**.

e. Haga clic en **Validate** para verificar la sintaxis de las reglas.

f. Si la regla es correcta, haga clic en **OK** en el cuadro de diálogo **Edit Rule** y haga clic en **OK** en la página **Modify Identity Provider**.

Si aparece un mensaje que indica que el archivo JSON está incompleto, modifique las instrucciones o haga clic en **Cancel** para cancelar las modificaciones.

Verificación de permisos de usuario federados

Después de configurar las reglas de conversión de identidad, compruebe los permisos de los usuarios federados.

Paso 1 Inicie sesión como usuario federado.

En la página **Identity Providers** de la consola de IAM, haga clic en **View** en la fila que contiene el IdP. Haga clic en para copiar el vínculo de inicio de sesión que se muestra en el área **Basic Information** y abra el vínculo con un explorador y, a continuación, introduzca el nombre de usuario y la contraseña utilizados en el sistema de gestión empresarial.

Paso 2 Compruebe que el usuario federado tiene los permisos asignados a su grupo de usuarios.

Por ejemplo, configure una regla de conversión de identidad para asignar el usuario federado **ID1** al grupo de usuarios **admin** para que **ID1** tenga permisos completos para todos los servicios en la nube. En la consola de gestión, seleccione un servicio en la nube y compruebe si puede acceder al servicio.

----Fin

Operaciones relacionadas

Ver reglas de conversión de identidad: haga clic en **View Rule** en la página **Modify Identity Provider**. Las reglas de conversión de identidad se muestran en formato JSON. Para obtener más información sobre el formato JSON, consulte **Sintaxis de reglas de conversión de identidad**.

9.5.4 (Opcional) Paso 3: Configurar el enlace de inicio de sesión en el sistema de gestión empresarial

Configure una entrada de inicio de sesión federada en el IdP empresarial para que los usuarios empresariales puedan usar el enlace de inicio de sesión para acceder a Huawei Cloud.

> **NOTA**
>
> Si no se ha configurado ningún enlace de inicio de sesión en su sistema de gestión empresarial, los usuarios federados de su empresa pueden iniciar sesión en Huawei Cloud a través de la página de inicio de sesión de Huawei Cloud. Para obtener más información, véase **Inicio de sesión como usuario federado**.

Prerrequisitos

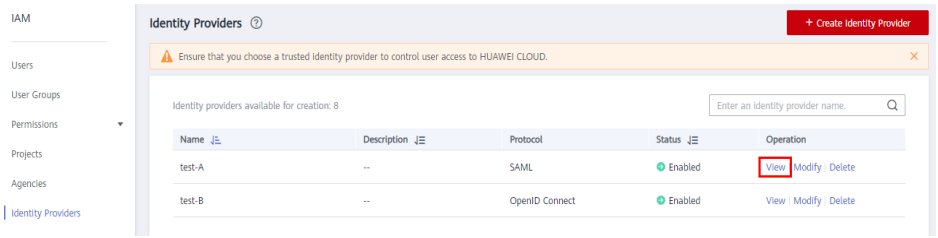
- Se ha creado una entidad IdP en Huawei Cloud. Para obtener más información acerca de cómo crear una entidad IdP, consulte **9.3.2 Paso 1: Crear una entidad IdP**.
- La entrada de inicio de sesión para iniciar sesión en Huawei Cloud se ha configurado en el sistema de gestión empresarial.

Procedimiento

Paso 1 Inicie sesión en la **consola de IAM**. En el panel de navegación, elija **Identity Providers**.

Paso 2 Haga clic en **View** en la fila que contiene el IdP.

Figura 9-33 Consulta de los detalles del IdP



Paso 3 Copie el enlace de inicio de sesión haciendo clic en en la fila **Login Link**.

Figura 9-34 Copia del enlace de inicio de sesión

Paso 4 Agregue la siguiente instrucción al archivo de página del sistema de gestión empresarial:

```
<a href="<Login link>"> Huawei Cloud login entry </a>
```

Paso 5 Inicie sesión en el sistema de gestión empresarial con su cuenta empresarial y haga clic en el enlace de inicio de sesión configurado para acceder a Huawei Cloud.

----Fin

9.6 Sintaxis de las reglas de conversión de identidad

Una regla de conversión de identidad es un objeto JSON que se puede modificar. El siguiente es un ejemplo de objeto JSON:

```
[
        {
                "local": [
                        {
                                "<user> or <group> or <groups>"
                        }
                ],
                "remote": [
                        {
                                "<condition>"
                        }
                ]
        }
]
```

Descripción de parámetros:

- **local**: información de identidad de un usuario federado asignado a IAM. El valor de este campo puede contener marcadores de posición, como **{0...n}**. Los atributos **{0}** y **{1}** representan los atributos remotos primero y segundo de la información de usuario, respectivamente.
- **remote**: Información sobre un usuario federado del IdP. Este campo es una expresión que consiste en atributos de aserción y operadores. El valor de este campo viene determinado por la aserción.
  - **condition**: Condiciones para que la regla de conversión de identidad entre en vigor. Se admiten los siguientes tres tipos de condiciones:
    - **empty**: la regla coincide con todas las notificaciones que contienen el tipo de atributo. No es necesario especificar esta condición. El resultado de la condición es el argumento que se pasa como entrada.
    - **any_one_of**: La regla solo coincide si alguna de las cadenas especificadas aparece en el tipo de atributo. El resultado de la condición es booleano, no el argumento que se pasa como entrada.
    - **not_any_of**: La regla no coincide si alguna de las cadenas especificadas aparece en el tipo de atributo. El resultado de la condición es booleano, no el argumento que se pasa como entrada.

AVISO

La información de usuario asignada a IAM solo puede contener letras, dígitos, espacios, guiones (-) guiones bajos y puntos (.), y no puede comenzar con un dígito.

Ejemplos de la condición empty

La condición **empty** devuelve cadenas de caracteres para reemplazar los atributos locales **{0..n}**.

- En el siguiente ejemplo, el nombre de usuario de un usuario federado será, "el valor del primer atributo remoto+espacio+el valor del segundo atributo remoto" en IAM, es decir,

FirstName LastName. El grupo al que pertenece el usuario es el valor del tercer atributo remoto *Group*. Este atributo solo tiene un valor.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0} {1}"
                    }
                },
                {
                    "group": {
                        "name": "{2}"
                    }
                }
            ],
            "remote": [
                {
                    "type": "FirstName"
                },
                {
                    "type": "LastName"
                },
                {
                    "type": "Group"
                }
            ]
        }
]
```

Si se recibe la siguiente aserción (simplificada para una fácil comprensión), el nombre de usuario del usuario federado será **John Smith** y el usuario solo pertenecerá al grupo de **admin**.

```
{FirstName: John}
{LastName: Smith}
{Group: admin}
```

- Si un usuario federado pertenecerá a varios grupos de usuarios en IAM, la regla de conversión de identidad se puede configurar de la siguiente manera:

  En el siguiente ejemplo, el nombre de usuario de un usuario federado será, "el valor del primer atributo remoto+espacio+el valor del segundo atributo remoto" en IAM, es decir, *FirstName LastName*. Los grupos a los que pertenece el usuario son el valor del tercer atributo remoto *Groups*.

  ```
  [
          {
              "local": [
                  {
                      "user": {
                          "name": "{0} {1}"
                      }
                  },
                  {
                      "group":   {
                          "name": "{2}"
                      }
                  }
              ],
              "remote": [
                  {
                      "type": "FirstName"
                  },
                  {
                      "type": "LastName"
                  },
                  {
                      "type": "Groups"
  ```



```
                }
            ]
        }
]
```

Si se recibe la siguiente aserción, el nombre de usuario del usuario federado será **John Smith** y el usuario pertenecerá a los grupos de **admin** y **manager**.

```
{FirstName: John}
{LastName: Smith}
{Groups: [admin, manager]}
```

Ejemplos de condiciones "any one of" y "not any of"

A diferencia de la condición **empty**, **any one of** y **not any of** ellas devuelven valores booleanos. Estos valores no se utilizarán para reemplazar los atributos locales. En el siguiente ejemplo, solo **{0}** será reemplazado por el valor devuelto de la primera condición de **empty** en el bloque **remote**. El valor de **group** se fija como **admin**.

- El UserName del usuario federado en IAM es el valor del primer atributo remoto, es decir, el *UserName*. El usuario federado pertenece al grupo de **admin**. Esta regla solo tiene efecto para los usuarios que son miembros del grupo **idp_admin** en el IdP.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                        "name": "admin"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "any_one_of": [
                        "idp_admin"
                    ]
                }
            ]
        }
]
```

- Si un usuario federado pertenecerá a varios grupos de usuarios en IAM, la regla de conversión de identidad se puede configurar de la siguiente manera:

  El UserName del usuario federado en IAM es el valor del primer atributo remoto, es decir, el *UserName*. El usuario federado pertenece a los grupos de **admin** y **manager**. Esta regla solo tiene efecto para los usuarios que son miembros del grupo **idp_admin** en el IdP.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
```



```
                            "name":"admin"
                    }
                },
                {
                    "group": {
                            "name":"manager"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "any_one_of": [
                        "idp_admin"
                    ]
                }
            ]
        }
]
```

– La siguiente afirmación indica que el usuario federado John Smith es miembro del grupo **idp_admin**. Por lo tanto, el usuario puede acceder a Huawei Cloud.

```
{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}
```

– La siguiente afirmación indica que el usuario federado John Smith no es miembro del grupo **idp_admin**. Por lo tanto, la regla no tiene efecto para el usuario y el usuario no puede acceder a Huawei Cloud.

```
{UserName: John Smith}
{Groups: [idp_user, idp_agency]}
```

Ejemplo de condición que contiene una expresión regular

Puede agregar **"regex": true** a una condición para calcular los resultados usando una expresión regular.

Esta regla entra en vigor para cualquier usuario cuyo nombre de usuario termine en **@mail.com**. El UserName de cada usuario federado aplicable es el *UserName* en IAM y el usuario pertenece al grupo de **admin**.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                        "name": "admin"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "any_one_of": [
                        ".*@mail.com$"
                    ],
                    "regex": true
                }
```



```
            ]
        }
]
```

Ejemplos de condiciones combinadas

Se pueden combinar múltiples condiciones usando el operador lógico AND.

Esta regla solo tiene efecto para los usuarios federados que no pertenecen al grupo de usuarios **idp_user** o **idp_agent** en el IdP. El UserName de cada usuario federado aplicable es el *UserName* en IAM y el usuario pertenece al grupo de **admin**.

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                        "name": "admin"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "not_any_of": [
                        "idp_user"
                    ]
                },
                {
                    "type": "Groups",
                    "not_any_of": [
                        "idp_agent"
                    ]
                }
            ]
        }
]
```

La regla anterior es equivalente a la siguiente:

```
[
        {
            "local": [
                {
                    "user": {
                        "name": "{0}"
                    }
                },
                {
                    "group": {
                        "name": "admin"
                    }
                }
            ],
            "remote": [
                {
                "type": "UserName"
                },
                {
                    "type": "Groups",
                    "not_any_of": [
```



```
                        "idp_user",
                        "idp_agent"
                    ]
                }
            ]
        }
]
```

Ejemplos de reglas combinadas

Si se combinan varias reglas, los métodos para coincidir nombres de usuario y grupos de usuarios son diferentes.

El nombre de un usuario federado será el nombre de usuario coincidente en la primera regla que surta efecto, y el usuario pertenecerá a todos los grupos coincidentes en todas las reglas que suban efecto. Un usuario federado solo puede iniciar sesión si al menos una regla entra en vigor para que coincida con el nombre de usuario. Para una fácil comprensión, las reglas de nombre de usuario y grupo de usuarios se pueden configurar por separado.

En el siguiente ejemplo, las reglas tienen efecto para los usuarios del grupo **idp_admin**. El UserName de cada usuario federado aplicable es el *UserName* en IAM y el usuario pertenece al grupo de **admin**.

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}"
                }
            }
        ],
        "remote": [
            {
                "type": "UserName"
            }
        ]
    },
    {
        "local": [
            {
                "group": {
                    "name": "admin"
                }
            }
        ],
        "remote": [
            {
                "type": "Groups",
                "any_one_of": [
                    "idp_admin"
                ]
            }
        ]
    }
]
```

La siguiente afirmación indica que el usuario John Smith es miembro del grupo **idp_admin** en el IdP y, por lo tanto, cumple con las reglas. El nombre de usuario de este usuario será **John Smith** en IAM, y el usuario pertenecerá al grupo de **admin**.

```
{UserName: John Smith}
{Groups: [idp_user, idp_admin, idp_agency]}
```


10 Broker de identidades personalizado

10.1 Habilitación del acceso de agente de identidad personalizado con una delegación

Si el IdP de su empresa no es compatible con SAML o OpenID Connect, puede crear un agente de identidad personalizado para habilitar el acceso a Huawei Cloud. Puede escribir y ejecutar código para generar una URL de inicio de sesión. Los usuarios de su empresa pueden usar la URL para iniciar sesión en Huawei Cloud. Los usuarios serán autenticados por su IdP de empresa.

NOTA

Si su IdP empresarial es compatible con SAML u OpenID Connect, configure **autenticación de identidad federada** para permitir que los usuarios de su empresa accedan a Huawei Cloud a través de SSO.

Prerrequisitos

- Su empresa tiene un sistema de gestión empresarial.
- Ha registrado una cuenta (por ejemplo, **DomainA**) en Huawei Cloud como administrador empresarial y ha creado un grupo de usuarios (por ejemplo, **GroupC**) y le ha asignado el rol de **Agent Operator**. (Para obtener más información, consulte **Creación de un grupo de usuarios y asignación de permisos**.)

Procedimiento

Paso 1 Utilice la cuenta **DomainA** para crear un usuario de IAM (por ejemplo, **UserB**) y agregar el usuario a **GroupC** siguiendo las instrucciones de **Agregar usuarios a un grupo de usuarios**.

NOTA

Asegúrese de que el usuario de IAM pueda **programmatically access** a los servicios de Huawei Cloud. Para obtener más información sobre cómo cambiar el tipo de acceso, consulte **3.4 Consulta o modificación de información de usuario de IAM**.

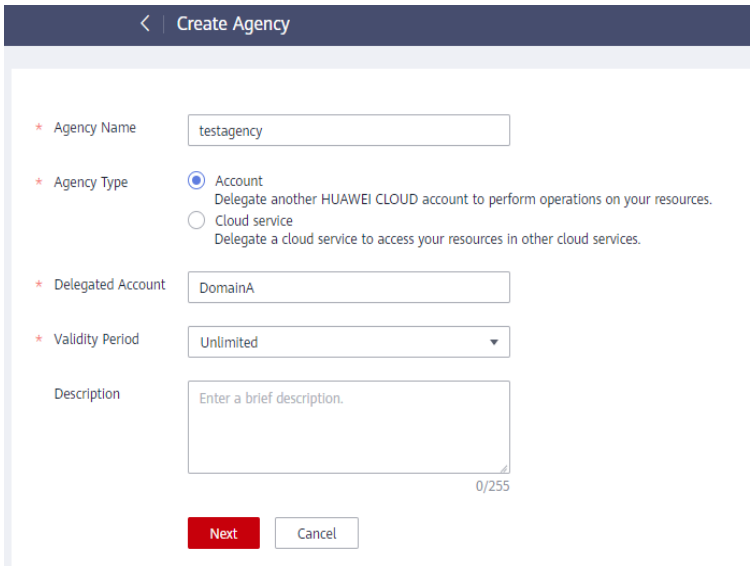
Paso 2 Configure la **clave de acceso** (recomendada) o el nombre de usuario y la contraseña de **UserB** en el archivo de configuración de su IdP de empresa para que el usuario pueda obtener un token para invocar a las API. Para la seguridad de la cuenta, cifre la contraseña y la clave de acceso antes de almacenarlos.

Paso 3 En el panel de navegación de la consola de IAM, seleccione **Agencies**. A continuación, haga clic en **Create Agency** en la esquina superior derecha.

Paso 4 Establezca los parámetros de la agencia.

Por ejemplo, establezca el nombre de la agencia en **testagency**, el tipo de agencia en **Account** y la cuenta delegada en **DomainA**. Establezca el período de validez y haga clic en **Next**.

Figura 10-1 Creación de una delegación



Paso 5 Establezca el ámbito de autorización y seleccione los permisos que desea conceder a la delegación.

Paso 6 En el IdP de empresa, cree un grupo de usuarios llamado **testagency** (igual que el nombre de la agencia creada en **Paso 4**), agregue usuarios de empresa al grupo y conceda a los usuarios permisos para iniciar sesión en Huawei Cloud a través de un agente de identidad personalizado. Para obtener más información, consulte la documentación del IdP empresarial.

Paso 7 Después de que un usuario de empresa inicie sesión en el sistema de gestión de empresa, el usuario puede acceder al agente de identidad personalizado del IdP de empresa seleccionando una agencia de la lista de agencias. El usuario puede obtener la agencia del administrador de seguridad o del usuario root. Para obtener más información, consulte la documentación del sistema de gestión empresarial.

NOTA

Las agencias del agente de identidad deben existir en Huawei Cloud y tener los mismos nombres que algunos grupos de usuarios creados en el IdP empresarial.

Paso 8 El agente de identidad personalizado utiliza el token de **userB** para llamar a la API **POST / v3.0/OS-CREDENTIAL/securitytokens** usados para obtener un securityToken temporal. Para obtener más información, consulte **Obtención de una clave de acceso temporal y SecurityToken a través de una delegación**.

NOTA

Cuando obtenga un securityToken con una agencia, establezca el parámetro **session_user.name** en el cuerpo de la solicitud.

Paso 9 El agente de identidad personalizado utiliza la clave de acceso temporal, securityToken y el nombre de dominio global de IAM () para invocar a la API **POST /v3.0/OS-AUTH/securitytoken/logintokens** para obtener un loginToken. El valor de **X-Subject-LoginToken** en el encabezado de respuesta es un loginToken. Para obtener más información, consulte **Obtención de un LoginToken**.

NOTA

- Para obtener un loginToken invocando a la API **POST /v3.0/OS-AUTH/securitytoken/logintokens**, utilice el nombre de dominio global () de IAM.
- Un loginToken se emite a un usuario para iniciar sesión a través de un agente de identidad personalizado y contiene información de identidad y sesión sobre el usuario. Un loginToken es válido durante 10 minutos por defecto. Las LoginTokens son necesarias para la autenticación cuando los usuarios inician sesión en una consola de servicio con el FederationProxyUrl.
- Puede establecer el período de validez de un loginToken mediante invocación a la API **POST / v3.0/OS-AUTH/securitytoken/logintokens**. El período de validez oscila entre 10 minutos y 12 horas. Si el valor especificado es mayor que el período de validez restante del SecurityToken temporal, se utiliza el período de validez restante del SecurityToken temporal.

Paso 10 El agente de identidad personalizado genera un FederationProxyUrl y lo devuelve al navegador a través de **Location**. El FederationProxyUrl tendrá el siguiente formato:

https:///authui/federation/login?idp_login_url={enterprise_system_loginURL}&service={console_service_region_url}*&logintoken={logintoken}*

Ejemplo:

*https:///authui/federation/login?idp_login_url=https%3A%2F%2Fexample.com&service=https%3a%2f%2f%2fapm%2f%3fregion%3dcn-north-4%23%2fapm%2fatps%2ftopology&logintoken=******

Tabla 10-1 Descripción del parámetro

Parámetro	Descripción
idp_login_url	URL de inicio de sesión del sistema de gestión empresarial.
service	Dirección de acceso de un servicio Huawei Cloud.
logintoken	LoginToken del agente de identidad personalizado.

Para obtener más información sobre cómo crear un FederationProxyUrl consulte el ejemplo proporcionado en **10.2 Creación de un FederationProxyUrl mediante una agencia**.

NOTA

El FederationProxyUrl contiene el loginToken que se ha obtenido de IAM, y está codificado por ciento.

Paso 11 Si el loginToken se autentica correctamente, los usuarios federados serán redirigidos automáticamente a la dirección de servicio de Huawei Cloud especificada en el parámetro de **service**.

Si el loginToken no se autentica, los usuarios serán redirigidos a la dirección especificada en **idp_login_url**.

----Fin

10.2 Creación de un FederationProxyUrl mediante una agencia

En esta sección se proporciona un ejemplo de código utilizado para crear un FederationProxyUrl mediante una agencia para iniciar sesión en los servicios de Huawei Cloud.

Ejemplo de código usando Java

El siguiente código Java muestra cómo crear un FederationProxyUrl que da a los usuarios federados acceso directo a la consola de Huawei Cloud.

```
import java.net.*;
import java.util.Collections;
import com.huaweicloud.sdk.core.auth.GlobalCredentials;
import com.huaweicloud.sdk.core.exception.ClientRequestException;
import com.huaweicloud.sdk.core.exception.ServerResponseException;
import com.huaweicloud.sdk.core.http.HttpConfig;
import com.huaweicloud.sdk.iam.v3.IamClient;
import com.huaweicloud.sdk.iam.v3.model.*;


// Use the global domain name to obtain a loginToken.
String endpoint = "https://iam.myhuaweicloud.com";

// Configure client attributes.
HttpConfig config = HttpConfig.getDefaultHttpConfig()
        .withIgnoreSSLVerification(true)
        .withProxyHost("proxy.huawei.com")
        .withProxyPort(8080);

// Use the domain ID (account ID), AK, and SK of userB to initialize the
specified IAM client "{Service}Client". For details about how to create userB,
see section "Creating an IAM User".
IamClient iamClient = IamClient.newBuilder().withCredential(new
GlobalCredentials()
        .withDomainId("domainId")
        .withAk("ak")
        .withSk("sk"))
        .withEndpoint(endpoint)
        .withHttpConfig(config)
        .build();
/*CreateTemporaryAccessKeyByAgency
Call the API used to obtain a temporary access key and securityToken with an
agency.
The default validity period of an access key and securityToken is 900 seconds,
that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this
example, the validity period is set to 3600 seconds, that is, 1 hour.
When you obtain a loginToken with a specified validity period, ensure that the
```



```
validity period of the loginToken is not greater than the remaining validity
period of the securityToken.
*/
IdentityAssumerole identityAssumerole = new IdentityAssumerole().

withAgencyName("testagency").withDomainId("0525e2c87exxxxxxx").withSessionUser(new
 AssumeroleSessionuser().withName("ExternalUser")).withDurationSeconds(3600);
AgencyAuth agencyAuth = new AgencyAuth().withIdentity(new
AgencyAuthIdentity().withAssumeRole(identityAssumerole).

withMethods(Collections.singletonList(AgencyAuthIdentity.MethodsEnum.fromValue("as
sume_role"))));
CreateTemporaryAccessKeyByAgencyRequestBody
createTemporaryAccessKeyByAgencyRequestBody = new
CreateTemporaryAccessKeyByAgencyRequestBody().withAuth(agencyAuth);
CreateTemporaryAccessKeyByAgencyResponse createTemporaryAccessKeyByAgencyResponse
= iamClient.createTemporaryAccessKeyByAgency(new
CreateTemporaryAccessKeyByAgencyRequest().withBody(createTemporaryAccessKeyByAgenc
yRequestBody));
Credential credential = createTemporaryAccessKeyByAgencyResponse.getCredential();

/*CreateLoginToken
Obtain a loginToken.
LoginTokens are issued to users to log in through custom identity brokers. Each
loginToken contains identity and session information of a user.
To log in to a cloud service console using a custom identity broker URL, call
this API to obtain a loginToken for authentication.
The default validity period of a loginToken is 600 seconds, that is, 10 minutes.
The value ranges from 10 minutes to 12 hours. In this example, the validity
period is set to 1800 seconds, that is, half an hour.
Ensure that the validity period of the loginToken is not greater than the
remaining validity period of the securityToken.
When obtaining a securityToken with an agency, set the session_user.name
parameter in the request body.
*/
CreateLoginTokenRequestBody createLoginTokenRequestBody = new
CreateLoginTokenRequestBody().
        withAuth(new LoginTokenAuth().withSecuritytoken(new
LoginTokenSecurityToken().
                withAccess(credential.getAccess()).
                withId(credential.getSecuritytoken()).
                withSecret(credential.getSecret()).withDurationSeconds(1800)));
CreateLoginTokenResponse createLoginTokenResponse =
iamClient.createLoginToken(new
CreateLoginTokenRequest().withBody(createLoginTokenRequestBody));
String loginToken = createLoginTokenResponse.getXSubjectLoginToken();

// Login URL of the custom identity broker
String authURL = "https://auth.huaweicloud.com/authui/federation/login";
// Login URL of an enterprise management system.
String enterpriseSystemLoginURL = "https://example.com/";
// HUAWEI CLOUD service address to access.
String targetConsoleURL = "https://console.huaweicloud.com/iam/?region=cn-
north-4";

// Create a FederationProxyUrl and return it to the browser through Location.
String FederationProxyUrl = authURL + "?idp_login_url=" +
        URLEncoder.encode(enterpriseSystemLoginURL, "UTF-8") +
        "&service=" + URLEncoder.encode(targetConsoleURL, "UTF-8") +
        "&logintoken=" +URLEncoder.encode(loginToken, "UTF-8");
```

Ejemplo de código usando Python

El siguiente código de Python muestra cómo crear un FederationProxyUrl que da a los usuarios federados acceso directo a la consola de Huawei Cloud.

```
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.http.http_config import HttpConfig
from huaweicloudsdkiam.v3 import *
```



```
import urllib


# Use the global domain name to obtain a loginToken.
endpoint = "https://iam.myhuaweicloud.com"

# Configure client attributes.
config = HttpConfig.get_default_config()
config.ignore_ssl_verification = True
config.proxy_protocol = "https"
config.proxy_host = "proxy.huawei.com"
config.proxy_port = 8080
credentials = GlobalCredentials(ak, sk, domain_id)

# Use the domain ID (account ID), AK, and SK of userB to initialize the specified
IAM client "{Service}Client". For details about how to create userB, see section
"Creating an IAM User".
client = IamClient().new_builder(IamClient) \
    .with_http_config(config) \
    .with_credentials(credentials) \
    .with_endpoint(endpoint) \
    .build()

# CreateTemporaryAccessKeyByAgency
# Call the API used to obtain a temporary access key and securityToken with an
agency.
# The default validity period of an access key and securityToken is 900 seconds,
that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this
example, the validity period is set to 3600 seconds, that is, 1 hour.
# When you obtain a loginToken with a specified validity period, ensure that the
validity period of the loginToken is not greater than the remaining validity
period of the securityToken.
# When obtaining a securityToken with an agency, set the session_user.name
parameter in the request body.
assume_role_session_user = AssumeroleSessionuser(name="ExternalUser")
identity_assume_role = IdentityAssumerole(agency_name="testagency",
                                          domain_id="0525e2c87exxxxxxx",
                      session_user=assume_role_session_user,
                      duration_seconds=3600)
identity_methods = ["assume_role"]
body = CreateTemporaryAccessKeyByAgencyRequestBody(
    AgencyAuth(AgencyAuthIdentity(methods=identity_methods,
assume_role=identity_assume_role)))
request = CreateTemporaryAccessKeyByAgencyRequest(body)
create_temporary_access_key_by_agency_response =
client.create_temporary_access_key_by_agency(request)
credential = create_temporary_access_key_by_agency_response.credential

# CreateLoginToken
# Obtain a loginToken.
# The default validity period of a loginToken is 600 seconds, that is, 10
minutes. The value ranges from 10 minutes to 12 hours. In this example, the
validity period is set to 1800 seconds, that is, half an hour.
# Ensure that the validity period of the loginToken is not greater than the
remaining validity period of the securityToken.
login_token_security_token = LoginTokenSecurityToken(access=credential.access,
secret=credential.secret,
                             id=credential.securitytoken, duration_seconds=1800)
body = CreateLoginTokenRequestBody(LoginTokenAuth(login_token_security_token))
request = CreateLoginTokenRequest(body)
create_login_token_response = client.create_login_token(request)
login_token = create_login_token_response.x_subject_login_token

# Obtain a custom identity broker URL.
auth_URL = "https://auth.huaweicloud.com/authui/federation/login"
# Login URL of an enterprise management system.
enterprise_system_login_URL = "https://example.com/"
# HUAWEI CLOUD service address to access.
```



```
target_console_URL = "https://console.huaweicloud.com/iam/?region=cn-north-4"

# Create a FederationProxyUrl and return it to the browser through Location.
FederationProxyUrl = auth_URL + "?idp_login_url=" + urllib.parse.quote(
    enterprise_system_login_URL) + "&service=" + urllib.parse.quote(
    target_console_URL) + "&logintoken=" + urllib.parse.quote(login_token)
print(FederationProxyUrl)
```

10.3 Habilitación del acceso de agente de identidad personalizado con un token

Si el IdP de su empresa no es compatible con SAML o OpenID Connect, puede crear un agente de identidad personalizado para habilitar el acceso a Huawei Cloud. Puede escribir y ejecutar código para generar una URL de inicio de sesión. Los usuarios de su empresa pueden usar la URL para iniciar sesión en Huawei Cloud. Los usuarios serán autenticados por su IdP de empresa.

NOTA

Si su IdP empresarial es compatible con SAML u OpenID Connect, configure la **federación de identidad** para permitir que los usuarios de su empresa accedan a Huawei Cloud a través de SSO.

Prerrequisitos

- Su empresa tiene un sistema de gestión empresarial.
- El administrador de la empresa ha creado una cuenta (por ejemplo, **DomainA**) en Huawei Cloud.

Procedimiento

Paso 1 Utilice la cuenta **DomainA** para crear un usuario IAM (por ejemplo, **UserB**) siguiendo las instrucciones en **3.1 Creación de un usuario de IAM**.

Paso 2 (Opcional) Agregar **UserB** a un grupo de usuarios (por ejemplo, **GroupC**) y conceder permisos al grupo de usuarios siguiendo las instrucciones en **4.1 Creación de un grupo de usuarios y asignación de permisos**.

Paso 3 Configure **clave de acceso** (recomendada) o el nombre de usuario y la contraseña de **UserB** en el archivo de configuración de su IdP de empresa para que el usuario pueda obtener un token de usuario. Para la seguridad de la cuenta, cifre la contraseña y la clave de acceso antes de almacenarlos.

Paso 4 Inicie sesión en el sistema de gestión empresarial, acceda al agente de identidad personalizado seleccionando un usuario común de la lista de usuarios. Para obtener más información, consulte la documentación del sistema de gestión empresarial. Para este ejemplo, seleccione usuario **UserB**.

NOTA

La lista de usuarios del agente personalizado es la misma que la lista de usuarios de IAM en su cuenta de Huawei Cloud. Para alinear estos usuarios de IAM con las cuentas de usuario de su empresa, configure las **claves de acceso** (recomendadas) o nombres de usuario y contraseñas en el archivo de configuración del IdP de empresa.

Paso 5 El agente de identidad personalizado utiliza el token de **userB** para invocar a la API **POST / v3.0/OS-CREDENTIAL/securitytokens** usada para obtener una clave de acceso temporal y

securityToken. Para obtener más información, consulte **Obtención de una clave de acceso temporal**.

Paso 6 El agente de identidad personalizado utiliza la clave de acceso temporal, securityToken y el nombre de dominio global de IAM () para invocar a la API **POST /v3.0/OS-AUTH/securitytoken/logintokens** para obtener un loginToken. El valor de **X-Subject-LoginToken** en el encabezado de respuesta es un loginToken. Para obtener más información, consulte **Obtención de un token de inicio de sesión**.

NOTA

- Para obtener un loginToken invocando a la API **POST /v3.0/OS-AUTH/securitytoken/logintokens**, utilice el nombre de dominio global () de IAM.
- Un loginToken se emite a un usuario para iniciar sesión a través de un agente de identidad personalizado y contiene información de identidad y sesión sobre el usuario. Un loginToken es válido durante 10 minutos por defecto.
- Puede establecer el período de validez de un loginToken mediante invocación a la API **POST /v3.0/OS-AUTH/securitytoken/logintokens**. El período de validez oscila entre 10 minutos y 12 horas. Si el valor especificado es mayor que el período de validez restante del securityToken temporal, se utiliza el período de validez restante del securityToken temporal.

Paso 7 El agente de identidad personalizado genera un FederationProxyUrl y lo devuelve al navegador a través de **Location**.

```
https:///authui/federation/login?
idp_login_url={enterprise_system_loginURL}&service={console_service_region_url}&lo
gintoken={logintoken}
```

Ejemplo:

```
https:///authui/federation/login?idp_login_url=https%3A%2F
%2Fexample.com&service=https%3a%2f%2f%2fapm%2f%3fregion%3dcn-north-4%23%2fapm
%2fatps%2ftopology&logintoken=******
```

Tabla 10-2 Descripción de parámetro

Parámetro	Descripción
idp_login_url	URL de inicio de sesión del sistema de gestión empresarial.
service	Dirección de acceso de un servicio de Huawei Cloud.
logintoken	LoginToken del agente de identidad personalizado.

Para obtener más información sobre cómo crear un FederationProxyUrl consulte el ejemplo proporcionado en **10.4 Creación de un FederationProxyUrl mediante un token**.

NOTA

El FederationProxyUrl contiene el loginToken que se ha obtenido de IAM, y el valor de cada parámetro en el FederationProxyUrl se codifica mediante URLEncode.

Paso 8 Si el loginToken se autentica correctamente, se le redirigirá automáticamente a la dirección de servicio de Huawei Cloud especificada en el parámetro de **service**.

Si el loginToken no se autentica, se le redirigirá a la dirección especificada en **idp_login_url**.

----Fin

10.4 Creación de un FederationProxyUrl mediante un token

En esta sección se proporciona un ejemplo de código utilizado para crear un FederationProxyUrl mediante un token para iniciar sesión en los servicios de Huawei Cloud.

Ejemplo de código usando Java

El siguiente código Java muestra cómo crear un FederationProxyUrl que da a los usuarios federados acceso directo a la consola de Huawei Cloud.

```
import java.net.URLEncoder;
import java.util.Collections;
import com.huaweicloud.sdk.core.auth.GlobalCredentials;
import com.huaweicloud.sdk.core.http.HttpConfig;
import com.huaweicloud.sdk.core.exception.*;
import com.huaweicloud.sdk.iam.v3.IamClient;
import com.huaweicloud.sdk.iam.v3.model.*;

// Use the global domain name to obtain a loginToken.
String endpoint = "https://iam.myhuaweicloud.com";

// Configure client attributes.
HttpConfig config = HttpConfig.getDefaultHttpConfig()
        .withIgnoreSSLVerification(true)
        .withProxyHost("proxy.huawei.com")
        .withProxyPort(8080);

// Use the domain ID (account ID), AK, and SK of userB to initialize the
specified IAM client "{Service}Client". For details about how to create userB,
see section "Creating an IAM User".
IamClient iamClient = IamClient.newBuilder().withCredential(new
GlobalCredentials()
        .withDomainId(domainId)
        .withAk(ak)
        .withSk(sk))
        .withEndpoint(endpoint)
        .withHttpConfig(config)
        .build();

/*CreateTemporaryAccessKeyByToken
Call the API used to obtain a temporary access key and securityToken with a token.
The default validity period of an access key and securityToken is 900 seconds,
that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this
example, the validity period is set to 3600 seconds, that is, 1 hour.
When you obtain a loginToken with a specified validity period, ensure that the
validity period of the loginToken is not greater than the remaining validity
period of the securityToken.
*/
TokenAuthIdentity tokenAuthIdentity = new
TokenAuthIdentity().withMethods(Collections.singletonList(TokenAuthIdentity.Method
sEnum.fromValue("token"))).withToken(new
IdentityToken().withDurationSeconds(3600));
CreateTemporaryAccessKeyByTokenRequestBody
createTemporaryAccessKeyByTokenRequestBody = new
CreateTemporaryAccessKeyByTokenRequestBody().withAuth(new
TokenAuth().withIdentity(tokenAuthIdentity));
CreateTemporaryAccessKeyByTokenResponse createTemporaryAccessKeyByTokenResponse =
iamClient.createTemporaryAccessKeyByToken(new
CreateTemporaryAccessKeyByTokenRequest().withBody(createTemporaryAccessKeyByTokenR
equestBody));
Credential credential = createTemporaryAccessKeyByTokenResponse.getCredential();
```



```
/*CreateLoginToken
Obtain a loginToken.
LoginTokens are issued to users to log in through custom identity brokers. Each
loginToken contains identity and session information of a user.
To log in to a cloud service console using a custom identity broker URL, call
this API to obtain a loginToken for authentication.
The default validity period of a loginToken is 600 seconds, that is, 10 minutes.
The value ranges from 10 minutes to 12 hours. In this example, the validity
period is set to 1800 seconds, that is, half an hour.
Ensure that the validity period of the loginToken is not greater than the
remaining validity period of the securityToken.
*/
CreateLoginTokenRequestBody createLoginTokenRequestBody = new
CreateLoginTokenRequestBody().
        withAuth(new LoginTokenAuth().withSecuritytoken(new
LoginTokenSecurityToken().
                withAccess(credential.getAccess()).
                withId(credential.getSecuritytoken()).
                withSecret(credential.getSecret()).withDurationSeconds(1800)));
CreateLoginTokenResponse createLoginTokenResponse =
iamClient.createLoginToken(new
CreateLoginTokenRequest().withBody(createLoginTokenRequestBody));
String loginToken = createLoginTokenResponse.getXSubjectLoginToken();

// Obtain a custom identity broker URL.
String authURL = "https://auth.huaweicloud.com/authui/federation/login";
// Login URL of an enterprise management system.
String enterpriseSystemLoginURL = "https://example.com/";
// HUAWEI CLOUD service address to access.
String targetConsoleURL = "https://console.huaweicloud.com/iam/?region=cn-
north-4";

// Create a FederationProxyUrl and return it to the browser through Location.
String FederationProxyUrl = authURL + "?idp_login_url=" +
        URLEncoder.encode(enterpriseSystemLoginURL, "UTF-8") +
        "&service=" + URLEncoder.encode(targetConsoleURL, "UTF-8") +
        "&logintoken=" +URLEncoder.encode(loginToken, "UTF-8");
```

Ejemplo de código usando Python

El siguiente código de Python muestra cómo crear un FederationProxyUrl que da a los usuarios federados acceso directo a la consola de Huawei Cloud.

```
from huaweicloudsdkcore.auth.credentials import GlobalCredentials
from huaweicloudsdkcore.http.http_config import HttpConfig
from huaweicloudsdkiam.v3 import *

import urllib

# Use the global domain name to obtain a loginToken.
endpoint = "https://iam.myhuaweicloud.com"

# Configure client attributes.
config = HttpConfig.get_default_config()
config.ignore_ssl_verification = True
config.proxy_protocol = "https"
config.proxy_host = "proxy.huawei.com"
config.proxy_port = 8080
credentials = GlobalCredentials(ak, sk, domain_id)

# Use the domain ID (account ID), AK, and SK of userB to initialize the specified
IAM client "{Service}Client". For details about how to create userB, see section
"Creating an IAM User".
client = IamClient().new_builder(IamClient) \
    .with_http_config(config) \
    .with_credentials(credentials) \
    .with_endpoint(endpoint) \
    .build()
```



```
# CreateTemporaryAccessKeyByToken
# Call the API used to obtain a temporary access key and securityToken with a
token.
# The default validity period of an access key and securityToken is 900 seconds,
that is, 15 minutes. The value ranges from 15 minutes to 24 hours. In this
example, the validity period is set to 3600 seconds, that is, 1 hour.
# When you obtain a loginToken with a specified validity period, ensure that the
validity period of the loginToken is not greater than the remaining validity
period of the securityToken.
identity_methods = ["token"]
identity_token = IdentityToken(duration_seconds=3600)
body = CreateTemporaryAccessKeyByTokenRequestBody(
    TokenAuth(TokenAuthIdentity(methods=identity_methods, token=identity_token)))
request = CreateTemporaryAccessKeyByTokenRequest(body)
create_temporary_access_key_by_token_response =
client.create_temporary_access_key_by_token(request)
credential = create_temporary_access_key_by_token_response.credential

# CreateLoginToken
# Obtain a loginToken.
# LoginTokens are issued to users to log in through custom identity brokers. Each
loginToken contains identity and session information of a user.
# To log in to a cloud service console using a custom identity broker URL, call
this API to obtain a loginToken for authentication.
# The default validity period of a loginToken is 600 seconds, that is, 10
minutes. The value ranges from 10 minutes to 12 hours. In this example, the
validity period is set to 1800 seconds, that is, half an hour.
# Ensure that the validity period of the loginToken is not greater than the
remaining validity period of the securityToken.
login_token_security_token = LoginTokenSecurityToken(access=credential.access,
secret=credential.secret,
                             id=credential.securitytoken, duration_seconds=1800)
body = CreateLoginTokenRequestBody(LoginTokenAuth(login_token_security_token))
request = CreateLoginTokenRequest(body)
create_login_token_response = client.create_login_token(request)
login_token = create_login_token_response.x_subject_login_token


# Login URL of the custom identity broker
auth_URL = "https://auth.huaweicloud.com/authui/federation/login"
# Login URL of an enterprise management system.
enterprise_system_login_URL = "https://example.com/"
# HUAWEI CLOUD service address to access.
target_console_URL = "https://console.huaweicloud.com/iam/?region=cn-north-4"

# Create a FederationProxyUrl and return it to the browser through Location.
FederationProxyUrl = auth_URL + "?idp_login_url=" + urllib.parse.quote(
    enterprise_system_login_URL) + "&service=" + urllib.parse.quote(
    target_console_URL) + "&logintoken=" + urllib.parse.quote(login_token)
print(FederationProxyUrl)
```


11 Autenticación MFA y dispositivo MFA virtual

11.1 Autenticación MFA

¿Qué es la autenticación MFA?

La autenticación MFA proporciona una capa adicional de protección sobre el nombre de usuario y la contraseña. Si habilita la autenticación MFA, los usuarios deben ingresar el nombre de usuario y la contraseña, así como un código de verificación para poder iniciar sesión en la consola.

La autenticación MFA también se puede habilitar para verificar la identidad de un usuario antes de que se permita al usuario realizar operaciones críticas.

Métodos de autenticación MFA

La autenticación MFA se puede realizar a través de SMS, correo electrónico y dispositivo MFA virtual.

Escenarios de aplicación

La autenticación MFA es adecuada para la protección de inicio de sesión y la protección de operaciones críticas. Si la autenticación MFA está habilitada, la configuración tiene efecto tanto para la consola de gestión como para las API de REST.

- Protección de inicio de sesión: Cuando usted o un IAM de su cuenta inicia sesión en la consola, usted y el usuario deben ingresar un código de verificación además del nombre de usuario y la contraseña.
- Protección de la operación: cuando usted o un IAM de su cuenta intenta realizar una operación crítica, como eliminar un recurso ECS, usted y el usuario deben introducir un código de verificación para continuar.

Para obtener más información acerca de la protección de inicio de sesión y la protección de operaciones críticas, consulte **8.3 Protección de operaciones críticas**.

11.2 Dispositivo MFA virtual

Esta sección describe cómo **vincular** y **desvincular** un dispositivo MFA virtual. Si se elimina el dispositivo MFA virtual enlazado de un usuario de IAM o el teléfono móvil en el que se ejecuta no está disponible, puede **quitar** el dispositivo MFA virtual para el usuario de IAM.

¿Qué es un dispositivo MFA virtual?

Un dispositivo MFA genera códigos de verificación de 6 dígitos de acuerdo con el algoritmo de contraseña de un solo uso basado en tiempo (TOTP). Los dispositivos MFA pueden estar basados en hardware o software. Actualmente, los dispositivos MFA virtuales basados en software son compatibles. Son programas de aplicación que se ejecutan en dispositivos inteligentes como teléfonos móviles.

Vinculación de un dispositivo MFA virtual

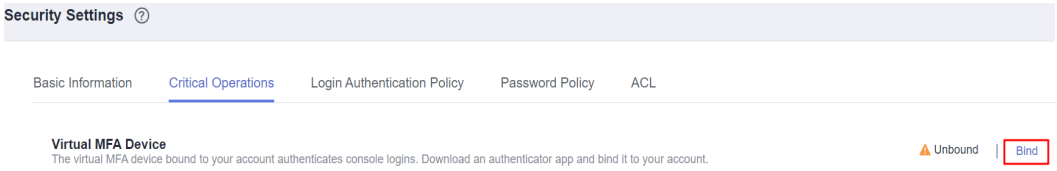
Antes de vincular un dispositivo MFA virtual, instale primero una aplicación de autenticación (como Google Authenticator o Microsoft Authenticator) en su dispositivo móvil.

- **Cuenta de Huawei Cloud**

Paso 1 Vaya a la página **Configuración de seguridad**.

Paso 2 Haga clic en la pestaña **Critical Operations** y haga clic en **Bind** en la fila **Virtual MFA Device**.

Figura 11-1 Dispositivo MFA virtual



Paso 3 Configure la aplicación MFA escaneando el código QR o introduciendo manualmente la clave secreta.

Puede vincular un dispositivo MFA virtual a su cuenta escaneando el código QR o introduciendo la clave secreta.

- Escanear el código QR

  Abra la aplicación MFA en su teléfono móvil y utilice la aplicación para escanear el código QR que se muestra en la página **Bind Virtual MFA Device**. Su cuenta o usuario de IAM se agrega a la aplicación.

- Introducir manualmente la clave secreta

  Abra la aplicación MFA en su teléfono móvil e introduzca la clave secreta.

  NOTA

  El usuario solo se puede agregar manualmente utilizando contraseñas de un solo uso basadas en el tiempo (TOTP). Se recomienda activar la configuración automática de la hora en su teléfono móvil.

Paso 4 Vea los códigos de verificación en la aplicación MFA. El código se actualiza automáticamente cada 30 segundos.

Paso 5 En la página **Bind Virtual MFA Device**, introduzca dos códigos de verificación consecutivos y haga clic en **OK**.

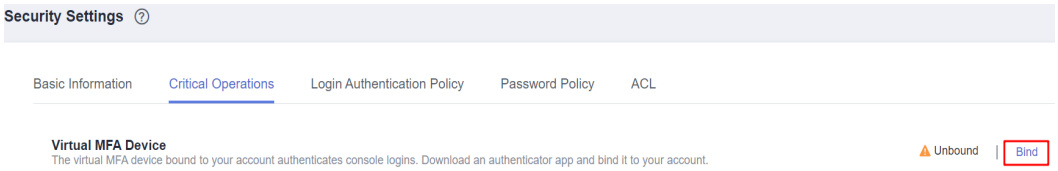
----Fin

- **HUAWEI ID**

Paso 1 Vaya a la página **Configuración de seguridad**.

Paso 2 Haga clic en la pestaña **Critical Operations** y haga clic en **Bind** en la fila **Virtual MFA Device**.

Figura 11-2 Vinculación de un dispositivo MFA virtual



Paso 3 En la página de **Account & security** del centro de cuentas de ID de HUAWEI, asocie un autenticador con su ID de HUAWEI según las instrucciones.

----Fin

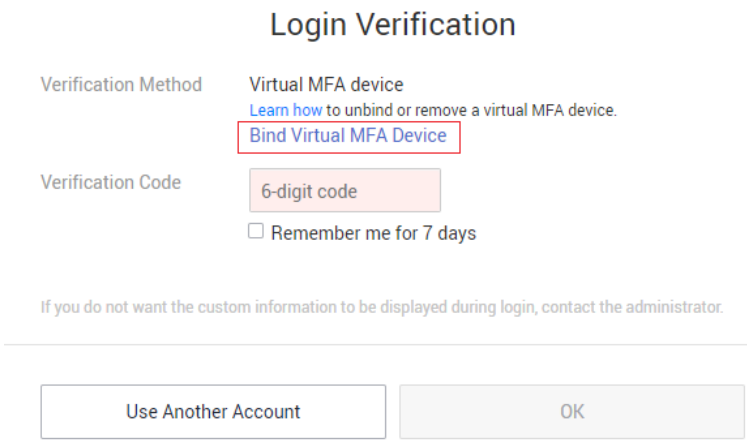
- **Usuario de IAM**

Los usuarios de IAM pueden enlazar un dispositivo MFA virtual en la consola de IAM. El procedimiento es el mismo que para **vincular un dispositivo MFA virtual para una cuenta de Huawei Cloud**.

Si el administrador ha restablecido el dispositivo MFA virtual de un usuario de IAM, o el usuario de IAM inicia sesión en el sistema por primera vez y se ha habilitado la protección de inicio de sesión con el dispositivo MFA virtual como método de verificación, el usuario de IAM necesita enlazar un dispositivo MFA virtual de nuevo durante el inicio de sesión. El procedimiento es el siguiente:

Paso 1 Inicie sesión en la consola de gestión como usuario de IAM.

Paso 2 En el cuadro de diálogo **Login Verification**, haga clic en **Bind Virtual MFA Device**.



Paso 3 En el panel deslizante, siga las indicaciones para enlazar un dispositivo MFA virtual.

----Fin

Obtención de un código de verificación MFA

Si está habilitada la protección de inicio de sesión virtual basada en MFA o la protección de operación, deberá introducir un código de verificación de MFA cuando inicie sesión en la consola o realice una operación crítica.

Abra la aplicación MFA en su dispositivo inteligente, vea el código de verificación que aparece junto a su cuenta y, a continuación, introduzca el código en la consola.

Desvinculación de un dispositivo MFA virtual

Puede desvincular el dispositivo MFA virtual siempre que el celular vinculado al dispositivo MFA virtual esté disponible y el dispositivo MFA virtual siga instalado en su teléfono.

- Usuario de IAM: Si el teléfono móvil de un usuario de IAM no está disponible o el dispositivo MFA virtual se ha eliminado del teléfono, solicite al administrador que **quite el dispositivo MFA virtual**.
- Administrador de la cuenta: si el teléfono móvil asociado a la cuenta no está disponible o el dispositivo MFA virtual se ha eliminado del teléfono, póngase en contacto con el servicio de atención al cliente para quitar el dispositivo MFA virtual.

Paso 1 Vaya a la página **Configuración de seguridad**.

Paso 2 Haga clic en la pestaña **Critical Operations** y haga clic en **Unbind** en la fila **Virtual MFA Device**.

NOTA

Si ha actualizado su cuenta de Huawei Cloud a un ID de HUAWEI, será redirigido al sitio web de ID de HUAWEI. Vaya a la página **Account center** > **Account and security** y haga clic en **Disassociate** en la fila **Authenticator** del área **Security verification**.

Paso 3 En la página **Unbind Virtual MFA Device**, introduzca un código de verificación generado por la aplicación MFA.

Figura 11-3 Introducir un código de verificación MFA virtual

Paso 4 Haga clic en **OK**.

----Fin

Eliminación del dispositivo MFA virtual

Como **account administrator**, si su teléfono móvil no está disponible o el dispositivo MFA virtual se ha eliminado del teléfono, póngase en contacto con el servicio de atención al cliente para quitar el dispositivo MFA virtual.

Si el teléfono móvil de un usuario de IAM no está disponible o el dispositivo MFA virtual se ha eliminado del teléfono del usuario, como un **administrador**, puede quitar el dispositivo MFA virtual realizando el siguiente procedimiento:

Paso 1 Inicie sesión en la consola de IAM.

Paso 2 En la página **Users**, haga clic en **Security Settings** en la fila que contiene el usuario para el que desea quitar el dispositivo MFA virtual enlazado.

Paso 3 En la página de la pestaña **Security Settings**, haga clic en **Remove** en la fila **Virtual MFA Device**.

Paso 4 Haga clic en **OK**.

----Fin

12 Consulta de registros de operación de IAM

12.1 Habilitación de CTS

CTS registra las operaciones realizadas en recursos en la nube en su cuenta. Los registros de operaciones se pueden utilizar para realizar análisis de seguridad, realizar un seguimiento de los cambios de recursos, realizar auditorías de cumplimiento y localizar fallas.

Se recomienda habilitar el servicio CTS para registrar las operaciones clave de IAM, como crear y eliminar usuarios.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

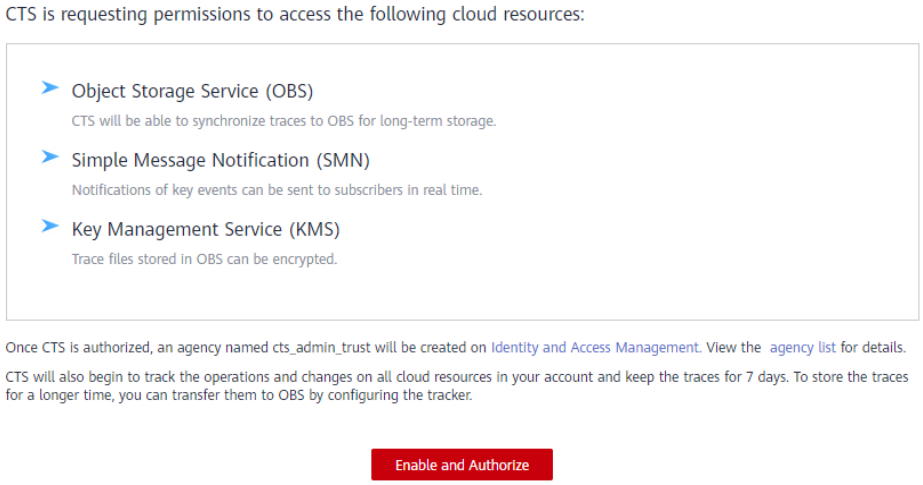
Paso 2 Si inicia sesión en Huawei Cloud con una cuenta, vaya a **Paso 3**. Si inicia sesión como usuario de IAM, solicite al administrador que asigne los siguientes permisos:

- Administrador de seguridad
- FullAccess de CTS

Para obtener más información, véase **3.2 Asignación de permisos a un usuario de IAM**.

Paso 3 Elija **Service List** >**Management & Governance** > **Cloud Trace Service**.

Figura 12-1 Habilitación y autorización de CTS



Paso 4 En la página de autorización mostrada, haga clic en **Enable and Authorize**.

NOTA

- Al utilizar CTS, debe tener los permisos necesarios para las operaciones pertinentes, pero no es necesario que se le conceda la función de **Security Administrator** de nuevo.
- Después de habilitar CTS, el sistema crea automáticamente dos rastreadores para registrar las trazas de gestión, es decir, las operaciones (como la creación, el inicio de sesión y la eliminación) realizadas en todos los recursos de la nube.
  - En la **current region**, se crea un rastreador para registrar las trazas de gestión de todos los servicios a nivel de proyecto desplegados en esta región.
  - En la región **CN-Hong Kong**, se crea un rastreador para registrar las trazas de gestión de todos los servicios globales, como IAM.

----Fin

CTS registra todas las operaciones realizadas en IAM, como la creación de usuarios y grupos de usuarios. **Tabla 12-1** muestra las operaciones de IAM que pueden ser registradas por CTS.

Tabla 12-1 Operaciones de IAM que pueden ser registradas por CTS

Operación	Tipo de recurso	Nombre del rastro
Inicio de sesión	user	login
Error en el inicio de sesión (no se incluyen los errores de inicio de sesión del ID de HUAWEI)	user	loginFailed
Cierre de sesión	user	logout
Iniciar sesión con un código QR	user	scanQRCodeLogin

Operación	Tipo de recurso	Nombre del rastro
Error al inicio de sesión usando un código QR	user	scanQRCodeLoginFailed
Inicio de sesión por OpenID Connect	user	oidcLoginSuccess
Error de inicio de sesión por OpenID Connect	user	oidcLoginFailed
Inicio de sesión por SSO	user	iamUserSsoLoginSuccess
Error al iniciar sesión mediante SSO	user	iamUserSsoLoginFailed
Restablecimiento de la contraseña	user	fpwdResetSuccess
Creación de un usuario de IAM	user	createUser
Cambio de la dirección de correo electrónico o el número de teléfono móvil	user	updateUser
Eliminación de un usuario	user	deleteUser
Cambio de contraseña	user	updateUserPwd
Establecimiento de una contraseña para un usuario (por el administrador)	user	updateUserPwd
Modificación de la protección de inicio de sesión de un usuario de IAM	user	modifyLoginProtect
Cambio del número de teléfono móvil mediante un correo electrónico	user	changeMobileByEmail

Operación	Tipo de recurso	Nombre del rastro
Cambio de la contraseña mediante un correo electrónico	user	updateUserPwdByEmail
Inicio de sesión inicial exitoso como usuario federado	user	tenantLoginBySamlSuccess
Inicio de sesión exitoso usando información en caché como usuario federado	user	federationLoginNoPwdSuccess
Error al iniciar sesión usando información en caché como usuario federado	user	federationLoginNoPwdFailed
Creación de un grupo de usuarios	userGroup	createGroup
Modificación de un grupo de usuarios	userGroup	updateGroup
Eliminación de un grupo de usuarios	userGroup	deleteGroup
Adición de usuarios a un grupo de usuarios	userGroup	addUserToGroup
Eliminación de usuarios de un grupo de usuarios	userGroup	removeUserFromGroup
Desvinculación de un dispositivo MFA virtual	MFA	UnBindMFA
Vinculación de un dispositivo MFA virtual	MFA	BindMFA
Creación de un proyecto	project	createProject
Modificación de un proyecto	project	updateProject

Operación	Tipo de recurso	Nombre del rastro
Eliminación de un proyecto	project	deleteProject
Creación de una delegación	agency	createAgency
Modificación de una delegación	agency	updateAgency
Eliminación de una delegación	agency	deleteAgency
Cambio de una delegación	agency	switchRole
Asignación de todos los permisos de proyecto a una delegación	agency	updateAgencyInheritedGrants
Revocación de todos los permisos de proyecto de una delegación	agency	deleteAgencyInheritedGrants
Asignación de permisos de servicio global a una delegación	agency	updateAgencyAssignsByRole
Asignación de permisos de servicio global a una delegación (API)	roleAgencyDomain	assignRoleToAgencyOnDomain
Actualización de permisos de delegación	agency	updateAgencyAssignsByRole
Registro de un proveedor de identidad	identityProvider	createIdentityProvider
Modificación de un proveedor de identidad	identityProvider	updateIdentityProvider
Eliminación de un proveedor de identidad	identityProvider	deleteIdentityProvider

Operación	Tipo de recurso	Nombre del rastro
Actualización de una regla de conversión de identidad	identityProvider	updateMapping
Actualización de los metadatos del proveedor de identidad	identityProvider	metadataConfiguration
Edición manual de metadatos de un IdP preestablecido	identityProvider	metadataConfiguration
Registro de una asignación	mapping	createMapping
Actualización de un mapeo	mapping	updateMapping
Supresión de un mapeo	mapping	deleteMapping
Registro de un protocolo	identityProvider	createProtocol
Actualización de un protocolo	identityProvider	updateProtocol
Eliminación de un protocolo	identityProvider	deleteProtocol
Revocación de los permisos de servicio global de una delegación	roleAgencyDomain	unassignRoleToAgencyOnDomain
Asignación de permisos de proyecto a una delegación	roleAgencyProject	assignRoleToAgencyOnProject
Revocación de permisos de proyecto desde una delegación	roleAgencyProject	unassignRoleToAgencyOnProject
Modificación de la política de autenticación de inicio de sesión	SecurityPolicy	modifySecurityPolicy

Operación	Tipo de recurso	Nombre del rastro
Modificación de la política de contraseñas	SecurityPolicy	modifySecurityPolicy
Modificación de la ACL	SecurityPolicy	modifySecurityPolicy
Modificación de la política de autenticación de inicio de sesión	loginpolicy	securitypolicy
Modificación de la política de contraseñas	passwordpolicy	securitypolicy
Modificación de la ACL	acl	securitypolicy
Creación de una cuenta	domain	createDomain
Actualizar una cuenta	domain	updateDomain
Eliminar una cuenta	domain	deleteDomain
Error de inicio de sesión a través de OpenID Connect	domain	oidcLoginFailed
Creación de una política personalizada	Policy	createRole
Modificación de una política personalizada	Policy	updateRole
Eliminación de una política personalizada	Policy	deleteRole
Asignación de permisos de servicio global a un grupo de usuarios (API)	assignment	createAssignment

Operación	Tipo de recurso	Nombre del rastro
Asignación de permisos de servicio global a un grupo de usuarios	group	updateGroupAssignsByRole
Revocación de permisos de servicio global de un grupo de usuarios	assignment	deleteAssignment
Creación de un AK/SK permanente	credential	createCredential
Actualización de una clave de acceso permanente (AK/SK)	credential	updateCredential
Eliminación de una clave de acceso permanente (AK/SK)	credential	deleteCredential
Desactivación o activación de una clave de acceso (AK/SK)	credential	updateCredential
Asignación de permisos a usuarios o proyectos de empresa	assignment	grantRoleToUserOnEnterpriseProject
Revocación de permisos de usuarios o proyectos empresariales	enterpriseProject	revokeRoleFromUserOnEnterpriseProject
Actualización de permisos de grupo de usuarios para proyectos de empresa	enterpriseProject	updateRoleFromGroupOnEnterpriseProject
Creación de un grupo de usuarios	group	createGroup

Operación	Tipo de recurso	Nombre del rastro
Eliminación de un grupo de usuarios	group	deleteGroup

12.2 Consulta de registros de auditoría de IAM

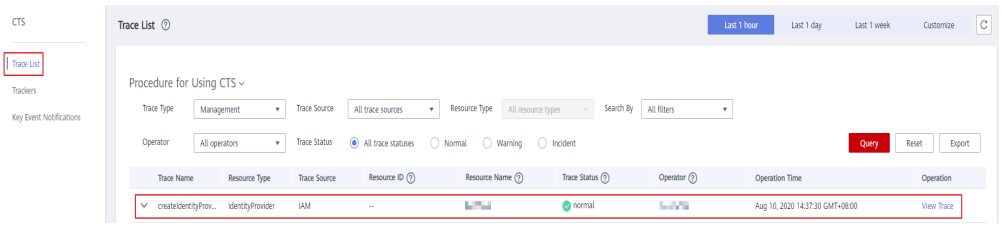
Después de habilitar CTS, registra las operaciones clave realizadas en IAM y otros servicios compatibles. CTS conserva los registros de operaciones durante los últimos 7 días.

Procedimiento

Paso 1 En la consola de IAM, realice una operación, como crear un usuario llamado **CTS-Test**.

Paso 2 Inicie sesión en la consola CTS y vea los registros de operación de IAM.

Figura 12-2 Consulta de registros de operación de IAM

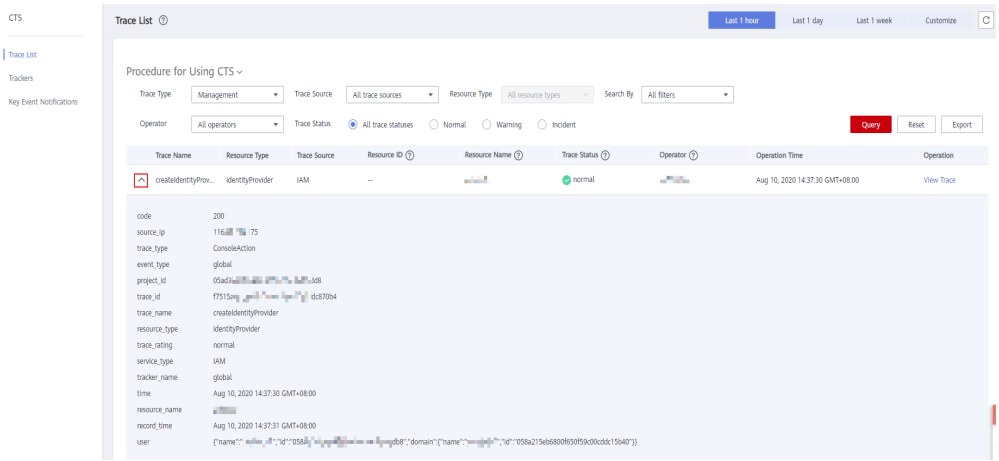


NOTA

IAM es un servicio global, y las operaciones en IAM serán registradas por CTS bajo el proyecto **CN-Hong Kong** por defecto. En la consola CTS, cambie a la región **CN-Hong Kong** y, a continuación, vea los registros de operación de IAM.

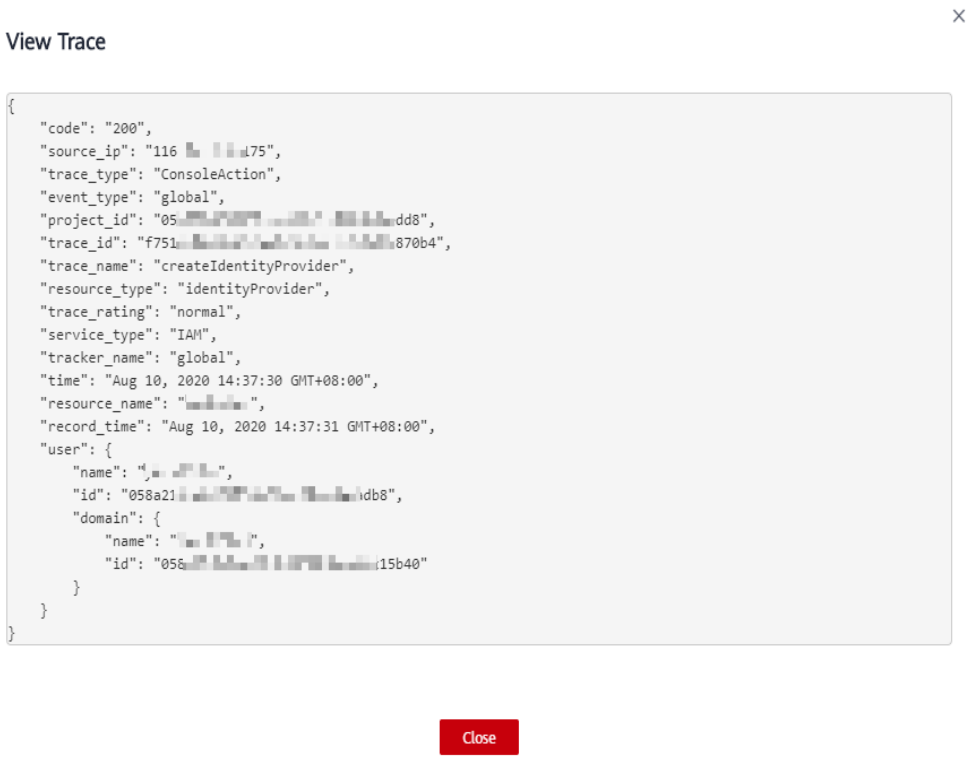
Paso 3 Haga clic en junto a una traza para ver su información básica.

Figura 12-3 Consulta de información básica del evento



Paso 4 Haga clic en **View Trace** a la derecha de una traza para ver la estructura de traza.

Figura 12-4 Consulta de los detalles del evento



----Fin

13 Cuotas

¿Qué es una cuota?

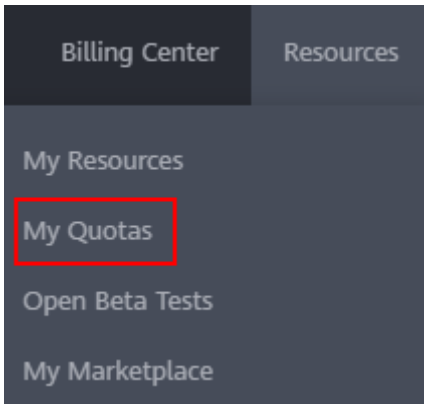
Una cuota es un límite en la cantidad o capacidad de un determinado tipo de recursos de servicio que un usuario puede utilizar, por ejemplo, el número máximo de usuarios o grupos de usuarios de IAM que puede crear.

Si la cuota de recursos actual no puede satisfacer sus requisitos de servicio, puede solicitar una cuota más alta.

¿Cómo puedo ver mis cuotas?

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione una región y un proyecto.
3. En la esquina superior derecha de la página, seleccione **Resources** > **My Quotas**.
   Se muestra la página **Quota**.

   Figura 13-1 Mis cuotas

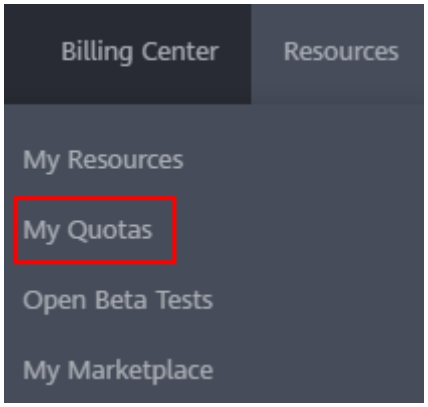
4. Click (the **My Quotas** icon) in the upper right corner.
   The **Quotas** page is displayed.
5. Click (the **My Quotas** icon) in the upper right corner.
   The **Quotas** page is displayed.

6. En la página **Quotas**, vea las cuotas usadas y totales de cada tipo de recursos.
   Si la cuota no puede cumplir con sus requisitos de servicio, aumente la cuota.

¿Cómo puedo aumentar mi cuota?

1. Inicie sesión en la consola de gestión.
2. En la esquina superior derecha de la página, seleccione **Resources** > **My Quotas**.
   Se muestra la página **Quotas**.

   Figura 13-2 Mis cuotas



3. Haga clic en **Increase Quota**.
4. En la página **Create Service Ticket**, establezca los parámetros.
   En el área **Problem Description**, introduzca la cuota requerida y el motivo del ajuste de cuota.
5. Lea los acuerdos y confirme que está de acuerdo con ellos y, a continuación, haga clic en **Submit**.

14 Historial de cambio

Tabla 14-1 Historial de cambio

Lanzado en	Descripción
2022-06-17	Este es el vigésimo quinto lanzamiento oficial. Se admite operaciones por lotes admitidas que incluyen información de modificación por lotes sobre usuarios de IAM, usuarios de eliminación por lotes, grupos de usuarios y agencias, y permisos de revocación por lotes.
2021-11-30	Esta versión es el vigésimo cuarto lanzamiento oficial, que incorpora los siguientes cambios: Actualizó secciones sobre autorización y políticas personalizadas basadas en cambios en la función de autorización.
2021-11-01	Esta versión es el vigésimo tercer lanzamiento oficial, que incorpora los siguientes cambios: Actualizado **2 Inicio de sesión en Huawei Cloud** basado en la nueva función de inicio de sesión de ID de HUAWEI.
2021-09-02	Este versión es el vigésimo segundo lanzamiento oficial, que incorpora los siguientes cambios: ● Agregada la sección **5.5 Registros de autorización**. ● Agregada la sección **Permisos**. ● Sección modificada **4.4 Consulta o modificación de la información del grupo de usuarios**.
2021-08-16	Esta versión es el vigésimo primer lanzamiento oficial, que incorpora el siguiente cambio: Agregada la sección **Autogestión de la información**.
2021-04-22	Esta edición es el vigésimo lanzamiento oficial, que incorpora el siguiente cambio: Agregada la sección **13 Cuotas**.

Lanzado en	Descripción
2021-04-16	Esta edición es el decimonoveno lanzamiento oficial, que incorpora el siguiente cambio: Agregada la sección **Inicio de sesión como usuario federado**.
2021-03-27	Esta edición es el decimoctavo lanzamiento oficial, que incorpora el siguiente cambio: Actualizado **2 Inicio de sesión en Huawei Cloud** basado en la nueva función de inicio de sesión de ID de HUAWEI.
2021-03-24	Esta versión es el decimoséptimo lanzamiento oficial, que incorpora el siguiente cambio: Agregada la sección **5.6.4 Servicios en la nube que admiten la autorización a nivel de recursos mediante IAM**.
2020-12-30	Esta versión es la decimosexta versión oficial, que incorpora los siguientes cambios: Se ha actualizado el documento en función de los cambios en la página de inicio de sesión, la función de configuración de seguridad y las cadenas de interfaz de usuario.
2020-11-26	Esta versión es el decimoquinto lanzamiento oficial, que incorpora el siguiente cambio: Modificada sección **8 Configuraciones de seguridad** basada en cambios de consola.
2020-11-05	Esta versión es la decimocuarta versión oficial, que incorpora los siguientes cambios: ● Ajustada la estructura de **9 Proveedores de identidades**. ● Agregada la sección **9.5.1 Descripción general del inicio de sesión único del usuario virtual mediante OpenID Connect**.
2020-10-26	Esta edición es la decimotercera versión oficial, que incorpora el siguiente cambio: Se han actualizado las capturas de pantalla de la página de inicio de sesión en función del cambio en el método de inicio de sesión.
2020-09-11	Esta versión es la duodécima versión oficial, que incorpora el siguiente cambio: Sección modificada **3 Usuarios de IAM** basada en cambios de consola.
2020-08-18	Esta edición es la undécima versión oficial, que incorpora el siguiente cambio: Agregada la sección **2 Inicio de sesión en Huawei Cloud**.

Lanzado en	Descripción
2020-04-20	Esta versión es el décimo lanzamiento oficial, que incorpora los siguientes cambios: Se han añadido descripciones acerca de la eliminación de usuarios en **4.2 Agregar o quitar usuarios de un grupo de usuarios**. Agregada la sección **4.5 Revocación de permisos de un grupo de usuarios**.
2020-03-30	Esta edición es la novena versión oficial, que incorpora el siguiente cambio: Descripciones eliminadas de pruebas beta abiertas para el control de acceso basado en políticas. Esta función está actualmente en uso comercial.
2020-02-10	Esta versión es el octavo lanzamiento oficial, que incorpora los siguientes cambios: Agregada la sección **5.4 Cambios en los nombres de políticas definidos por el sistema**. Sección modificada **4.1 Creación de un grupo de usuarios y asignación de permisos** basada en cambios de nombre de política.
2020-01-20	Esta versión es el séptimo lanzamiento oficial, que incorpora los siguientes cambios: Modificadas las siguientes secciones según los cambios de consola: **4 Grupos de usuarios y autorización** y **5 Gestión de permisos**
2019-11-20	Esta versión es el sexto lanzamiento oficial, que incorpora los siguientes cambios: Agregado **Puntos de conexión de la VPC** en **8.6 ACL**. Agregado **Activación/Desactivación de una clave de acceso** en **3.7 Gestión de claves de acceso para un usuario de IAM**.
2019-10-15	Esta versión es el quinto lanzamiento oficial, que incorpora los siguientes cambios: Agregada la sección **5.6.2 Modificación o eliminación de una política personalizada**. Descripciones agregadas sobre la creación de políticas personalizadas en el editor visual en **5.6.1 Creación de una política personalizada**. Agregadas descripciones acerca de la sintaxis de las políticas utilizadas para asignar permisos a nivel de recursos y condiciones en **5.3 Políticas** y **5.6.3 Casos de uso de políticas personalizadas**.

Lanzado en	Descripción
2019-09-29	Esta versión es el cuarto lanzamiento oficial, que incorpora el siguiente cambio: Agregada la sección **10 Broker de identidades personalizado**.
2019-06-11	Esta edición es la tercera versión oficial, que incorpora el siguiente cambio: Optimizados capítulos **1 Antes de comenzar**, **3 Usuarios de IAM**, **4 Grupos de usuarios y autorización**, **5 Gestión de permisos**, **6 Proyectos**, **8 Configuraciones de seguridad**, y **12 Consulta de registros de operación de IAM**.
2018-02-13	Esta versión es el segundo lanzamiento oficial, que incorpora el siguiente cambio: Agregada una tabla que describe los tipos de delegación en **7 Agencias**.
2017-12-30	Esta edición es el primer lanzamiento oficial.

